Cisco ASA Series 명령 참조, S 명령

업데이트 날짜: 2014년 11월 5일

Cisco Systems, Inc.
www.cisco.com

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.
주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트
www.cisco.com/go/offices에서 확인하십시오.

텍스트 파트 번호: 해당 사항 없음, 온라인 전용

이 설명서의 제품 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항은 정확한 것으로 간주되지만 이에 대해 명시적이든 묵시적이든 어떠한 보증도 없이 제공됩니다. 모든 제품의 애플리케이션 사용에 대한 책임은 전적으로 사용자에게 있습니다.

동봉된 제품의 소프트웨어 라이센스 및 제한 보증은 제품과 함께 제공되는 정보 패킷에 설명되어 있으며 본 참조 문서에 통합되어 있습니다. 소프트웨어 라이센스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

Cisco 또는 해당 공급업체는 피해의 가능성에 대해 언급한 경우라도 이 설명서의 사용 또는 사용 불능으로 인해 발생하는 이익 손실, 데이터 손실 또는 손상을 포함하여(단, 이에 한하지 않음) 간접, 특별, 중대 또는 부수적 손해에 대해 어떠한 경우라도 책임을 지지 않습니다.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASA Series 명령 참조, S 명령
© 2014 Cisco Systems, Inc. All rights reserved.

1 장

same-security-traffic through shape 명령

same-security-traffic

보안 수준이 같은 인터페이스 간의 통신을 허용하거나, 트래픽이 동일한 인터페이스로 들어오고 나가도록 허용하려면 글로벌 컨피그레이션 모드에서 **same-security-traffic** 명령을 사용합니다. same-security traffic을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

same-security-traffic permit {**inter-interface** | **intra-interface**}

no same-security-traffic permit {**inter-interface** | **intra-interface**}

구문 설명

inter-interface	보안 수준이 동일한 인터페이스 간의 통신을 허용합니다.
intra-interface	동일한 인터페이스로 들어오고 나가는 통신을 허용합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.2(1)	이제 **intra-interface** 키워드는 IPsec 트래픽뿐만 아니라 모든 트래픽이 동일한 인터페이스로 들어오고 나가도록 허용합니다.

사용 지침

동일한 보안 인터페이스 간의 통신을 허용하면(**same-security-traffic inter-interface** 명령을 통해 활성화됨) 다음과 같은 이점이 있습니다.

- 101개가 넘는 통신 인터페이스를 구성할 수 있습니다. 각 인터페이스에 서로 다른 수준을 사용하는 경우 수준(0~100)당 하나의 인터페이스만 구성할 수 있습니다.
- 액세스 목록 없이 동일한 모든 보안 인터페이스 간에 트래픽이 자유롭게 흐르도록 허용할 수 있습니다.

same-security-traffic intra-interface 명령은 트래픽이 동일한 인터페이스로 들어오고 나가도록 해 줍니다(이는 일반적으로 허용되지 않음). 이 기능은 인터페이스로 들어온 다음 동일한 인터페이스에서 라우팅되는 VPN 트래픽에 유용할 수 있습니다. 이 경우 VPN 트래픽은 암호화되지 않거나 다른 VPN 연결을 위해 다시 암호화될 수 있습니다. 예를 들어 허브 및 스포크 VPN 네트워크가 있는 경우(여기서 ASA는 허브이고 원격 VPN 네트워크는 스포크) 스포크 간에 통신하려면 트래픽이 ASA로 들어간 다음 다른 스포크로 다시 나가야 합니다.

참고 **same-security-traffic intra-interface** 명령에서 허용하는 모든 트래픽에는 방화벽 규칙이 여전히 적용됩니다. 따라서 ASA를 트래버스하지 않기 위해 트래픽을 반환할 수 있는 비대칭 라우팅 상황을 만들지 마십시오.

예

다음 예에서는 동일한 보안 인터페이스 통신을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# same-security-traffic permit inter-interface
```

다음 예에서는 트래픽이 동일한 인터페이스로 들어오고 나가도록 허용하는 방법을 보여 줍니다.

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

관련 명령

명령	설명
show running-config same-security-traffic	**same-security-traffic** 컨피그레이션을 표시합니다.

sasl-mechanism

LDAP 서버에 LDAP 클라이언트를 인증하는 SASL(Simple Authentication and Security Layer) 메커니즘을 지정하려면 aaa-server 호스트 컨피그레이션 모드에서 **sasl-mechanism** 명령을 사용합니다. SASL 인증 메커니즘 옵션은 **digest-md5** 및 **kerberos**입니다.

인증 메커니즘을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

참고 ASA는 VPN 사용자를 위해 LDAP 서버의 클라이언트 프록시 역할을 하므로 여기에서 LDAP 클라이언트는 ASA를 의미합니다.

구문 설명

digest-md5	ASA는 사용자 이름 및 비밀번호에서 계산된 MD5 값으로 응답합니다.
kerberos	ASA는 GSSAPI(Generic Security Services Application Programming Interface) Kerberos 메커니즘을 사용하여 사용자 이름 및 영역을 전송하는 방식으로 응답합니다.
server-group-name	Kerberos aaa-server 그룹(최대 64자)을 지정합니다.

기본값

기본 동작 또는 값은 없습니다. ASA는 인증 파라미터를 일반 텍스트로 LDAP 서버에 전달합니다.

참고 SASL을 구성하지 않은 경우 **ldap-over-ssl** 명령을 사용하여 SSL로 LDAP 통신의 보안을 유지하는 것이 좋습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
aaa-server 호스트 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 SASL 메커니즘을 통해 LDAP 서버에 대한 ASA 인증을 지정할 수 있습니다.

ASA와 LDAP 서버 둘 다 여러 SASL 인증 메커니즘을 지원할 수 있습니다. SASL 인증을 협상할 때 ASA에서는 서버에 구성된 SASL 메커니즘 목록을 검색하여 ASA와 서버 모두에 구성된 가장 강력한 메커니즘으로 인증 메커니즘을 설정합니다. Kerberos 메커니즘이 Digest-MD5 메커니즘보다 강력합니다. 예를 들어 LDAP 서버와 ASA가 두 메커니즘을 모두 지원하는 경우 ASA는 보다 강력한 메커니즘인 Kerberos를 선택합니다.

SASL 메커니즘을 비활성화하려면 비활성화할 각 메커니즘에 대해 별도의 **no** 명령을 입력해야 합니다. 이러한 메커니즘은 독립적으로 구성되기 때문입니다. 특별히 비활성화하지 않은 메커니즘은 계속 적용됩니다. 예를 들어 두 SASL 메커니즘을 모두 비활성화하려면 다음 명령을 둘 다 입력해야 합니다.

no sasl-mechanism digest-md5

no sasl-mechanism kerberos *server-group-name*

예

aaa-server 호스트 컨피그레이션 모드에서 입력된 다음 명령은 IP 주소가 10.10.0.1인 ldapsvr1이라는 LDAP 서버에 대한 SASL 인증 메커니즘을 활성화합니다. 이 예에서는 SASL digest-md5 인증 메커니즘을 활성화합니다.

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism digest-md5
```

다음 예에서는 SASL Kerberos 인증 메커니즘을 활성화하고 kerb-servr1을 Kerberos AAA 서버로 지정합니다.

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

관련 명령

명령	설명
ldap-over-ssl	SSL을 통해 LDAP 클라이언트-서버 연결의 보안을 유지하도록 지정합니다.
server-type	LDAP 서버 공급업체를 Microsoft 또는 Sun으로 지정합니다.
ldap attribute-map(글로벌 컨피그레이션 모드)	사용자 정의 특성 이름을 Cisco LDAP 특성 이름에 매핑하는 LDAP 특성 맵을 만들고 이름을 지정합니다.

sast

CTL 레코드에 만들 SAST 인증서 수를 지정하려면 ctl-file 컨피그레이션 모드에서 **sast** 명령을 사용합니다. CTL 파일의 SAST 인증서 수를 다시 기본값 2로 설정하려면 이 명령의 **no** 형식을 사용합니다.

sast *number_sasts*

no sast *number_sasts*

구문 설명

number_sasts	만들려는 SAST 키 수를 지정합니다. 기본값은 2입니다. 허용되는 최대값은 5입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Ctl-file 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.

사용 지침

CTL 파일은 SAST(System Administrator Security Token)에 의해 서명됩니다.

Phone Proxy는 CTL 파일을 생성하기 때문에 CTL 파일 자체를 서명할 SAST 키를 만들어야 합니다. 이 키는 ASA에서 생성될 수 있습니다. SAST는 자체 서명된 인증서로 만들어집니다.

일반적으로 CTL 파일은 둘 이상의 SAST를 포함합니다. 하나의 SAST를 복구할 수 없는 경우 나중에 다른 SAST를 사용하여 파일을 서명할 수 있습니다.

예

다음 예에서는 **sast** 명령을 사용하여 CTL 파일에서 5개의 SAST 인증서를 만드는 방법을 보여 줍니다.

```
ciscoasa(config-ctl-file)# sast 5
```

관련 명령

명령	설명
ctl-file(전역)	Phone Proxy 컨피그레이션을 위해 만들 CTL 파일 또는 플래시 메모리에서 구문 분석할 CTL 파일을 지정합니다.
ctl-file(phone-proxy)	Phone Proxy 컨피그레이션에 사용할 CTL 파일을 지정합니다.
phone-proxy	Phone Proxy 인스턴스를 구성합니다.

scansafe

상황에 대한 Cloud Web Security 검사를 활성화하려면 상황 컨피그레이션 모드에서 **scansafe** 명령을 사용합니다. Cloud Web Security를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

scansafe [**license** *key*]

no scansafe [**license** *key*]

구문 설명

license *key*	이 상황에 대한 인증 키를 입력합니다. 키를 지정하지 않으면 상황에서 시스템 컨피그레이션에 설정된 라이센스를 사용합니다. ASA에서는 요청을 보낸 조직을 나타내기 위해 Cloud Web Security 프록시 서버로 인증 키를 보냅니다. 인증 키는 16바이트 16진수입니다.

명령 기본값

기본적으로 이 상황에서는 시스템 컨피그레이션에 입력된 라이센스를 사용합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

다중 상황 모드에서는 상황별로 Cloud Web Security를 허용해야 합니다.

예

다음 샘플 컨피그레이션에서는 기본 라이센스가 있는 상황 1과 라이센스 키를 재정의하는 상황 2에서 Cloud Web Security를 활성화합니다.

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
```

```
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

관련 명령

명령	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](파라미터)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스의 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	사용자 또는 그룹이 허용 목록과 일치하는지 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	ASA에서 Cloud Web Security 프록시 서버를 폴링하여 해당 가용성을 확인하기 전에 대기할 시간인 재시도 카운터 값을 입력합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe server	현재 활성 서버인지, 백업 서버인지 또는 연결할 수 없는지와 같은 서버의 상태를 표시합니다.
show scansafe statistics	총 HTTP 연결 수와 현재 HTTP 연결 수를 표시합니다.
user-identity monitor	AD 에이전트에서 지정된 사용자 또는 그룹 정보를 다운로드합니다.
whitelist	트래픽의 클래스에 대해 허용 목록 작업을 수행합니다.

scansafe general-options

Cloud Web Security 프록시 서버와의 통신을 구성하려면 글로벌 컨피그레이션 모드에서 **scansafe general-options** 명령을 사용합니다. 서버 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

scansafe general-options

no scansafe general-options

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

Cloud Web Security의 기본 및 백업 프록시 서버를 구성할 수 있습니다.

예

다음 예에서는 기본 서버를 구성합니다.

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

관련 명령

명령	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](파라미터)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스의 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	사용자 또는 그룹이 허용 목록과 일치하는지 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	ASA에서 Cloud Web Security 프록시 서버를 폴링하여 해당 가용성을 확인하기 전에 대기할 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 상황 모드에서 상황별로 Cloud Web Security를 허용합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe server	현재 활성 서버인지, 백업 서버인지 또는 연결할 수 없는지와 같은 서버의 상태를 표시합니다.
show scansafe statistics	총 HTTP 연결 수와 현재 HTTP 연결 수를 표시합니다.
user-identity monitor	AD 에이전트에서 지정된 사용자 또는 그룹 정보를 다운로드합니다.
whitelist	트래픽의 클래스에 대해 허용 목록 작업을 수행합니다.

scep-enrollment enable

터널 그룹에 대한 Simple Certificate Enrollment Protocol를 활성화하거나 비활성화하려면 tunnel-group general-attributes 모드에서 **scep-enrollment enable** 명령을 사용합니다.

컨피그레이션에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

scep-enrollment enable

no scep-enrollment enable

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 이 명령은 터널 그룹 컨피그레이션에 제공되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

사용 지침

Cisco AnyConnect Secure Mobility Client 릴리스 3.0 이상에서만 이 기능을 지원합니다.

ASA는 AnyConnect와 서드파티 인증 기관 간의 SCEP 요청을 프록시할 수 있습니다. 인증 기관은 ASA가 프록시 역할을 하는 경우에만 ASA에 액세스할 수 있으면 됩니다. ASA에서 이 서비스를 제공하려면 사용자가 ASA에서 등록 요청을 보내기 전에 AAA에서 지원되는 방법 중 하나를 사용하여 인증해야 합니다. Host Scan 및 동적 액세스 정책을 사용하여 등록 자격 규칙을 적용할 수도 있습니다.

ASA에서는 AnyConnect SSL 또는 IKEv2 VPN 세션에서만 이 기능을 지원합니다. IOS CS, Windows Server 2003 CA 및 Windows Server 2008 CA를 비롯한 모든 SCEP 호환 인증 기관을 지원합니다.

클라이언트리스(브라우저 기반) 액세스는 SCEP 프록시를 지원하지 않습니다(단, WebLaunch(클라이언트리스로 시작된 AnyConnect)는 지원함).

ASA에서는 인증서 폴링을 지원하지 않습니다.

ASA에서는 이 기능에 대해 부하 균형을 지원합니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예제에서는 remotegrp라는 원격 액세스 터널 그룹을 만들고 그룹 정책에 SCEP를 사용하도록 설정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this
option.
```

관련 명령

명령	설명
crypto ikev2 enable	IPsec 피어가 통신하는 인터페이스에서 IKEv2 협상을 활성화합니다.
scep-forwarding-url	정책 그룹에 대한 SCEP 인증 기관을 등록합니다.
secondary-pre-fill-username clientless	SCEP 프록시의 WebLaunch 지원을 위해 인증서를 사용할 수 없는 경우 일반적인 보조 비밀번호를 제공합니다.
secondary-authentication-server-group	인증서를 사용할 수 없는 경우 사용자 이름을 제공합니다.

scep-forwarding-url

그룹 정책에 대한 SCEP 인증 기관을 등록하려면 group-policy 컨피그레이션 모드에서 **scep-forwarding-url** 명령을 사용합니다.

컨피그레이션에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

scep-forwarding-url {**none** | **value** [*URL*]}

no scep-forwarding-url

구문 설명

none	그룹 정책에 대한 인증 기관이 없음을 지정합니다.
URL	인증 기관의 SCEP URL을 지정합니다.
value	클라이언트리스 연결에 이 기능을 사용하도록 설정합니다.

기본값

기본적으로 이 명령은 제공되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

사용 지침

서드파티 디지털 인증서를 지원하려면 그룹 정책마다 한 번씩 이 명령을 입력합니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예제에서는 FirstGroup이라는 그룹 정책을 만들고 그룹 정책에 대한 인증 기관을 등록합니다.

```
ciscoasa(config)# group-policy FirstGroup internal
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
Attempting to retrieve the CA/RA certificate(s) using the URL. Please wait ...
```

관련 명령

명령	설명
crypto ikev2 enable	IPsec 피어가 통신하는 인터페이스에서 IKEv2 협상을 활성화합니다.
scep-enrollment enable	터널 그룹에 Simple Certificate Enrollment Protocol을 사용하도록 설정합니다.
secondary-pre-fill-username clientless	SCEP 프록시의 WebLaunch 지원을 위해 인증서를 사용할 수 없는 경우 일반적인 보조 비밀번호를 제공합니다.
secondary-authentication-server-group	인증서를 사용할 수 없는 경우 사용자 이름을 제공합니다.

secondary

대체작동 그룹에서 보조 디바이스에 더 높은 우선순위를 부여하려면 대체작동 그룹 컨피그레이션 모드에서 **secondary** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

secondary

no secondary

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

대체작동 그룹에 대해 **primary** 또는 **secondary**를 지정하지 않으면 대체작동 그룹이 기본적으로 **primary**로 설정됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
대체작동 그룹 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

대체작동 그룹에 기본 또는 보조 우선순위를 지정하면 두 디바이스가 동시에 부팅되는 경우(디바이스 polltime 내) 대체작동 그룹이 활성화되는 디바이스가 지정됩니다. 하나의 디바이스가 다른 디바이스보다 먼저 부팅되는 경우에는 두 대체작동 그룹 모두 해당 디바이스에서 활성화됩니다. 다른 디바이스가 온라인 상태가 되면 두 번째 디바이스를 우선적으로 사용하는 대체작동 그룹이 **preempt** 명령을 사용하여 구성되거나 **no failover active** 명령을 사용하여 다른 디바이스에 수동으로 강제로 적용되지 않는 한 두 번째 디바이스에서 활성화되지 않습니다.

예

다음 예에서는 기본 디바이스를 우선적으로 사용하도록 대체작동 그룹 1을 구성하고, 보조 디바이스를 우선적으로 사용하도록 대체작동 그룹2를 구성합니다. 두 대체작동 그룹 모두 **preempt** 명령을 사용하여 구성되었으므로 디바이스를 사용할 수 있게 되면 각 그룹이 해당 기본 설정 디바이스에서 자동으로 활성화됩니다.

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
failover group	활성/활성 대체작동을 위한 대체작동 그룹을 정의합니다.
preempt	디바이스를 사용할 수 있게 되면 대체작동 그룹을 해당 기본 설정 디바이스에서 강제로 활성화합니다.
primary	기본 디바이스에 보조 디바이스보다 높은 우선순위를 부여합니다.

secondary-authentication-server-group

이중 인증이 활성화된 경우 세션과 연결할 보조 인증 서버 그룹을 지정하려면 tunnel-group general-attributes 모드에서 **secondary-authentication-server-group** 명령을 사용합니다. 컨피그레이션에서 이 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

secondary-authentication-server-group [*interface_name*] {**none** | **LOCAL** | *groupname* [**LOCAL**]} [**use-primary-username**]}

no secondary-authentication-server-group

구문 설명

interface_name	(선택 사항) IPsec 터널이 종료되는 인터페이스를 지정합니다.
LOCAL	(선택 사항) 서버 그룹의 모든 서버가 통신 오류로 인해 비활성화된 경우 로컬 사용자 데이터베이스에 대한 인증을 요구합니다. 서버 그룹 이름이 **LOCAL** 또는 **NONE**인 경우 여기에 **LOCAL** 키워드를 사용하지 마십시오.
none	(선택 사항) 서버 그룹 이름을 **NONE**으로 지정합니다. 이는 인증이 필요하지 않음을 나타냅니다.
groupname [**LOCAL**]	이전에 구성된 인증 서버 또는 서버 그룹을 식별합니다. 선택적으로, 이는 LOCAL 그룹일 수 있습니다.
use-primary-username	기본 사용자 이름을 보조 인증을 위한 사용자 이름으로 사용합니다.

기본값

기본값은 **none**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 이중 인증이 활성화된 경우에만 적용됩니다. **secondary-authentication-server-group** 명령은 보조 AAA 서버 그룹을 지정합니다. 보조 서버 그룹은 SDI 서버 그룹일 수 없습니다.

use-primary-username 키워드가 구성된 경우에는 로그인 대화 상자에서 사용자 이름이 하나만 요청됩니다.

사용자 이름이 디지털 인증서에서 추출된 경우에는 기본 사용자 이름만 인증에 사용됩니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예제에서는 remotegrp라는 원격 액세스 터널 그룹을 만들고, group sdi_server를 기본 서버 그룹으로, group ldap_ server를 연결을 위한 보조 인증 서버 그룹으로 지정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-server-group sdi_server
ciscoasa(config-tunnel-webvpn)# secondary-authentication-server-group ldap_server
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

명령	설명
pre-fill-username	사용자 이름 미리 채우기 기능을 활성화합니다.
show running-config tunnel-group	지정된 tunnel-group 컨피그레이션을 표시합니다.
tunnel-group general-attributes	명명된 tunnel-group의 일반 특성을 지정합니다.
username-from-certificate	인증서에서 권한 부여를 위한 사용자 이름으로 사용할 필드를 지정합니다.

secondary-color

WebVPN 로그인, 홈 페이지 및 파일 액세스 페이지의 보조 색상을 설정하려면 webvpn 컨피그레이션 모드에서 **secondary-color** 명령을 사용합니다. 컨피그레이션에서 색상을 제거하고 기본값을 다시 설정하려면 이 명령의 **no** 형식을 사용합니다.

secondary-color [*color*]

no secondary-color

구문 설명

color	(선택 사항) 색상을 지정합니다. 쉼표로 구분된 RGB 값, HTML 색상 값 또는 색상 이름(HTML에서 인식되는 경우)을 사용할 수 있습니다. • RGB 형식은 0,0,0이며, 각 색상(빨간색, 녹색, 파란색)의 십진수 범위는 0~255입니다. 여기서 쉼표로 구분된 항목은 다른 색상과 조합할 각 색상의 강도를 나타냅니다. • HTML 형식은 16진수 형식의 6자리 숫자인 #000000입니다. 여기서 첫 번째와 두 번째는 빨간색, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파란색을 나타냅니다. • 이름 길이 최대값은 32자입니다.

기본값

기본 보조 색상은 연보라색인 HTML #CCCCFF입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

권장되는 RGB 값 수는 수학적으로 가능한 개수보다 훨씬 적은 216개입니다. 대부분의 디스플레이는 256색만 처리할 수 있으며, 그 중 40개는 MAC과 PC에서 서로 다르게 보입니다. 최상의 결과를 얻으려면 게시된 RGB 표를 확인하십시오. RGB 표를 온라인으로 찾으려면 검색 엔진에서 RGB를 입력합니다.

예

다음 예에서는 청록색인 HTML 색상 값 #5F9EAO를 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-color #5F9EAO
```

관련 명령

명령	설명
title-color	로그인, 홈 페이지 및 파일 액세스 페이지의 WebVPN 제목 표시줄에 대한 색상을 설정합니다.

secondary-pre-fill-username

클라이언트 인증서에서 사용자 이름을 추출하여 클라이언트리스 또는 AnyConnect 연결을 위한 이중 인증에서 사용하도록 설정하려면 tunnel-group webvpn-attributes 모드에서 **secondary-pre-fill-username** 명령을 사용합니다. 컨피그레이션에서 이 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

secondary-pre-fill-username {**clientless** | **ssl-client**} [**hide**]

secondary-pre-fill-username {**clientless** | **ssl-client**} **hide** [**use-primary-password** | **use-common-password** [*type_num*] *password*]

no secondary-no pre-fill-username

구문 설명

clientless	클라이언트리스 연결에 이 기능을 사용하도록 설정합니다.
hide	VPN 사용자에서 인증에 사용할 사용자 이름을 숨깁니다.
password	비밀번호 문자열을 입력합니다.
ssl-client	AnyConnect VPN 클라이언트 연결에 이 기능을 사용하도록 설정합니다.
type_num	다음 옵션 중 하나를 입력합니다. • 입력할 비밀번호가 일반 텍스트인 경우 0 • 입력할 비밀번호가 암호화된 경우 8. 입력할 때 비밀번호는 별표로 표시됩니다.
use-common-password	사용자에게 비밀번호를 묻는 메시지를 표시하지 않고 일반 보조 인증 비밀번호를 사용하도록 지정합니다.
use-primary-password	사용자에게 비밀번호를 묻는 메시지를 표시하지 않고 기본 인증 비밀번호를 보조 인증에 다시 사용합니다.

기본값

이 기능은 기본적으로 비활성화되어 있습니다. **hide** 키워드 없이 이 명령을 입력하면 추출된 사용자 이름이 VPN 사용자에게 노출됩니다. **use-primary-password** 키워드와 **use-common-password** 키워드 중 어떤 것도 지정하지 않으면 사용자에게 비밀번호를 묻는 메시지가 표시됩니다. *type_num*의 기본값은 8입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tunnel-group webvpn-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.
8.3(2)	[**use-primary-password** | **use-common-password** [*type_num*] *password*] 가 명령에 추가되었습니다.

사용 지침

이 기능을 활성화하려면 tunnel-group general-attributes 모드에서 **secondary-username-from-certificate** 명령도 입력해야 합니다.

이 명령은 이중 인증이 활성화된 경우에만 적용됩니다. **secondary-pre-fill-username** 명령은 **secondary-username-from-certificate** 명령에 지정된 인증서 필드에서 추출된 사용자 이름을 보조 사용자 이름/비밀번호 인증을 위한 사용자 이름으로 사용하도록 설정합니다. 이 secondary-pre-fill username-from-certificate 기능을 사용하려면 두 명령을 모두 구성해야 합니다.

참고 클라이언트리스 및 SSL 클라이언트 연결은 상호 배타적인 옵션이 아닙니다. 커맨드 라인당 하나만 지정할 수 있지만 둘 다 동시에 활성화할 수 있습니다.

두 번째 사용자 이름을 숨기고 기본 또는 일반 비밀번호를 사용하는 경우에는 사용자 경험이 단일 인증과 유사합니다. 기본 또는 일반 비밀번호를 사용하면 디바이스 인증서를 사용하여 디바이스를 인증하는 사용자 경험이 원활해집니다.

use-primary-password 키워드는 모든 인증에 기본 비밀번호를 보조 비밀번호로 사용하도록 지정합니다.

use-common-password 키워드는 모든 보조 인증에 일반 보조 비밀번호를 사용하도록 지정합니다. 엔드포인트에 설치된 디바이스 인증서에 BIOS ID 또는 다른 식별자가 포함된 경우 보조 인증 요청에서 미리 채워진 BIOS ID를 두 번째 사용자 이름으로 사용하고, 해당 터널 그룹에서 모든 인증에 구성된 일반 비밀번호를 사용할 수 있습니다.

예

다음 예에서는 remotegrp라는 IPsec 원격 액세스 터널 그룹을 만들고, 연결이 브라우저 기반인 경우 엔드포인트의 디지털 인증서에 있는 이름을 인증 또는 권한 부여 쿼리에 사용할 이름으로 다시 사용하도록 지정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless
```

다음 예는 위 명령과 동일한 기능을 수행하지만 추출된 사용자 이름을 사용자에게 숨깁니다.

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
```

다음 예는 위 명령과 동일한 기능을 수행하지만 AnyConnect 연결에만 적용됩니다.

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
```

다음 예에서는 사용자 이름을 숨기며, 사용자에게 비밀번호를 묻는 메시지를 표시하지 않고 보조 인증에 기본 인증 비밀번호를 다시 사용합니다.

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-primary-password
```

다음 예에서는 사용자 이름을 숨기며, 입력한 비밀번호를 보조 인증에 사용합니다.

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password **********
```

관련 명령

명령	설명
pre-fill-username	사용자 이름 미리 채우기 기능을 활성화합니다.
show running-config tunnel-group	지정된 tunnel-group 컨피그레이션을 표시합니다.
tunnel-group general-attributes	명명된 tunnel-group의 일반 특성을 지정합니다.
username-from-certificate	인증서에서 권한 부여를 위한 사용자 이름으로 사용할 필드를 지정합니다.

secondary-text-color

WebVPN 로그인, 홈 페이지 및 파일 액세스 페이지에 대한 보조 텍스트 색상을 설정하려면 webvpn 모드에서 **secondary-text-color** 명령을 사용합니다. 컨피그레이션에서 색상을 제거하고 기본값을 다시 설정하려면 이 명령의 **no** 형식을 사용합니다.

secondary-text-color [*black* | *white*]

no secondary-text-color

구문 설명

auto	text-color 명령에 대한 설정에 따라 검은색 또는 흰색을 선택합니다. 즉, 기본 색상이 검은색인 경우 이 값은 white입니다.
black	기본 보조 텍스트 색상은 검은색입니다.
white	텍스트 색상을 흰색으로 변경할 수 있습니다.

기본값

기본 보조 텍스트 색상은 검은색입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 보조 텍스트 색상을 흰색으로 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-text-color white
```

관련 명령

명령	설명
text-color	로그인, 홈 페이지 및 파일 액세스 페이지의 WebVPN 제목 표시줄에 표시되는 텍스트의 색상을 설정합니다.

secondary-username-from-certificate

인증서의 필드를 클라이언트리스 또는 AnyConnect(SSL 클라이언트) 연결의 이중 인증을 위한 보조 사용자 이름으로 사용하도록 지정하려면 tunnel-group general-attributes 모드에서 **secondary-username-from-certificate** 명령을 사용합니다.

컨피그레이션에서 이 특성을 제거하고 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

secondary-username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**}

no secondary-username-from-certificate

구문 설명

primary-attr	인증서에서 권한 부여 쿼리를 위한 사용자 이름을 파생시키는 데 사용할 특성을 지정합니다. pre-fill-username이 활성화된 경우 파생된 이름을 인증 쿼리에서도 사용할 수 있습니다.
secondary-attr	(선택 사항) 디지털 인증서에서 인증 또는 권한 부여 쿼리를 위한 사용자 이름을 파생시키는 데 기본 특성과 함께 사용할 추가 특성을 지정합니다. pre-fill-username이 활성화된 경우 파생된 이름을 인증 쿼리에서도 사용할 수 있습니다.
use-entire-name	ASA에서 전체 주체 DN(RFC1779)을 사용하여 디지털 인증서에서 권한 부여 쿼리를 위한 이름을 파생시키도록 지정합니다.
use-script	ASDM에서 생성된 스크립트 이름을 통해 인증서에서 DN 필드를 추출하여 사용자 이름으로 사용하도록 지정합니다.

기본값

이 기능은 기본적으로 비활성화되어 있으며, 이중 인증이 활성화된 경우에만 적용됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 이중 인증이 활성화된 경우에만 적용됩니다.

이중 인증이 활성화된 경우 이 명령은 인증서에서 하나 이상의 필드를 선택하여 사용자 이름으로 사용합니다. **secondary-username-from-certificate** 명령은 보안 어플라이언스에서 지정된 인증서 필드를 두 번째 사용자 이름/비밀번호 인증을 위한 두 번째 사용자 이름으로 사용하도록 강제합니다.

인증서에서 사용자 이름 미리 채우기 기능에서 파생된 이 사용자 이름을 보조 사용자 이름/비밀번호 인증 또는 권한 부여에 사용하려면 tunnel-group webvpn-attributes 모드에서 **pre-fill-username** 및 **secondary-pre-fill-username** 명령도 구성해야 합니다. 즉, 보조 사용자 이름 미리 채우기 기능을 사용하려면 두 명령을 모두 구성해야 합니다.

기본 및 보조 특성에 사용할 수 있는 값은 다음과 같습니다.

특성	정의
C	Country(국가): 2자로 된 국가 약어입니다. 이러한 코드는 ISO 3166 국가 약어를 따릅니다.
CN	Common Name(공통 이름): 사람, 시스템 또는 기타 실체의 이름입니다. 보조 특성으로는 사용할 수 없습니다.
DNQ	Domain Name Qualifier(도메인 이름 한정자)입니다.
EA	E-mail Address(이메일 주소)입니다.
GENQ	Generational Qualifier(세대 한정자)입니다.
GN	Given Name(이름)입니다.
I	Initials(이니셜)입니다.
L	Locality(구/군/시): 조직이 있는 구/군/시입니다.
N	Name(이름)입니다.
O	Organization(조직): 회사, 기관, 에이전시, 협회 또는 기타 실체의 이름입니다.
OU	Organizational Unit(조직 구성 단위): 조직(O) 내의 하위 그룹입니다.
SER	Serial Number(일련 번호)입니다.
SN	Surname(성)입니다.
SP	State/Province(주/도): 조직이 있는 주/도입니다.
T	Title(직함)입니다.
UID	User Identifier(사용자 ID)입니다.
UPN	User Principal Name(사용자 계정 이름)입니다.
use-entire-name	전체 DN 이름을 사용합니다. 보조 특성으로는 사용할 수 없습니다.
use-script	ASDM에서 생성된 스크립트 파일을 사용합니다.

참고 **secondary-username-from-certificate** 명령과 함께 **secondary-authentication-server-group** 명령도 지정한 경우에는 기본 사용자 이름만 인증에 사용됩니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예제에서는 remotegrp라는 원격 액세스 터널 그룹을 만들고, CN(공통 이름)을 기본 특성, OU를 보조 특성으로 사용하여 디지털 인증서에서 권한 부여 쿼리를 위한 이름을 파생시키도록 지정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN
ciscoasa(config-tunnel-general)# secondary-username-from-certificate OU
ciscoasa(config-tunnel-general)#
```

다음 예에서는 tunnel-group 특성을 수정하여 사용자 이름 미리 채우기를 구성하는 방법을 보여 줍니다.

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

관련 명령

명령	설명
pre-fill-username	사용자 이름 미리 채우기 기능을 활성화합니다.
secondary-pre-fill-username	클라이언트리스 또는 AnyConnect 클라이언트 연결에서 사용자 이름 추출을 활성화합니다.
username-from-certificate	인증서에서 권한 부여를 위한 사용자 이름으로 사용할 필드를 지정합니다.
show running-config tunnel-group	지정된 tunnel-group 컨피그레이션을 표시합니다.
secondary-authentication-server-group	보조 AAA 서버 그룹을 지정합니다. 사용자 이름이 디지털 인증서에서 추출된 경우에는 기본 사용자 이름만 인증에 사용됩니다.

secure-unit-authentication

보안 디바이스 인증을 활성화하려면 group-policy 컨피그레이션 모드에서 **secure-unit-authentication enable** 명령을 사용합니다. 보안 디바이스 인증을 비활성화하려면 **secure-unit-authentication disable** 명령을 사용합니다. 실행 중인 컨피그레이션에서 보안 디바이스 인증 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. **secure-unit-authentication** {**enable** | **disable**}

no secure-unit-authentication

구문 설명

disable	보안 디바이스 인증을 비활성화합니다.
enable	보안 디바이스 인증을 활성화합니다.

기본값

보안 디바이스 인증은 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

보안 디바이스 인증을 사용하려면 하드웨어 클라이언트에서 사용하는 터널 그룹에 대해 인증 서버 그룹을 구성해야 합니다.

기본 ASA에서 보안 디바이스 인증이 필요한 경우 모든 백업 서버에서도 이를 구성해야 합니다.

no 옵션은 다른 그룹 정책에서 보안 디바이스 인증 값을 상속하도록 허용합니다.

보안 디바이스 인증은 VPN 하드웨어 클라이언트가 터널을 시작할 때마다 사용자 이름 및 비밀번호로 인증하도록 함으로써 보안을 강화합니다. 이 기능이 활성화되면 하드웨어 클라이언트에 사용자 이름 및 비밀번호가 저장되지 않습니다.

참고 이 기능을 활성화한 경우 VPN 터널을 호출하려면 사용자가 사용자 이름 및 비밀번호를 입력해야 합니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대한 보안 디바이스 인증을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# secure-unit-authentication enable
```

관련 명령

명령	설명
ip-phone-bypass	IP 전화기가 사용자 인증 없이 연결되도록 합니다. 보안 디바이스 인증은 그대로 적용됩니다.
leap-bypass	VPN 하드웨어 클라이언트 뒤에 있는 무선 디바이스의 LEAP 패킷이 사용자 인증(활성화된 경우) 전에 VPN 터널을 통과하도록 합니다. 이를 통해 Cisco 무선 액세스 포인트 디바이스를 사용하는 워크스테이션에서 LEAP 인증을 설정할 수 있습니다. 그런 다음 사용자 인증 시마다 다시 인증합니다.
user-authentication	하드웨어 클라이언트 뒤에 있는 사용자가 연결하기 전에 ASA에 자신을 식별해야 합니다.

security-group

Cisco TrustSec에서 사용할 보안 개체 그룹에 보안 그룹을 추가하려면 object-group 보안 컨피그레이션 모드에서 **security-group** 명령을 사용합니다. 서버 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

security-group {**tag** *sgt#* | **name** *sg_name*}

no security-group {**tag** *sgt#* | **name** *sg_name*}

구문 설명

tag *sgt#*	보안 그룹 개체를 인라인 태그로 지정합니다. 태그 보안 유형의 경우 1에서 65533 사이의 숫자를 입력합니다. SGT는 IEEE 802.1X 인증, 웹 인증 또는 MAB(MAC Authentication Bypass)를 통해 ISE에 의해 디바이스에 할당됩니다. 보안 그룹 이름은 ISE에서 생성되며, 보안 그룹의 이름을 제공합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다.
name *sg_name*	보안 그룹 개체를 명명된 개체로 지정합니다. 이름 보안 유형의 경우 32바이트 문자열(대/소문자 구분)을 입력합니다. *sg_name*은 [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.] 등 모든 문자를 포함할 수 있습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
object-group 보안 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

확장된 ACL에 그룹을 포함하여 Cisco TrustSec을 지원하는 기능에서 사용할 보안 그룹 개체 그룹을 만들 수 있습니다. 그러면 액세스 규칙 등에서 사용할 수 있습니다.

Cisco TrustSec과 통합된 경우 ASA는 ISE에서 보안 그룹 정보를 다운로드합니다. ISE는 Cisco TrustSec 태그를 사용자 ID 매핑에 제공하고 Cisco TrustSec 태그를 서버 리소스 매핑에 제공함으로써 ID 저장소 역할을 합니다. 중앙의 ISE에서 보안 그룹 액세스 목록을 프로비저닝 및 관리할 수 있습니다.

그러나 ASA에 전역적으로 정의되지 않고 현지화된 보안 정책이 적용되는 로컬 보안 그룹이 필요한 현지화된 네트워크 리소스가 있을 수 있습니다. 로컬 보안 그룹은 ISE에서 다운로드한 중첩된 보안 그룹을 포함할 수 있습니다. ASA는 로컬 보안 그룹과 중앙 보안 그룹을 통합합니다.

ASA에서 로컬 보안 그룹을 만들려면 로컬 보안 개체 그룹을 생성합니다. 로컬 보안 개체 그룹은 하나 이상의 중첩된 보안 개체 그룹이나 보안 ID 또는 보안 그룹 이름을 포함할 수 있습니다. 또한 사용자는 ASA에 존재하지 않는 새 보안 ID 또는 보안 그룹 이름을 만들 수 있습니다.

ASA에서 만든 보안 개체 그룹을 사용하여 네트워크 리소스에 대한 액세스를 제어할 수 있습니다. 보안 개체 그룹을 액세스 그룹 또는 서비스 정책의 일부로 사용할 수 있습니다.

예

다음 예에서는 보안 그룹 개체를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# object-group security mktg-sg
ciscoasa(config)# security-group name mktg
ciscoasa(config)# security-group tag 1
```

다음 예에서는 보안 그룹 개체를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# object-group security mktg-sg-all
ciscoasa(config)# security-group name mktg-managers
ciscoasa(config)# group-object mktg-sg // nested object-group
```

관련 명령

명령	설명
object-group security	보안 그룹 개체를 생성합니다.

security-group-tag value

로컬 사용자 데이터베이스와 VPN 세션에 대한 그룹 정책에서 보안 그룹 태그 지정 특성을 구성하려면 group-policy 컨피그레이션 모드에서 **security-group-tag value** 명령을 사용합니다. 서버 그룹 태그 지정 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

security-group-tag value *sgt*

no security-group-tag value *sgt*

구문 설명

sgt	보안 그룹 태그 번호를 지정합니다.

명령 기본값

이 명령의 기본 형식은 **security-group-tag none**입니다. 이는 이 특성 집합에 보안 그룹 태그가 없음을 의미합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(1)	이 명령이 도입되었습니다.

사용 지침

ASA 버전 9.3(1)은 VPN 세션의 보안 그룹 태그 지정을 모두 지원합니다. 외부 AAA 서버를 사용하거나 로컬 사용자 데이터베이스를 구성하여 SGT(보안 그룹 태그)를 VPN 세션에 할당할 수 있습니다. 그런 다음 계층 2 이더넷에서 Cisco TrustSec 시스템을 통해 이 태그를 전파할 수 있습니다. 보안 그룹 태그는 AAA 서버에서 SGT를 제공할 수 없는 경우 그룹 정책 및 로컬 사용자에게 유용합니다.

AAA 서버의 특성에 VPN 사용자에게 할당할 SGT가 없는 경우에는 ASA에서 기본 그룹 정책의 SGT를 사용합니다. 그룹 정책에 SGT가 없으면 0x0 태그가 할당됩니다.

서버에 연결하는 원격 사용자에 대한 일반적인 단계

1. 사용자가 ASA에 연결합니다.
2. ASA가 ISE에서 AAA 정보를 요청합니다. 여기에는 SGT가 포함될 수 있습니다. 또한 ASA에서 사용자의 터널링된 트래픽에 대한 IP 주소를 할당합니다.
3. ASA에서는 AAA 정보를 사용하여 터널을 인증하고 생성합니다.
4. ASA에서는 AAA 정보의 SGT 및 할당된 IP 주소를 사용하여 계층 2 헤더에 SGT를 추가합니다.
5. SGT가 포함된 패킷은 Cisco TrustSec 네트워크의 다음 피어 디바이스로 전달됩니다.

예

다음 예에서는 명명된 그룹 정책 또는 로컬 사용자 이름 특성 집합에 대해 SGT 특성을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config-group-policy)# security-group-tag value 101
```

관련 명령

명령	설명
show asp table cts sgt-map	데이터 경로에 유지되는 IP 주소-보안 그룹 테이블 매핑 데이터베이스에서 IP 주소-보안 그룹 테이블 매핑 항목을 표시합니다.
show cts sgt-map	제어 경로의 IP 주소-보안 그룹 테이블 관리자 항목을 표시합니다.

security-level

인터페이스의 보안 수준을 설정하려면 인터페이스 컨피그레이션 모드에서 **security-level** 명령을 사용합니다. 보안 수준을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다. 보안 수준은 두 보안 네트워크 사이에 추가 보호를 적용하여 하위 보안 네트워크로부터 상위 보안 네트워크를 보호합니다.

security-level *number*

no security-level

구문 설명

number	0(가장 낮음)에서 100(가장 높음) 사이의 정수입니다.

기본값

기본적으로 보안 수준은 0입니다.

인터페이스 이름을 "inside"로 지정한 경우 보안 수준을 명시적으로 설정하지 않으면 ASA에서 보안 수준을 100으로 설정합니다(**nameif** 명령 참고). 원하는 경우 이 수준을 변경할 수 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 **nameif** 명령의 키워드에서 인터페이스 컨피그레이션 모드 명령으로 이동되었습니다.

사용 지침

수준은 다음 동작을 제어합니다.

- 네트워크 액세스 - 기본적으로 상위 보안 인터페이스에서 하위 보안 인터페이스(아웃바운드)로의 액세스는 암시적으로 허용됩니다. 상위 보안 인터페이스의 호스트에서 하위 보안 인터페이스의 모든 호스트에 액세스할 수 있습니다. 인터페이스에 액세스 목록을 적용하여 액세스를 제한할 수 있습니다.

  동일한 보안 인터페이스의 경우 인터페이스에서 보안 수준이 동일하거나 더 낮은 다른 인터페이스에 액세스할 수 있도록 암시적으로 허용됩니다.

- 검사 엔진 - 일부 검사 엔진은 보안 수준에 따라 달라집니다. 동일한 보안 인터페이스의 경우 한쪽 방향의 트래픽에 검사 엔진이 적용됩니다.
  - NetBIOS 검사 엔진 - 아웃바운드 연결에만 적용됩니다.
  - OraServ 검사 엔진 - OraServ 포트에 대한 제어 연결이 호스트 쌍 간에 존재하는 경우 인바운드 데이터 연결만 ASA를 통해 허용됩니다.

- 필터링 - HTTP(S) 및 FTP 필터링은 아웃바운드 연결(상위 수준에서 하위 수준으로)에만 적용됩니다.

  동일한 보안 인터페이스의 경우 한쪽 방향의 트래픽을 필터링할 수 있습니다.

- NAT 제어 - NAT 제어를 활성화한 경우 하위 보안 인터페이스(외부)의 호스트에 액세스할 때 상위 보안 인터페이스(내부)의 호스트에 대해 NAT를 구성해야 합니다.

  NAT 제어를 사용하지 않는 경우 또는 동일한 보안 인터페이스의 경우 원하는 인터페이스 간에 NAT를 사용하도록 선택하거나 NAT를 사용하지 않도록 선택할 수 있습니다. 외부 인터페이스에 대해 NAT를 구성하려면 특수한 키워드가 필요할 수도 있습니다.

- **established** 명령 - 이 명령은 상위 수준 호스트에서 하위 수준 호스트로의 연결이 이미 설정된 경우 하위 보안 호스트에서 상위 보안 호스트로의 반환 연결을 허용합니다.

  동일한 보안 인터페이스의 경우 양방향에 대해 **established** 명령을 구성할 수 있습니다.

일반적으로 동일한 보안 수준의 인터페이스는 통신할 수 없습니다. 동일한 보안 수준의 인터페이스에서 통신하도록 하려면 **same-security-traffic** 명령을 참고하십시오. 101이 넘는 통신 인터페이스를 만들려는 경우 또는 두 인터페이스 간의 트래픽에 보호 기능을 동일하게 적용하려는 경우(예: 보안 수준이 동일한 두 부서가 있는 경우) 두 인터페이스를 동일한 수준에 할당하고 이러한 인터페이스에서 통신하도록 허용할 수 있습니다.

인터페이스의 보안 수준을 변경한 경우 새 보안 정보를 사용하기 전에 기존 연결이 시간 초과될 때까지 기다리지 않으려면 **clear local-host** 명령을 사용하여 연결을 해제하면 됩니다.

예

다음 예에서는 두 인터페이스의 보안 수준을 100과 0으로 구성합니다.

```
ciscoasa(config)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

관련 명령

명령	설명
clear local-host	모든 연결을 재설정합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
nameif	인터페이스 이름을 설정합니다.
vlan	하위 인터페이스에 VLAN ID를 할당합니다.

send response

RADIUS 계정 관리-요청 시작 및 중지 메시지의 보낸 사람에게 RADIUS 계정 관리-응답 시작 및 계정 관리-응답 중지 메시지를 보내려면 radius-accounting 파라미터 컨피그레이션 모드(**inspect radius-accounting** 명령을 사용하여 액세스)에서 **send response** 명령을 사용합니다.

이 옵션은 기본적으로 비활성화되어 있습니다.

send response

no send response

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
radius-accounting 파라미터 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예에서는 RADIUS 계정 관리가 포함된 응답을 보내는 방법을 보여 줍니다.

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# send response
ciscoasa(config-pmap-p)# send response
```

관련 명령

명령	설명
inspect radius-accounting	RADIUS 계정 관리에 대한 검사를 설정합니다.
parameters	검사 정책 맵의 파라미터를 설정합니다.

seq-past-window

past-window 시퀀스 번호(받은 TCP 패킷의 시퀀스 번호가 TCP 수신 창의 오른쪽 경계보다 큰 경우)가 있는 패킷에 대한 작업을 설정하려면 tcp-map 컨피그레이션 모드에서 **seq-past-window** 명령을 사용합니다. 이 값을 다시 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 **set connection advanced-options** 명령을 사용하여 활성화된 TCP 정규화 정책의 일부입니다.

seq-past-window {**allow** | **drop**}

no seq-past-window

구문 설명

allow	past-window 시퀀스 번호가 있는 패킷을 허용합니다. 이 작업은 **queue-limit** 명령이 0(비활성화)으로 설정된 경우에만 허용됩니다.
drop	past-window 시퀀스 번호가 있는 패킷을 삭제합니다.

기본값

기본 작업은 past-window 시퀀스 번호가 있는 패킷을 삭제하는 것입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(4)/8.0(4)	이 명령이 도입되었습니다.

사용 지침

TCP 정규화를 활성화하려면 MPF(Modular Policy Framework)를 사용합니다.

1. **tcp-map** - TCP 정규화 작업을 식별합니다.
   a. **seq-past-window** - tcp-map 컨피그레이션 모드에서 **seq-past-window** 명령 및 다른 여러 명령을 입력할 수 있습니다.
2. **class-map** - TCP 정규화를 수행할 트래픽을 식별합니다.
3. **policy-map** - 각 클래스 맵과 연계된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **set connection advanced-options** - 생성한 tcp-map을 식별합니다.
4. **service-policy** - 하나의 인터페이스 또는 전역적으로 정책 맵을 할당합니다.

예

다음 예에서는 past-window 시퀀스 번호가 있는 패킷을 허용하도록 ASA를 설정합니다.

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# seq-past-window allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

관련 명령

명령	설명
class-map	서비스 정책의 트래픽을 식별합니다.
policy-map	서비스 정책의 트래픽에 적용할 작업을 식별합니다.
queue-limit	비순차적 패킷 제한을 설정합니다.
set connection advanced-options	TCP 정규화를 활성화합니다.
service-policy	인터페이스에 서비스 정책을 적용합니다.
show running-config tcp-map	TCP 맵 컨피그레이션을 표시합니다.
tcp-map	TCP 맵을 만들고 tcp-map 컨피그레이션 모드에 대한 액세스를 허용합니다.

serial-number

등록하는 동안 인증서에 ASA 일련 번호를 포함하려면 crypto ca trustpoint 컨피그레이션 모드에서 **serial-number** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

serial-number

no serial-number

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 설정은 일련 번호를 포함하지 않는 것입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 trustpoint central에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작하고 trustpoint central에 대한 등록 요청에 ASA 일련 번호를 포함합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# serial-number
```

관련 명령

명령	설명
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.

server(pop3s, imap4s, smtps)

기본 이메일 프록시 서버를 지정하려면 적용 가능한 이메일 프록시 컨피그레이션 모드에서 **server** 명령을 사용합니다. 컨피그레이션에서 이 특성을 제거하려면 이 명령의 **no** 버전을 사용합니다. ASA에서는 사용자가 서버를 지정하지 않고 이메일 프록시에 연결하는 경우 기본 이메일 서버로 요청을 보냅니다. 기본 서버를 구성하지 않은 경우 사용자가 서버를 지정하면 ASA에서 오류를 반환합니다.

server {*ipaddr or hostname*}

no server

구문 설명

hostname	기본 이메일 프록시 서버의 DNS 이름입니다.
ipaddr	기본 이메일 프록시 서버의 IP 주소입니다.

기본값

기본적으로 기본 이메일 프록시 서버는 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Pop3s 컨피그레이션	• 예	• 예	—	—	• 예
Imap4s 컨피그레이션	• 예	• 예	—	—	• 예
Smtps 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 IP 주소 10.1.1.7을 사용하여 기본 POP3S 이메일 서버를 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# server 10.1.1.7
```

server(ssh pubkey-chain)

ASA 데이터베이스에서 온보드 SCP(Secure Copy) 클라이언트에 대한 SSH 서버 및 해당 키를 수동으로 추가하거나 삭제하려면 ssh pubkey-chain 컨피그레이션 모드에서 **server** 명령을 사용합니다. 서버와 해당 호스트 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

server *ip_address*

no server *ip_address*

구문 설명

ip_address	SSH 서버 IP 주소를 지정합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
ssh pubkey-chain 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.1(5)	이 명령이 도입되었습니다.

사용 지침

온보드 SCP 클라이언트를 사용하여 ASA와 파일을 서로 복사할 수 있습니다. ASA는 연결한 각 SCP 서버에 대한 SSH 호스트 키를 저장합니다. 원하는 경우 서버와 해당 키를 ASA 데이터베이스에서 수동으로 추가하거나 삭제할 수 있습니다.

각 서버에 대해 SSH 호스트의 **key-string**(공개 키) 또는 **key-hash**(해시 값)를 지정할 수 있습니다.

예

다음 예에서는 10.86.94.170에서 서버의 이미 해시된 호스트 키를 추가합니다.

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

다음 예에서는 10.7.8.9에서 서버의 호스트 문자열을 추가합니다.

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

관련 명령

명령	설명
copy	ASA와 파일을 서로 복사합니다.
key-hash	해시된 SSH 호스트 키를 입력합니다.
key-string	공개 SSH 호스트 키를 입력합니다.
ssh pubkey-chain	서버와 해당 키를 ASA 데이터베이스에서 수동으로 추가하거나 삭제합니다.
ssh stricthostkeycheck	온보드 SCP(Secure Copy) 클라이언트에 대한 SSH 호스트 키 확인을 활성화합니다.

server authenticate-client

TLS 핸드셰이크 중에 ASA에서 TLS 클라이언트를 인증하도록 하려면 tls-proxy 컨피그레이션 모드에서 **server authenticate-client** 명령을 사용합니다.

클라이언트 인증을 우회하려면 이 명령의 **no** 형식을 사용합니다.

server authenticate-client

no server authenticate-client

구문 설명

이 명령에는 인수 또는 키워드가 있습니다.

기본값

이 명령은 기본적으로 활성화되어 있습니다. 즉, ASA와의 핸드셰이크 중에 TLS 클라이언트가 인증서를 제공해야 합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tls-proxy 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.

사용 지침

server authenticate-client 명령을 사용하여 TLS 프록시 핸드셰이크 중에 클라이언트 인증이 필요한지 여부를 제어할 수 있습니다. 활성화된 경우(기본값) 보안 어플라이언스에서 인증서 요청 TLS 핸드셰이크 메시지를 TLS 클라이언트로 보내면 TLS 클라이언트에서 인증서를 제공해야 합니다.

클라이언트 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. TLS 클라이언트 인증을 비활성화하는 것은 ASA가 클라이언트 인증서를 보낼 수 없는 웹 브라우저와 같은 CUMA 클라이언트와 상호 작용해야 하는 경우에 적절합니다.

예

다음 예에서는 클라이언트 인증이 비활성화된 TLS 프록시 인스턴스를 구성합니다.

```
ciscoasa(config)# tls-proxy mmp_tls
ciscoasa(config-tlsp)# no server authenticate-client
ciscoasa(config-tlsp)# server trust-point cuma_server_proxy
```

관련 명령

명령	설명
tls-proxy	TLS 프록시 인스턴스를 구성합니다.

server backup

백업 Cloud Web Security 프록시 서버를 구성하려면 scansafe general-options 컨피그레이션 모드에서 **server backup** 명령을 사용합니다. 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

server backup {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

no server backup [**ip** *ip_address* | **fqdn** *fqdn*] [**port** *port*]

구문 설명

ip *ip_address*	서버 IP 주소를 지정합니다.
fqdn *fqdn*	서버 FQDN(정규화된 도메인 이름)을 지정합니다.
port *port*	(선택 사항) 기본적으로 Cloud Web Security 프록시 서버는 HTTP 및 HTTPS 트래픽 모두에 포트 8080을 사용합니다. 별도의 지시가 없는 한 이 값을 변경하지 마십시오.

명령 기본값

기본 포트는 8080입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
scansafe general-options 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

Cisco Cloud Web Security 서비스를 구독하면 기본 Cloud Web Security 프록시 서버와 백업 프록시 서버가 할당됩니다. 기본 서버를 구성하려면 **server primary** 명령을 참고하십시오. 이러한 서버는 해당 가용성을 확인하기 위해 정기적으로 폴링됩니다. ASA에서 Cloud Web Security 프록시 서버에 연결할 수 없는 경우(예: 프록시 서버에서 수신되는 SYN/ACK 패킷이 없는 경우)에는 해당 가용성을 확인하기 위해 TCP 3방향 핸드셰이크를 통해 프록시 서버가 폴링됩니다. 구성된 재시도 횟수(기본값은 5) 이후에도 프록시 서버를 사용할 수 없는 경우에는 서버가 연결할 수 없는 것으로 선언되며 백업 프록시 서버가 활성화됩니다.

ASA는 연속 폴링에서 두 번의 연속된 재시도 기간 동안 기본 서버가 활성화된 것으로 표시되면 백업 서버에서 기본 Cloud Web Security 프록시 서버로 자동으로 대체됩니다. **retry-count** 명령을 사용하여 이 폴링 간격을 변경할 수 있습니다.

프록시 서버에 연결할 수 없는 트래픽 조건	서버 시간 제한 계산	연결 시간 제한 결과
높은 트래픽	클라이언트 반 열린 연결 시간 제한 + ASA TCP 연결 시간 제한	(30 + 30) = 60초
단일 연결 실패	클라이언트 반 열린 연결 시간 제한 + ((재시도 임계값 - 1) x (ASA TCP 연결 시간 제한))	(30 + ((5-1) x (30)) = 150초
유휴 상태 - 전달되는 연결 없음	15분 + ((재시도 임계값) x (ASA TCP 연결 시간 제한))	900 + (5 x (30)) = 1050초

예

다음 예에서는 기본 및 백업 서버를 구성합니다.

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

관련 명령

명령	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](파라미터)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스의 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	사용자 또는 그룹이 허용 목록과 일치하는지 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	ASA에서 Cloud Web Security 프록시 서버를 폴링하여 해당 가용성을 확인하기 전에 대기할 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 상황 모드에서 상황별로 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe server	현재 활성 서버인지, 백업 서버인지 또는 연결할 수 없는지와 같은 서버의 상태를 표시합니다.
show scansafe statistics	총 HTTP 연결 수와 현재 HTTP 연결 수를 표시합니다.
user-identity monitor	AD 에이전트에서 지정된 사용자 또는 그룹 정보를 다운로드합니다.
whitelist	트래픽의 클래스에 대해 허용 목록 작업을 수행합니다.

server primary

기본 Cloud Web Security 프록시 서버를 구성하려면 scansafe general-options 컨피그레이션 모드에서 **server primary** 명령을 사용합니다. 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

server primary {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

no server primary [**ip** *ip_address* | **fqdn** *fqdn*] [**port** *port*]

구문 설명

ip *ip_address*	서버 IP 주소를 지정합니다.
fqdn *fqdn*	서버 FQDN(정규화된 도메인 이름)을 지정합니다.
port *port*	(선택 사항) 기본적으로 Cloud Web Security 프록시 서버는 HTTP 및 HTTPS 트래픽 모두에 포트 8080을 사용합니다. 별도의 지시가 없는 한 이 값을 변경하지 마십시오.

명령 기본값

기본 포트는 8080입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
scansafe general-options 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

Cisco Cloud Web Security 서비스를 구독하면 기본 Cloud Web Security 프록시 서버와 백업 프록시 서버가 할당됩니다. 백업 서버를 구성하려면 **server backup** 명령을 참고하십시오. 이러한 서버는 해당 가용성을 확인하기 위해 정기적으로 폴링됩니다. ASA에서 Cloud Web Security 프록시 서버에 연결할 수 없는 경우(예: 프록시 서버에서 수신되는 SYN/ACK 패킷이 없는 경우)에는 해당 가용성을 확인하기 위해 TCP 3방향 핸드셰이크를 통해 프록시 서버가 폴링됩니다. 구성된 재시도 횟수(기본값은 5) 이후에도 프록시 서버를 사용할 수 없는 경우에는 서버가 연결할 수 없는 것으로 선언되며 백업 프록시 서버가 활성화됩니다.

ASA는 연속 폴링에서 두 번의 연속된 재시도 기간 동안 기본 서버가 활성화된 것으로 표시되면 백업 서버에서 기본 Cloud Web Security 프록시 서버로 자동으로 대체됩니다. **retry-count** 명령을 사용하여 이 폴링 간격을 변경할 수 있습니다.

프록시 서버에 연결할 수 없는 트래픽 조건	서버 시간 제한 계산	연결 시간 제한 결과
높은 트래픽	클라이언트 반 열린 연결 시간 제한 + ASA TCP 연결 시간 제한	(30 + 30) = 60초
단일 연결 실패	클라이언트 반 열린 연결 시간 제한 + ((재시도 임계값 - 1) x (ASA TCP 연결 시간 제한))	(30 + ((5-1) x (30)) = 150초
유휴 상태 - 전달되는 연결 없음	15분 + ((재시도 임계값) x (ASA TCP 연결 시간 제한))	900 + (5 x (30)) = 1050초

예

다음 예에서는 기본 및 백업 서버를 구성합니다.

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

관련 명령

명령	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](파라미터)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스의 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	사용자 또는 그룹이 허용 목록과 일치하는지 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	ASA에서 Cloud Web Security 프록시 서버를 폴링하여 해당 가용성을 확인하기 전에 대기할 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 상황 모드에서 상황별로 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe server	현재 활성 서버인지, 백업 서버인지 또는 연결할 수 없는지와 같은 서버의 상태를 표시합니다.
show scansafe statistics	총 HTTP(S) 연결 수와 현재 HTTP(S) 연결 수를 표시합니다.
user-identity monitor	AD 에이전트에서 지정된 사용자 또는 그룹 정보를 다운로드합니다.
whitelist	트래픽의 클래스에 대해 허용 목록 작업을 수행합니다.

server trust-point

TLS 핸드셰이크 중에 제공할 프록시 신뢰 지점 인증서를 지정하려면 TLS 서버 컨피그레이션 모드에서 **server trust-point** 명령을 사용합니다.

server trust-point *proxy_trustpoint*

구문 설명

proxy_trustpoint	**crypto ca trustpoint** 명령으로 정의된 신뢰 지점을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
TLS-proxy 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.

사용 지침

신뢰 지점은 자체 서명되거나, 인증 기관에 등록되거나, 가져온 자격 증명일 수 있습니다. **server trust-point** 명령은 전역 **ssl trust-point** 명령에 우선합니다.

server trust-point 명령은 TLS 핸드셰이크 중에 제공되는 프록시 신뢰 지점 인증서를 지정합니다. ASA에서 인증서를 소유해야 합니다(ID 인증서). 인증서는 자체 서명되거나, 인증 기관에 등록되거나, 가져온 자격 증명일 수 있습니다.

연결을 시작할 수 있는 각 엔터티에 대해 TLS 프록시 인스턴스를 생성합니다. TLS 연결을 시작하는 엔티티는 TLS 클라이언트의 역할을 합니다. TLS 프록시에는 클라이언트 프록시 및 서버 프록시가 엄격히 정의되므로 두 엔터티 중 하나에서 연결을 시작할 수 있는 경우 두 TLS 프록시 인스턴스를 모두 정의해야 합니다.

참고 Phone Proxy와 함께 사용할 TLS 프록시 인스턴스를 만드는 경우 서버 신뢰 지점은 내부 Phone Proxy 신뢰 지점에서 만든 CTL 파일 인스턴스입니다. 신뢰 지점은 *internal_PP_<ctl-file_instance_name>* 형식입니다.

예

다음 예에서는 **server trust-point** 명령을 사용하여 TLS 핸드셰이크 중에 제공할 프록시 신뢰 지점 인증서를 지정하는 방법을 보여 줍니다.

```
ciscoasa(config-tlsp)# server trust-point ent_y_proxy
```

관련 명령

명령	설명
client(tls-proxy)	TLS 프록시 인스턴스에 대한 신뢰 지점, 키 쌍 및 암호 그룹을 구성합니다.
client trust-point	TLS 핸드셰이크 중에 제공할 프록시 신뢰 지점 인증서를 지정합니다.
ssl trust-point	인터페이스에 대한 SSL 인증서를 나타내는 인증서 신뢰 지점을 지정합니다.
tls-proxy	TLS 프록시 인스턴스를 구성합니다.

server-port

호스트의 AAA 서버 포트를 구성하려면 aaa-server 호스트 모드에서 **server-port** 명령을 사용합니다. 지정된 서버 포트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

server-port *port-number*

no server-port *port-number*

구문 설명

port-number	0~65535 범위의 포트 번호입니다.

기본값

기본 서버 포트는 다음과 같습니다.

- SDI-5500
- LDAP-389
- Kerberos-88
- NT-139
- TACACS+-49

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
aaa-server 그룹	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 서버 포트 번호 8888을 사용하도록 srvgrp1이라는 SDI AAA 서버를 구성합니다.

```
ciscoasa(config)# aaa-server srvgrp1 protocol sdi
ciscoasa(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
ciscoasa(config-aaa-server-host)# server-port 8888
```

관련 명령

명령	설명
aaa-server host	호스트별 AAA 서버 파라미터를 구성합니다.
clear configure aaa-server	모든 AAA 서버 컨피그레이션을 제거합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내의 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

server-separator

이메일 및 VPN 서버 이름 사이의 구분 기호 문자를 지정하려면 적용 가능한 이메일 프록시 모드에서 **server-separator** 명령을 사용합니다. 기본값인 ":"으로 되돌리려면 이 명령의 no 형식을 사용합니다.

server-separator {*symbol*}

no server-separator

구문 설명

symbol	이메일 및 VPN 서버 이름을 구분하는 문자입니다. "@"(앳), "l"(파이프), ":"(콜론), "#"(해시), ","(쉼표) 또는 ";"(세미콜론)을 선택할 수 있습니다.

기본값

기본값은 "@"(앳)입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Pop3s	• 예	—	• 예	—	—
Imap4s	• 예	—	• 예	—	—
Smtps	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

서버 구분 기호는 이름 구분 기호와 달라야 합니다.

예

다음 예에서는 파이프(l)를 IMAP4S의 서버 구분 기호로 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# server-separator |
```

관련 명령

명령	설명
name-separator	이메일과 VPN 사용자 이름 및 비밀번호를 구분합니다.

server-type

LDAP 서버 모델을 수동으로 구성하려면 aaa-server host 컨피그레이션 모드에서 **server-type** 명령을 사용합니다. ASA에서 지원하는 서버 모델은 다음과 같습니다.

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server(이전의 Sun ONE Directory Server)
- LDAPv3을 준수하는 일반 LDAP 디렉토리 서버(비밀번호 관리 없음)

이 명령을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

no server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

구문 설명

auto-detect	ASA에서 자동 감지를 통해 LDAP 서버 유형을 확인하도록 지정합니다.
generic	Sun 및 Microsoft LDAP 디렉토리 서버가 아닌 다른 LDAP v3 호환 디렉토리 서버를 지정합니다. 비밀번호 관리는 일반 LDAP 서버에서 지원되지 않습니다.
microsoft	LDAP 서버를 Microsoft Active Directory로 지정합니다.
openldap	LDAP 서버를 OpenLDAP 서버로 지정합니다.
novell	LDAP 서버를 Novell 서버로 지정합니다.
sun	LDAP 서버를 Sun Microsystems JAVA System Directory Server로 지정합니다.

기본값

기본적으로 자동 감지를 통해 서버 유형이 확인됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Aaa-server 호스트 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.
8.0(2)	OpenLDAP 및 Novell 서버 유형에 대한 지원이 추가되었습니다.

사용 지침

ASA는 LDAP 버전 3을 지원하며, Sun Microsystems JAVA System Directory Server, Microsoft Active Directory 및 기타 LDAPv3 디렉토리 서버와 호환됩니다.

참고

- Sun - Sun 디렉토리 서버에 액세스하려면 ASA에 구성된 DN이 이 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 디렉토리 관리자 권한이 있는 사용자를 DN으로 사용할 것을 권장합니다. 또는 기본 비밀번호 정책에 ACI를 배치할 수 있습니다.
- Microsoft - Microsoft Active Directory에서 비밀번호 관리를 활성화하려면 SSL을 통해 LDAP를 구성해야 합니다.
- 일반 - 비밀번호 관리 기능이 지원되지 않습니다.

기본적으로 ASA에서는 Microsoft 디렉토리 서버, Sun LDAP 디렉토리 서버 또는 일반 LDAPv3 서버에 연결되었는지 자동으로 감지합니다. 그러나 자동 감지 기능이 LDAP 서버 유형을 확인하지 못한 경우 서버가 Microsoft 서버인지 또는 Sun 서버인지 알고 있다면 **server-type** 명령을 사용하여 서버를 Microsoft 또는 Sun Microsystems LDAP 서버로 수동으로 구성할 수 있습니다.

예

aaa-server host 컨피그레이션 모드에서 입력된 다음 예에서는 IP 주소 10.10.0.1에서 LDAP 서버 ldapsvr1의 서버 유형을 구성합니다. 첫 번째 예에서는 Sun Microsystems LDAP 서버를 구성합니다.

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type sun
```

다음 예에서는 ASA에서 자동 감지를 사용하여 서버 유형을 확인하도록 지정합니다.

```
ciscoasa(config)# aaa-server ldapsvr1 protocol LDAP
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type auto-detect
```

관련 명령

명령	설명
ldap-over-ssl	SSL을 통해 LDAP 클라이언트-서버 연결의 보안을 유지하도록 지정합니다.
sasl-mechanism	LDAP 클라이언트와 서버 간에 SASL 인증을 구성합니다.
ldap attribute-map(글로벌 컨피그레이션 모드)	사용자 정의 특성 이름을 Cisco LDAP 특성 이름에 매핑하는 LDAP 특성 맵을 만들고 이름을 지정합니다.

service

거부된 TCP 연결에 대한 재설정을 활성화하려면 글로벌 컨피그레이션 모드에서 **service** 명령을 사용합니다. 재설정을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

service sw-reset-button

no service sw-reset-button

구문 설명

interface *interface_name*	지정된 인터페이스에 대한 재설정을 활성화하거나 비활성화합니다.
resetinbound	ASA를 통과하려고 시도했지만 액세스 목록 또는 AAA 설정에 따라 ASA에서 거부된 모든 인바운드 TCP 세션에 대한 TCP 재설정을 보냅니다. 또한 ASA에서는 액세스 목록 또는 AAA에서 허용되지만 기존 연결에 속하지 않아 상태 저장 방화벽에서 거부된 패킷에 대한 재설정도 보냅니다. 동일한 보안 수준 인터페이스 간의 트래픽도 영향을 받습니다. 이 옵션이 활성화되어 있지 않으면 ASA에서 거부된 패킷을 자동으로 취소합니다. 인터페이스를 지정하지 않은 경우 이 설정은 모든 인터페이스에 적용됩니다.
resetoutbound	ASA를 통과하려고 시도했지만 액세스 목록 또는 AAA 설정에 따라 ASA에서 거부된 모든 아웃바운드 TCP 세션에 대한 TCP 재설정을 보냅니다. 또한 ASA에서는 액세스 목록 또는 AAA에서 허용되지만 기존 연결에 속하지 않아 상태 저장 방화벽에서 거부된 패킷에 대한 재설정도 보냅니다. 동일한 보안 수준 인터페이스 간의 트래픽도 영향을 받습니다. 이 옵션이 활성화되어 있지 않으면 ASA에서 거부된 패킷을 자동으로 취소합니다. 이 옵션은 기본적으로 활성화되어 있습니다. 예를 들어 트래픽이 급증하는 동안 CPU 부하를 줄이기 위해 아웃바운드 재설정을 비활성화할 수도 있습니다.
resetoutside	최소 보안 인터페이스에서 종료되고 액세스 목록 또는 AAA 설정에 따라 ASA에서 거부된 TCP 패킷에 대한 재설정을 활성화합니다. 또한 ASA에서는 액세스 목록 또는 AAA에서 허용되지만 기존 연결에 속하지 않아 상태 저장 방화벽에서 거부된 패킷에 대한 재설정도 보냅니다. 이 옵션이 활성화되어 있지 않으면 ASA에서 거부된 패킷을 자동으로 취소합니다. 인터페이스 PAT와 함께 **resetoutside** 키워드를 사용하는 것이 좋습니다. 이 키워드는 ASA가 외부 SMTP 또는 FTP 서버의 IDENT를 종료하도록 허용합니다. 이러한 연결을 능동적으로 재설정하면 30초 시간 제한 지연이 방지됩니다.
sw-reset-button	소프트웨어 재설정 버튼을 구성합니다.

기본값

기본적으로 **service resetoutbound**는 모든 인터페이스에 대해 활성화됩니다. 기본적으로 **service sw-reset-button**은 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.1(1)	**interface** 키워드 및 **resetoutbound** 명령이 추가되었습니다.

사용 지침

ID 요청(IDENT) 연결을 재설정해야 하는 경우 인바운드 트래픽에 대한 재설정을 명시적으로 보낼 수 있습니다. 거부된 호스트에 TCP RST(TCP 헤더의 재설정 플래그)를 보내면 IDENT가 시간 초과될 때까지 기다릴 필요가 없도록 RST에서 들어오는 IDENT 프로세스를 중지합니다. IDENT가 시간 초과될 때까지 기다리면 외부 호스트에서 IDENT가 시간 초과될 때까지 SYN을 계속 재전송하기 때문에 트래픽이 느려질 수 있으므로 **service resetinbound** 명령을 사용하면 성능이 향상될 수 있습니다.

예

다음 예에서는 내부 인터페이스를 제외하고 모든 인터페이스에 대한 아웃바운드 재설정을 비활성화합니다.

```
ciscoasa(config)# no service resetoutbound
ciscoasa(config)# service resetoutbound interface inside
```

다음 예에서는 DMZ 인터페이스를 제외하고 모든 인터페이스에 대한 아웃바운드 재설정을 비활성화합니다.

```
ciscoasa(config)# service resetinbound
ciscoasa(config)# no service resetinbound interface dmz
```

다음 예에서는 외부 인터페이스를 종료하는 연결에 대한 재설정을 활성화합니다.

```
ciscoasa(config)# service resetoutside
```

관련 명령

명령	설명
show running-config service	서비스 컨피그레이션을 표시합니다.

service(ctl-provider)

인증서 신뢰 목록 공급자가 수신 대기하는 포트를 지정하려면 CTL 공급자 컨피그레이션 모드에서 **service** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

service port *listening_port*

no service port *listening_port*

구문 설명

port *listening_port*	클라이언트로 내보낼 인증서를 지정합니다.

기본값

기본 포트는 2444입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CTL 공급자 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

CTL 공급자 컨피그레이션 모드에서 **service** 명령을 사용하여 CTL 공급자가 수신 대기할 포트를 지정할 수 있습니다. 이 포트는 클러스터의 CallManager 서버에서 수신 대기하는 포트여야 합니다(CallManager 관리 페이지의 엔터프라이즈 파라미터 아래에 구성). 기본 포트는 2444입니다.

예

다음 예에서는 CTL 공급자 인스턴스를 만드는 방법을 보여 줍니다.

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

관련 명령

명령	설명
client	CTL 공급자에 연결할 수 있는 클라이언트와 클라이언트 인증에 사용할 사용자 이름 및 비밀번호를 지정합니다.
ctl	CTL 클라이언트에서 CTL 파일을 구문 분석하고 신뢰 지점을 설치합니다.
ctl-provider	CTL 공급자 모드에서 CTL 공급자 인스턴스를 구성합니다.
export	클라이언트로 내보낼 인증서를 지정합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

service(object service)

서비스 개체의 프로토콜 및 선택적 특성을 정의하려면 개체 서비스 컨피그레이션 모드에서 **service** 명령을 사용합니다. 이 정의를 제거하려면 이 명령의 **no** 형식을 사용합니다.

service {*protocol* | {**tcp** | **udp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

no service {*protocol* | {**tcp** | **udp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

구문 설명

destination *operator number*	(선택 사항) **tcp** 및 **udp** 프로토콜의 경우 대상 포트 이름 또는 번호(0~65535)를 지정합니다. 지원되는 이름 목록은 CLI 도움말을 참고하십시오. 연산자는 다음과 같습니다. • **eq** - 포트 번호와 같음 • **gt** - 포트 번호보다 큼 • **lt** - 포트 번호보다 작음 • **neq** - 포트 번호와 같지 않음 • **range** - 포트 범위. 공백으로 구분된 두 숫자를 지정합니다(예: **range 1024 4500**).
{**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]	서비스 유형이 ICMP 또는 ICMP 버전 6 연결에 해당되도록 지정합니다. 선택적으로 이름 또는 번호(0~255)로 ICMP 유형을 지정할 수 있습니다. 사용 가능한 선택적 ICMP 유형 이름은 CLI 도움말을 참고하십시오. 유형을 지정한 경우 선택적으로 ICMP 코드(1~255)를 포함할 수 있습니다.
protocol	프로토콜 이름 또는 번호(0~255)를 식별합니다. 지원되는 이름 목록은 CLI 도움말을 참고하십시오.
source *operator number*	(선택 사항) **tcp** 및 **udp** 프로토콜의 경우 소스 포트 이름 또는 번호(0~65535)를 지정합니다. 지원되는 이름 목록은 CLI 도움말을 참고하십시오. 연산자는 **destination**의 연산자와 같습니다.
tcp	서비스 유형이 TCP 연결에 해당되도록 지정합니다.
udp	서비스 유형이 UDP 연결에 해당되도록 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
개체 서비스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.
9.0(1)	ICMP 코드에 대한 지원이 추가되었습니다.

사용 지침

ACL(**access-list** 명령) 및 NAT(**nat** 명령)와 같은 컨피그레이션의 다른 부분에서 이름으로 서비스 개체를 사용할 수 있습니다.

기존 서비스 개체를 다른 프로토콜 및 포트로 구성한 경우에는 새 컨피그레이션이 기존 프로토콜 및 포트를 새 프로토콜 및 포트로 대체합니다.

예

다음 예에서는 SSH 트래픽에 대한 서비스 개체를 만드는 방법을 보여 줍니다.

```
ciscoasa(config)# service object SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
```

다음 예에서는 EIGRP 트래픽에 대한 서비스 개체를 만드는 방법을 보여 줍니다.

```
ciscoasa(config)# service object EIGRP
ciscoasa(config-service-object)# service eigrp
```

다음 예에서는 포트 0~1024에서 HTTPS로 들어오는 트래픽에 대한 서비스 개체를 만드는 방법을 보여 줍니다.

```
ciscoasa(config)# service object HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
```

관련 명령

명령	설명
clear configure object	생성된 모든 개체를 지웁니다.
object-group service	서비스 개체를 구성합니다.
show running-config object service	현재 서비스 개체 컨피그레이션을 표시합니다.

service call-home

Call Home 서비스를 활성화하려면 글로벌 컨피그레이션 모드에서 **service call-home** 명령을 사용합니다. Call Home 서비스를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

service call-home

no service call-home

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 서비스 Call Home 명령은 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.2(2)	이 명령이 도입되었습니다.

예

다음 예에서는 Call Home 서비스를 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# service call-home
```

다음 예에서는 Call Home 서비스를 비활성화하는 방법을 보여 줍니다.

```
hostname(config)# no service call-home
```

관련 명령

명령	설명
call-home(글로벌 컨피그레이션)	Call Home 컨피그레이션 모드를 시작합니다.
call-home test	Call Home 테스트 메시지를 수동으로 보냅니다.
show call-home	Call Home 컨피그레이션 정보를 표시합니다.

service password-recovery

비밀번호 복구를 활성화하려면 글로벌 컨피그레이션 모드에서 **service password-recovery** 명령을 사용합니다. 비밀번호 복구를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 비밀번호 복구는 기본적으로 활성화되어 있지만 권한 없는 사용자가 비밀번호 복구 메커니즘을 사용하여 ASA를 손상시킬 수 없도록 하기 위해 비활성화할 수 있습니다.

service password-recovery

no service password-recovery

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

비밀번호 복구는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

ASA 5500 Series Adaptive Security Appliance에서는 비밀번호를 잊어버린 경우 시작하는 동안 프롬프트가 표시될 때 터미널 키보드에서 **Esc** 키를 눌러 ASA를 ROMMON으로 부팅할 수 있습니다. 그런 다음 컨피그레이션 레지스터를 변경하여 시작 컨피그레이션을 무시하도록 ASA를 설정합니다(**config-register** 명령 참고). 예를 들어 컨피그레이션 레지스터가 기본값인 0x1인 경우 **confreg 0x41** 명령을 입력하여 값을 0x41로 변경합니다. ASA를 다시 로드하면 기본 컨피그레이션이 로드되며, 기본 비밀번호를 사용하여 특권 EXEC 모드를 시작할 수 있습니다. 그런 다음 시작 컨피그레이션을 실행 중인 컨피그레이션에 복사하여 로드하고 비밀번호를 재설정합니다. 마지막으로 컨피그레이션 레지스터를 원래 설정으로 지정하여 이전처럼 부팅하도록 ASA를 설정합니다. 예를 들어 글로벌 컨피그레이션 모드에서 **config-register 0x1** 명령을 입력합니다.

PIX 500 Series 보안 어플라이언스의 경우 시작하는 동안 프롬프트가 표시될 때 터미널 키보드에서 **Esc** 키를 눌러 ASA를 모니터 모드로 부팅합니다. 그런 다음 PIX 비밀번호 툴을 ASA에 다운로드합니다. 그러면 모든 비밀번호와 **aaa authentication** 명령이 지워집니다.

ASA 5500 Series Adaptive Security Appliance에서 **no service password-recovery** 명령은 사용자가 컨피그레이션을 그대로 유지한 채 ROMMON을 시작하지 못하도록 합니다. 사용자가 ROMMON을 시작하면 ASA에서 모든 플래시 파일 시스템을 지우라는 프롬프트를 표시합니다. 사용자는 이 지우기를 먼저 수행해야 ROMMON을 시작할 수 있습니다. 사용자가 플래시 파일 시스템을 지우지 않도록 선택한 경우에는 ASA가 다시 로드됩니다. 비밀번호 복구는 ROMMON 사용 및 기존 컨피그레이션 유지에 따라 결정되므로 이 지우기는 비밀번호를 복구하지 못하도록 합니다. 그러나 비

밀번호 복구를 비활성화하면 권한 없는 사용자가 컨피그레이션을 보거나 다른 비밀번호를 삽입하지 못하게 됩니다. 이 경우 시스템을 작동 상태로 복구하려면 새 이미지 및 백업 컨피그레이션 파일(사용 가능한 경우)을 로드합니다. **service password-recovery** 명령은 정보 제공을 위한 목적으로만 컨피그레이션 파일에 표시되며, CLI 프롬프트에 명령을 입력하면 설정이 NVRAM에 저장됩니다. 설정을 변경하는 방법은 CLI 프롬프트에 명령을 입력하는 방법밖에 없습니다. 다른 버전의 명령을 사용하여 새 컨피그레이션을 로드하면 설정이 변경되지 않습니다. ASA가 시작(비밀번호 복구 준비) 시 시작 컨피그레이션을 무시하도록 구성된 경우 비밀번호 복구를 비활성화하면 ASA가 시작 컨피그레이션을 평소대로 부팅하도록 설정을 변경합니다. 대체작동을 사용하고 대기 디바이스가 시작 컨피그레이션을 무시하도록 구성된 경우 **no service password recovery** 명령이 대기 디바이스에 복제되면 동일한 변경 사항이 컨피그레이션 레지스터에 적용됩니다.

PIX 500 Series 보안 어플라이언스에서 **no service password-recovery** 명령은 PIX 비밀번호 툴이 사용자에게 모든 플래시 파일 시스템을 삭제하라는 프롬프트를 강제로 표시하도록 합니다. 사용자는 이 지우기를 먼저 수행해야 PIX 비밀번호 툴을 사용할 수 있습니다. 사용자가 플래시 파일 시스템을 지우지 않도록 선택한 경우에는 ASA가 다시 로드됩니다. 비밀번호 복구는 기존 컨피그레이션 유지에 따라 결정되므로 이 지우기는 비밀번호를 복구하지 못하도록 합니다. 그러나 비밀번호 복구를 비활성화하면 권한 없는 사용자가 컨피그레이션을 보거나 다른 비밀번호를 삽입하지 못하게 됩니다. 이 경우 시스템을 작동 상태로 복구하려면 새 이미지 및 백업 컨피그레이션 파일(사용 가능한 경우)을 로드합니다.

예

다음 예에서는 ASA 5500 Series에 대한 비밀번호 복구를 비활성화합니다.

```
ciscoasa(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.  The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images.  You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

ASA 5500 Series에 대한 다음 예에서는 시작 시 ROMMON을 시작하는 경우와 비밀번호 복구 작업을 완료하는 방법을 보여 줍니다.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
```

```
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# configure terminal
ciscoasa(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
ciscoasa(config)# enable password NewPassword
ciscoasa(config)# config-register 0x1
```

관련 명령

명령	설명
config-register	다시 로드할 때 시작 컨피그레이션을 무시하도록 ASA를 설정합니다.
enable password	enable 비밀번호를 설정합니다.
password	로그인 비밀번호를 설정합니다.

service-object

서비스 또는 서비스 개체를 TCP, UDP 또는 TCP-UDP로 미리 정의되지 않은 서비스 개체 그룹에 추가하려면 object-group service 컨피그레이션 모드에서 **service-object** 명령을 사용합니다. 서비스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

service-object {*protocol* | {**tcp** | **udp** | **tcp-udp**} [**source** *operator number*]
[**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

no service-object {*protocol* | {**tcp** | **udp** | **tcp-udp**} [**source** *operator number*]
[**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

구문 설명

destination *operator number*	(선택 사항) **tcp**, **udp** 또는 **tcp-udp** 프로토콜의 경우 대상 포트 이름 또는 번호(0~65535)를 지정합니다. 지원되는 이름 목록은 CLI 도움말을 참고하십시오. 연산자는 다음과 같습니다. • **eq** - 포트 번호와 같음 • **gt** - 포트 번호보다 큼 • **lt** - 포트 번호보다 작음 • **neq** - 포트 번호와 같지 않음 • **range** - 포트 범위. 공백으로 구분된 두 숫자를 지정합니다(예: **range 1024 4500**).
{**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]	서비스 유형이 ICMP 또는 ICMP 버전 6 연결에 해당되도록 지정합니다. 선택적으로 이름 또는 번호(0~255)로 ICMP 유형을 지정할 수 있습니다. 사용 가능한 선택적 ICMP 유형 이름은 CLI 도움말을 참고하십시오. 유형을 지정한 경우 선택적으로 ICMP 코드(1~255)를 포함할 수 있습니다.
protocol	프로토콜 이름 또는 번호(0~255)를 식별합니다. 지원되는 이름 목록은 CLI 도움말을 참고하십시오.
source *operator number*	(선택 사항) **tcp**, **udp** 또는 **tcp-udp** 프로토콜의 경우 소스 포트 이름 또는 번호(0~65535)를 지정합니다. 지원되는 이름 목록은 CLI 도움말을 참고하십시오. 연산자는 **destination**의 연산자와 같습니다.
tcp	서비스 유형이 TCP 연결에 해당되도록 지정합니다.
tcp-udp	서비스 유형이 TCP 또는 UDP 연결에 해당되도록 지정합니다.
udp	서비스 유형이 UDP 연결에 해당되도록 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
object-group service 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(1)	이 명령이 도입되었습니다.
8.3(1)	**object** 키워드가 서비스 개체(**object service** 명령)를 지원하기 위해 추가되었습니다.
9.0(1)	ICMP 코드에 대한 지원이 추가되었습니다.

사용 지침

object-group service 명령을 사용하여 서비스 개체 그룹을 만들 때 전체 그룹에 대한 프로토콜 유형을 미리 정의하지 않은 경우 **service-object** 명령을 사용하여 포트를 비롯한 여러 서비스 및 서비스 개체를 여러 프로토콜 그룹에 추가할 수 있습니다. **object-group service [tcp | udp | tcp-udp]** 명령을 사용하여 특정 프로토콜 유형의 서비스 개체 그룹을 만든 경우 **port-object** 명령을 사용하여 개체 그룹의 대상 포트를 식별할 수만 있습니다.

예

다음 예에서는 서비스 개체 그룹에 TCP 서비스와 UDP 서비스를 모두 추가하는 방법을 보여 줍니다.

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

다음 예에서는 서비스 개체 그룹에 여러 서비스 개체를 추가하는 방법을 보여 줍니다.

```
hostname(config)# service object SSH
hostname(config-service-object)# service tcp destination eq ssh

hostname(config)# service object EIGRP
hostname(config-service-object)# service eigrp

hostname(config)# service object HTTPS
hostname(config-service-object)# service tcp source range 0 1024 destination eq https

ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

관련 명령

명령	설명
clear configure object-group	모든 **object-group** 명령을 컨피그레이션에서 제거합니다.
network-object	네트워크 개체 그룹에 네트워크 개체를 추가합니다.
object service	서비스 개체를 추가합니다.
object-group	컨피그레이션을 최적화할 개체 그룹을 정의합니다.
port-object	서비스 개체 그룹에 포트 개체를 추가합니다.
show running-config object-group	현재 개체 그룹을 표시합니다.

service sw-reset-button

ASA 5506-X 및 ASA 5508-X Series 보안 어플라이언스에서 재설정 버튼을 활성화하려면 글로벌 컨피그레이션 모드에서 **service sw-reset-button** 명령을 사용합니다. 재설정 버튼을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

service sw-reset-button

no service sw-reset-button

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 **service sw-reset-button**은 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 추가되었습니다.

예

다음 예에서는 소프트웨어 재설정 버튼을 활성화합니다.

```
ciscoasa(config)# service sw-reset-button
ciscoasa# show sw-reset-button

Software Reset Button is configured.
```

다음 예에서는 소프트웨어 재설정 버튼을 비활성화합니다.

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is not configured.
```

관련 명령

명령	설명
show running-config service	서비스 컨피그레이션을 표시합니다.

service-policy(class)

다른 정책 맵 아래의 계층적 정책 맵을 적용하려면 클래스 컨피그레이션 모드에서 **service-policy** 명령을 사용합니다. 서비스 정책을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 계층적 정책은 셰이핑된 트래픽의 하위 집합에서 우선순위 대기열 처리를 수행하려는 경우 QoS 트래픽 셰이핑에만 지원됩니다.

service-policy *policymap_name*

no service-policy *policymap_name*

구문 설명

policymap_name	**policy-map** 명령에서 구성한 정책 맵 이름을 지정합니다. **priority** 명령에 포함된 계층 3/4 정책 맵만 지정할 수 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(4)/8.0(4)	이 명령이 도입되었습니다.

사용 지침

계층적 우선순위 대기열 처리는 트래픽 셰이핑 대기열을 활성화한 인터페이스에서 사용됩니다. 셰이핑된 트래픽의 하위 집합에 대한 우선순위를 지정할 수 있습니다. 표준 우선순위 대기열은 사용되지 않습니다(**priority-queue** 명령).

계층적 우선순위 대기열 처리의 경우 MPF(Modular Policy Framework)를 사용하여 다음 작업을 수행합니다.

1. **class-map** - 우선순위 대기열 처리를 수행할 트래픽을 식별합니다.
2. **policy-map**(우선순위 대기열 처리의 경우) - 각 클래스 맵과 연계된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **priority** - 클래스 맵에 대한 우선순위 대기열 처리를 활성화합니다. 사용하려는 정책 맵이 계층적인 경우에만 priority 명령을 포함할 수 있습니다.

3. **policy-map**(트래픽 셰이핑의 경우) - **class-default** 클래스 맵과 연계된 작업을 식별합니다.
   a. **class class-default** - 작업을 수행할 **class-default** 클래스 맵을 식별합니다.
   b. **shape** - 클래스 맵에 트래픽 셰이핑을 적용합니다.
   c. **service-policy** - 셰이핑된 트래픽의 하위 집합에 우선순위 대기열 처리를 적용할 수 있도록 **priority** 명령을 구성한 우선순위 대기열 처리 정책 맵을 호출합니다.
4. **service-policy** - 하나의 인터페이스 또는 전역적으로 정책 맵을 할당합니다.

예

다음 예에서는 외부 인터페이스의 모든 트래픽에 대한 트래픽 셰이핑을 활성화하고 VPN tunnel-grp1 내에서 DSCP 비트가 ef로 설정된 트래픽의 우선순위를 지정합니다.

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef

ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

ciscoasa(config-pmap-c)# service-policy shape_policy interface outside
```

관련 명령

명령	설명
class(policy-map)	정책 맵의 클래스 맵을 식별합니다.
clear configure service-policy	서비스 정책 컨피그레이션을 지웁니다.
clear service-policy	서비스 정책 통계를 지웁니다.
policy-map	클래스 맵에서 수행할 작업을 식별합니다.
priority	우선순위 대기열 처리를 활성화합니다.
service-policy(global)	인터페이스에 정책 맵을 적용합니다.
shape	트래픽 셰이핑을 활성화합니다.
show running-config service-policy	실행 중인 컨피그레이션에 구성된 서비스 정책을 표시합니다.
show service-policy	서비스 정책 통계를 표시합니다.

service-policy(global)

모든 인터페이스 또는 대상 인터페이스에서 정책 맵을 전역적으로 활성화하려면 글로벌 컨피그레이션 모드에서 **service-policy** 명령을 사용합니다. 서비스 정책을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 인터페이스에서 정책 집합을 활성화하려면 **service-policy** 명령을 사용합니다.

service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

no service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

구문 설명

fail-close	IPv6 트래픽을 지원하지 않는 애플리케이션 검사에서 삭제된 IPv6 트래픽에 대한 syslog(767001)를 생성합니다. 기본적으로 syslog는 생성되지 않습니다.
global	모든 인터페이스에 정책 맵을 적용합니다.
interface *intf*	특정 인터페이스에 정책 맵을 적용합니다.
policymap_name	**policy-map** 명령에서 구성한 정책 맵 이름을 지정합니다. 검사 정책 맵(**policy-map type inspect**)은 지정하지 않고 계층 3/4 정책 맵만 지정할 수 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	**fail-close** 키워드가 추가되었습니다.

사용 지침

서비스 정책을 활성화하려면 MPF(Modular Policy Framework)를 사용합니다.

1. **class-map** - 우선순위 대기열 처리를 수행할 트래픽을 식별합니다.
2. **policy-map** - 각 클래스 맵과 연계된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. *지원되는 기능에 대한 명령* - 지정된 클래스 맵에 대해 QoS, 애플리케이션 검사, CSC 또는 AIP SSM, TCP 및 UDP 연결 제한 및 시간 제한, TCP 정규화 등 여러 기능에 대한 다양한 작업을 구성할 수 있습니다. 각 기능에 사용할 수 있는 명령에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.

3. **service-policy** - 하나의 인터페이스 또는 전역적으로 정책 맵을 할당합니다.

인터페이스 서비스 정책은 지정된 기능에 대한 전역 서비스 정책보다 우선합니다. 예를 들어 검사에 대한 전역 정책과 TCP 정규화에 대한 인터페이스 정책이 있는 경우 검사와 TCP 정규화 모두 인터페이스에 적용됩니다. 그러나 검사에 대한 전역 정책이 있고 검사에 대한 인터페이스 정책이 있는 경우에는 인터페이스 정책 검사만 해당 인터페이스에 적용됩니다.

기본적으로 이 컨피그레이션은 모든 기본 애플리케이션 검사 트래픽과 일치하는 전역 정책을 포함하며, 트래픽에 전역적으로 검사를 적용합니다. 하나의 전역 정책만 적용할 수 있으므로 전역 정책을 변경하려면 기본 정책을 수정하거나, 기본 정책을 비활성화하고 새 정책을 적용해야 합니다.

기본 서비스 정책에는 다음 명령이 포함됩니다.

```
service-policy global_policy global
```

예

다음 예에서는 외부 인터페이스에서 inbound_policy 정책 맵을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# service-policy inbound_policy interface outside
```

다음 명령은 기본 전역 정책을 비활성화하며, 다른 모든 ASA 인터페이스에서 new_global_policy라는 새 정책을 활성화합니다.

```
ciscoasa(config)# no service-policy global_policy global
ciscoasa(config)# service-policy new_global_policy global
```

관련 명령

명령	설명
clear configure service-policy	서비스 정책 컨피그레이션을 지웁니다.
clear service-policy	서비스 정책 통계를 지웁니다.
service-policy(class)	다른 정책 맵 아래의 계층적 정책을 적용합니다.
show running-config service-policy	실행 중인 컨피그레이션에 구성된 서비스 정책을 표시합니다.
show service-policy	서비스 정책 통계를 표시합니다.

session

모듈 CLI에 액세스하기 위해 ASA에서 IPS SSP 또는 CSC SSM과 같은 모듈로의 텔넷 세션을 설정하려면 특권 EXEC 모드에서 **session** 명령을 사용합니다.

session *id*

구문 설명

id	모듈 ID를 지정합니다. • 물리적 모듈 - **1**(슬롯 번호 1) • 소프트웨어 모듈, ASA FirePOWER- **sfr** • 소프트웨어 모듈, IPS - **ips** • 소프트웨어 모듈, ASA CX - **cxsc**

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.6(1)	IPS SSP 소프트웨어 모듈에 대한 **ips** 모듈 ID가 추가되었습니다.
9.1(1)	ASA CX 모듈에 대한 지원이 추가되었습니다(**cxsc** 키워드).
9.2(1)	ASA FirePOWER 모듈에 대한 지원이 추가되었습니다(**sfr** 키워드).

사용 지침

이 명령은 모듈이 가동 상태인 경우에만 사용할 수 있습니다. 상태 정보는 **show module** 명령을 참고하십시오.

세션을 종료하려면 **exit** 또는 **Ctrl-Shift-6**을 입력한 다음 **x** 키를 입력합니다.

다음 하드웨어 모듈에서는 **session 1** 명령이 작동하지 않습니다.

- ASA CX
- ASA FirePOWER

예

다음 예에서는 슬롯 1의 모듈에 대한 세션을 설정합니다.

```
ciscoasa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

관련 명령

명령	설명
debug session-command	세션에 대한 디버깅 메시지를 표시합니다.

session console

ASA에서 IPS SSP 소프트웨어 모듈과 같은 소프트웨어 모듈로의 가상 콘솔 세션을 설정하려면 특권 EXEC 모드에서 **session console** 명령을 사용합니다. 이 명령은 제어 평면의 작동이 중지되어 **session** 명령을 사용하여 텔넷 세션을 설정할 수 없는 경우에 유용할 수 있습니다.

session *id* **console**

구문 설명

id	모듈 ID를 지정합니다. • ASA FirePOWER 모듈 - **sfr** • IPS 모듈 - **ips** • ASA CX 모듈 - **cxsc**

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.
9.1(1)	ASA CX 모듈에 대한 지원이 추가되었습니다(**cxsc** 키워드).
9.2(1)	ASA FirePOWER 모듈에 대한 지원이 추가되었습니다(**sfr** 키워드).

사용 지침

세션을 종료하려면 **Ctrl-Shift-6**을 입력한 다음 **x** 키를 입력합니다.

터미널 서버와 함께 이 명령을 사용하지 마십시오. 여기서 **Ctrl-Shift-6, x**는 터미널 서버 프롬프트로 되돌아가는 이스케이프 시퀀스입니다. 또한 **Ctrl+Shift+A 6, x**는 모듈 콘솔을 이스케이프하고 ASA 프롬프트로 돌아갑니다. 따라서 이 경우 모듈 콘솔을 종료하려고 하면 터미널 서버 프롬프트로의 모든 경로가 종료됩니다. 터미널 서버를 ASA에 다시 연결하면 모듈 콘솔 세션이 여전히 활성 상태이므로 ASA 프롬프트를 종료할 수 없습니다. 콘솔을 ASA 프롬프트로 되돌리려면 직접 시리얼 연결을 사용해야 합니다.

대신 **session** 명령을 사용하십시오.

예

다음 예에서는 IPS 모듈에 대한 콘솔 세션을 생성합니다.

```
ciscoasa# session ips console

Establishing console session with slot 1
Opening console session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-SHIFT-6 then x'.

sensor login: service
Password: test
```

관련 명령

명령	설명
session	모듈에 대한 텔넷 세션을 시작합니다.
show module log console	콘솔 로그 정보를 표시합니다.

session do

텔넷 세션을 설정하고 ASA에서 모듈로 명령을 수행하려면 특권 EXEC 모드에서 **session do** 명령을 사용합니다.

session *id* **do** *command*

구문 설명

id	모듈 ID를 지정합니다. • 물리적 모듈 - **1**(슬롯 번호 1) • 소프트웨어 모듈, ASA FirePOWER- **sfr** • 소프트웨어 모듈, IPS - **ips** • 소프트웨어 모듈, ASA CX - **cxsc**
command	모듈에 대한 명령을 수행합니다. 지원되는 명령은 다음과 같습니다. • **setup host ip** *ip_address*/*mask*,*gateway_ip*—관리 IP 주소 및 게이트웨이를 설정합니다. • **get-config** - 모듈 컨피그레이션을 가져옵니다. • **password-reset** - 모듈 비밀번호를 기본값으로 재설정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.
8.6(1)	IPS SSP 소프트웨어 모듈에 대한 **ips** 모듈 ID가 추가되었습니다.
8.4(4.1)	ASA CX 모듈에 대한 지원이 추가되었습니다.
9.2(1)	**sfr** 키워드를 포함하여 ASA FirePOWER 모듈에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 모듈이 가동 상태인 경우에만 사용할 수 있습니다. 상태 정보는 **show module** 명령을 참고하십시오.

세션을 종료하려면 **exit** 또는 **Ctrl-Shift-6**을 입력한 다음 **X** 키를 입력합니다.

예

다음 예에서는 기본 게이트웨이 10.1.1.1을 사용하여 관리 IP 주소를 10.1.1.2/24로 설정합니다.

```
ciscoasa# session 1 do setup host ip 10.1.1.2/24,10.1.1.1
```

관련 명령

명령	설명
debug session-command	세션에 대한 디버깅 메시지를 표시합니다.

session ip

IPS SSP 또는 CSC SSM과 같은 모듈의 로깅 IP 주소를 구성하려면 특권 EXEC 모드에서 **session ip** 명령을 사용합니다.

session *id* **ip** {**address** *address mask* | **gateway** *address*}

구문 설명

id	모듈 ID를 지정합니다. • 물리적 모듈 - **1**(슬롯 번호 1) • 소프트웨어 모듈, IPS - **ips**
address *address*	syslog 서버 주소를 설정합니다.
gateway *address*	게이트웨이를 syslog 서버로 설정합니다.
mask	서브넷 마스크를 설정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.
8.4(4.1)	ASA CX 모듈에 대한 지원이 추가되었습니다.
8.6(1)	IPS SSP 소프트웨어 모듈에 대한 **ips** 모듈 ID가 추가되었습니다.

사용 지침

이 명령은 모듈이 가동 상태인 경우에만 사용할 수 있습니다. 상태 정보는 **show module** 명령을 참고하십시오.

세션을 종료하려면 **exit** 또는 **Ctrl-Shift-6**을 입력한 다음 **X** 키를 입력합니다.

예

다음 예에서는 슬롯 1의 모듈에 대한 세션을 설정합니다.

```
ciscoasa# session 1 ip address
```

관련 명령

명령	설명
debug session-command	세션에 대한 디버깅 메시지를 표시합니다.

session-limit

최대 동시 MDM 프록시 세션 수를 설정합니다. config-mdm-proxy 모드에서 사용합니다. 이 명령의 no 형식에서는 구성된 제한을 지정해야 합니다.

session-limit *session-limit*

no session-limit *session-limit*

구문 설명

session-limit	최대 동시 MDM 세션 수를 설정합니다. 유효 범위는 1~10000이고, 기본값은 1000입니다.

기본값

기본 세션 제한은 1000입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
config-mdm-proxy	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.3(1)	MDM 프록시 서비스에 대한 명령이 도입되었습니다.

예

다음 예에서는 MDM 프록시 서비스에 대해 세션 제한을 5000으로 설정하는 방법을 보여 줍니다.

```
ciscoasa (config)# mdm-proxy
ciscoasa (config-mdm-proxy)# session-limit 5000
```

관련 명령

명령	설명
mdm-proxy	config-mdm-proxy 모드를 시작하고 MDM 프록시 서비스를 구성합니다.
show running-config mdm-proxy	현재 MDM 프록시 컨피그레이션을 표시합니다.

session-timeout

MDM 프록시 등록 및 체크인 세션의 최대 기간(초)을 설정합니다. config-mdm-proxy 모드에서 사용합니다. 이 명령의 no 형식은 구성된 시간 제한을 지정해야 합니다.

session-timeout [enrollment *seconds***] [checkin** *seconds***]**

no session-timeout [enrollment *seconds***] [checkin** *seconds***]**

구문 설명

seconds	MDM 등록 및 체크인 세션의 최대 기간(초)입니다. 유효 범위는 60~600입니다. 기본값은 300초입니다.

기본값

기본 세션 시간 제한은 300초입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
config-mdm-proxy	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.3(1)	MDM 프록시 서비스에 대한 명령이 도입되었습니다.

예

다음 예에서는 MDM 프록시 체크인 세션에 대한 세션 시간 제한을 600초로 설정하는 방법을 보여줍니다.

```
ciscoasa (config)# mdm-proxy
ciscoasa (config-mdm-proxy)# session-timeout checkin 600
```

관련 명령

명령	설명
mdm-proxy	config-mdm-proxy 모드를 시작하고 MDM 프록시 서비스를 구성합니다.
show running-config mdm-proxy	현재 MDM 프록시 컨피그레이션을 표시합니다.

set as-path

BGP 경로에 대한 자동 시스템 경로를 수정하려면 route-map 컨피그레이션 모드에서 **set as-path** 명령을 사용합니다. 자동 시스템 경로를 수정하지 않으려면 이 명령의 **no** 형식을 사용합니다.

set as-path {tag | prepend *as-path-string***}**

no set as-path {tag | prepend *as-path-string***}**

구문 설명

as-path-string	AS_PATH 특성 앞에 추가할 자동 시스템의 번호입니다. 이 인수 값의 범위는 1에서 65535 사이의 자동 시스템 번호입니다. 10개의 AS 번호까지 여러 값을 입력할 수 있습니다. 자동 시스템 번호 형식에 대한 자세한 내용은 **router bgp** 명령을 참고하십시오.
prepend	경로 맵과 일치하는 경로의 자동 시스템 경로에 **prepend** 키워드 뒤의 문자열을 추가합니다. 인바운드 및 아웃바운드 BGP 경로 맵에 적용됩니다.
tag	경로의 태그를 자동 시스템 경로로 변환합니다. 경로를 BGP로 재배포할 때만 적용됩니다.

기본값

자동 시스템 경로는 수정되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

최적 경로 선택에 영향을 줄 수 있는 전역 BGP 메트릭만 자동 시스템 경로 길이입니다. 자동 시스템 경로 길이를 변경하면 BGP 스피커가 멀리 있는 피어의 최적 경로 선택에 영향을 줄 수 있습니다.

태그를 자동 시스템 경로로 변환할 수 있도록 허용하면 이 명의 **set as-path tag** 변형이 자동 시스템 길이를 수정합니다. **set as-path prepend** 변형을 사용하면 임의 자동 시스템 경로 문자열을 BGP 경로 "앞에 추가"할 수 있습니다. 일반적으로 로컬 자동 시스템 번호가 앞에 여러 번 추가되어 자동 시스템 경로 길이를 늘립니다.

4바이트 자동 시스템 번호의 Cisco 구현에서는 asplain(예: 65538)을 자동 시스템 번호의 기본 정규식 일치 및 출력 표시 형식으로 사용하지만 RFC 5396에 설명된 대로 asplain 형식과 asdot 형식으로 4바이트 자동 시스템 번호를 구성할 수 있습니다. 4바이트 자동 시스템 번호의 기본 정규식 일치 및 출력 표시를 asdot 형식으로 변경하려면 **clear bgp *** 명령이 뒤에 오는 **bgp asnotation dot** 명령을 사용하여 모든 현재 BGP 세션의 하드 재설정을 수행합니다.

예

다음 예에서는 재배포된 경로의 태그를 자동 시스템 경로로 변환합니다.

```
ciscoasa(config)# route-map set-as-path-from-tag
ciscoasa(config-route-map)# set as-path tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute ospf 109 route-map set-as-path-from-tag
```

다음 예에서는 10.108.1.1로 보급되는 모든 경로 앞에 100 100 100을 추가합니다.

```
ciscoasa(config)# route-map set-as-path
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set as-path prepend 100 100 100
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 route-map set-as-path out
```

관련 명령

명령	설명
clear bgp	하드 또는 소프트 재구성을 사용하여 BGP 연결을 재설정합니다.
bgp asnotation dot	BGP(Border Gateway Protocol) 4바이트 자동 시스템 번호의 기본 표시 및 정규식 일치 형식을 asplain 형식(십진수 값)에서 점 표기법으로 변경합니다.

set automatic-tag

태그 값을 자동으로 계산하려면 route-map 컨피그레이션 모드에서 set automatic-tag 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

set automatic-tag

no set automatic-tag

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

태그를 설정하려면 match 절이 있어야 합니다(모두 허용하는 경우도 포함).

route-map 글로벌 컨피그레이션 명령과 match 및 set **route-map** 컨피그레이션 명령을 사용하여 라우팅 프로토콜 간의 재배포 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연계된 match 및 set 명령 목록이 있습니다. match 명령은 일치 조건(현재 **route-map** 명령에 재배포가 허용되는 조건)을 지정합니다. set 명령은 설정 작업(match 명령에서 적용하는 조건이 충족된 경우에 수행할 특정 재배포 작업)을 지정합니다. 또한 **no route-map** 명령은 경로 맵을 삭제합니다.

set **route-map** 컨피그레이션 명령은 경로 맵의 모든 일치 조건이 충족된 경우에 수행할 재배포 설정 작업을 지정합니다. 모든 일치 조건이 충족되면 모든 설정 작업이 수행됩니다.

예

다음 예에서는 BGP(Border Gateway Protocol)에서 학습한 경로에 대한 태그 값을 자동으로 계산하도록 Cisco ASA 소프트웨어를 구성합니다.

```
ciscoasa(config-route-map)# route-map tag
ciscoasa(config-route-map)# match as-path 10
iscoasa(config-route-map)# set automatic-tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# table-map tag
```

set community

BGP 커뮤니티 특성을 설정하려면 **set community** 경로 맵 컨피그레이션 명령을 사용합니다. 이 항목을 제거하려면 이 명령의 **no** 형식을 사용합니다.

set community {*community-number* [**additive**] | [*well-known-community*] [**additive**] | **none**}

no set community

구문 설명

additive	(선택 사항) 기존 커뮤니티에 커뮤니티를 추가합니다.
community-number	해당 커뮤니티 번호를 지정합니다. 유효한 값은 1~4294967200, **no-export** 또는 **no-advertise**입니다.
none	(선택 사항) 경로 맵을 전달하는 접두사에서 커뮤니티 특성을 제거합니다.
well-known-community	(선택 사항) 다음 키워드를 사용하여 잘 알려진 커뮤니티를 지정할 수 있습니다. • **internet** • **local-as** • **no-advertise** • **no-export**

기본값

BGP 커뮤니티 특성은 존재하지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

태그를 설정하려면 match 절이 있어야 합니다("모두 허용" 목록을 가리키는 경우도 포함).

route-map 글로벌 컨피그레이션 명령과 **match** 및 **set** 경로 맵 컨피그레이션 명령을 사용하여 라우팅 프로토콜 간의 재배포 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연계된 **match** 및 **set** 명령 목록이 있습니다. **match** 명령은 *일치 조건*(현재 **route-map** 명령에 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 *설정 작업*(**match** 명령에서 적용하는 조건이 충족된 경우에 수행할 특정 재배포 작업)을 지정합니다. 또한 **no route-map** 명령은 경로 맵을 삭제합니다.

set 경로 맵 컨피그레이션 명령은 경로 맵의 모든 일치 조건이 충족된 경우에 수행할 재배포 *설정 작업*을 지정합니다. 모든 일치 조건이 충족되면 모든 설정 작업이 수행됩니다.

예

다음 예에서 자동 시스템 경로 액세스 목록 1을 전달하는 경로에는 109로 설정된 커뮤니티가 있습니다. 자동 시스템 경로 액세스 목록 2를 전달하는 경로에는 no-export로 설정된 커뮤니티가 있습니다(이러한 경로는 외부 BGP[eBGP] 피어로 보급되지 않음).

```
ciscoasa(config-route-map)# set community 10
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set community 109
ciscoasa(config-route-map)# set community 20
ciscoasa(config-route-map)# match as-path 2
ciscoasa(config-route-map)# set community no-export
```

관련 명령

명령	설명
match as-path	액세스 목록에 지정된 BGP 자동 시스템 경로를 일치시킵니다.

set connection

정책 맵 내에서 트래픽 클래스에 대한 연결 제한을 지정하려면 클래스 컨피그레이션 모드에서 **set connection** 명령을 사용합니다. 이러한 지정을 제거하여 무제한 연결을 허용하려면 이 명령의 **no** 형식을 사용합니다.

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

구문 설명

conn-max *n*	허용되는 최대 동시 TCP 및/또는 UDP 연결 수(0~2000000)를 설정합니다. 기본값은 무제한 연결을 허용하는 0입이다. 예를 들어 두 개의 서버가 동시 TCP 및/또는 UDP 연결을 허용하도록 구성된 경우 연결 제한은 구성된 각 서버에 개별적으로 적용됩니다. 클래스 아래에 구성된 경우 이 인수는 전체 클래스에 허용되는 최대 동시 연결 수를 제한합니다. 이 경우 하나의 공격 호스트가 모든 연결을 사용하여 클래스 아래의 액세스 목록에 일치하는 호스트를 남겨두지 않을 수 있습니다.
embryonic-conn-max *n*	허용되는 최대 동시 원시 연결 수(0~2000000)를 설정합니다. 기본값은 무제한 연결을 허용하는 0입이다.
per-client-embryonic-max *n*	클라이언트당 허용되는 최대 동시 원시 연결 수(0~2000000)를 설정합니다. 클라이언트는 ASA를 통해 원시 연결 패킷을 전송(새 연결을 생성)하는 호스트로 정의됩니다. 이 기능을 위해 **class-map**에서 트래픽을 일치시키도록 **access-list**가 사용된 경우에는 액세스 목록과 일치하는 모든 클라이언트의 누적 원시 연결이 아니라 호스트별로 원시 제한이 적용됩니다. 기본값은 무제한 연결을 허용하는 0입이다. 관리 클래스 맵에는 이 키워드를 사용할 수 없습니다.
per-client-max *n*	클라이언트당 허용되는 최대 동시 연결 수(0~2000000)를 설정합니다. 클라이언트는 ASA를 통해 원시 연결 패킷을 전송(새 연결을 생성)하는 호스트로 정의됩니다. 이 기능을 위해 **class-map**에서 트래픽을 일치시키도록 **access-list**가 사용된 경우에는 액세스 목록과 일치하는 모든 클라이언트의 누적 연결이 아니라 호스트별로 연결 제한이 적용됩니다. 기본값은 무제한 연결을 허용하는 0입이다. 관리 클래스 맵에는 이 키워드를 사용할 수 없습니다. 클래스 아래에 구성된 경우 이 키워드는 클래스 아래의 액세스 목록과 일치하는 각 호스트에 허용되는 최대 동시 연결 수를 제한합니다.
random-sequence-number {enable | disable}	TCP 시퀀스 번호 임의 설정을 활성화하거나 비활성화합니다. 관리 클래스 맵에는 이 키워드를 사용할 수 없습니다. 자세한 내용은 "사용 지침" 섹션을 참고하십시오.

기본값

conn-max, **embryonic-conn-max**, **per-client-embryonic-max** 및 **per-client-max** 파라미터의 경우 *n*의 기본값은 무제한 연결을 허용하는 0입니다.

시퀀스 번호 임의 설정은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.1(1)	**per-client-embryonic-max** 및 **per-client-max** 키워드가 추가되었습니다.
8.0(2)	이제 계층 3/4 관리 클래스 맵의 to-the-ASA 관리 트래픽에 이 명령을 사용할 수 있습니다. **conn-max** 및 **embryonic-conn-max** 키워드만 사용할 수 있습니다.
9.0(1)	최대 연결 수가 65535에서 2000000으로 증가되었습니다.

사용 지침

모듈러 정책 프레임 워크를 사용하여 이 명령을 구성합니다. 먼저 **class-map** 명령(통과 트래픽의 경우) 또는 **class-map type management** 명령(관리 트래픽의 경우)을 사용하여 시간 제한을 적용할 트래픽을 정의합니다. 그런 다음 **policy-map** 명령을 입력하여 정책을 정의하고, **class** 명령을 입력하여 클래스 맵을 참조합니다. 클래스 컨피그레이션 모드에서 **set connection** 명령을 입력할 수 있습니다. 마지막으로 **service-policy** 명령을 사용하여 정책 맵을 인터페이스에 적용합니다. 모듈러 정책 프레임 워크의 작동 방식에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.

참고 ASA 모델의 CPU 코어 수에 따라 각 코어에서 연결을 관리하는 방식으로 인해 최대 동시 및 원시 연결이 구성된 개수를 초과할 수도 있습니다. 최악의 경우 ASA는 최대 *n*-1개(여기서 *n*은 코어 수)의 추가 연결 및 원시 연결을 허용합니다. 예를 들어 모델에 4개의 코어가 있는 경우 6개의 동시 연결과 4개의 원시 연결을 구성하면 유형별로 3개가 추가될 수 있습니다. 모델의 코어 수를 확인하려면 **show cpu core** 명령을 입력합니다.

TCP Intercept 개요

원시 연결 수를 제한하면 DoS 공격으로부터 보호됩니다. ASA에서는 클라이언트별 제한 및 원시 연결 제한을 사용하여 TCP Intercept를 트리거합니다. 이는 TCP SYN 패킷과의 인터페이스를 플러딩하여 실행되는 DoS 공격으로부터 내부 시스템을 보호합니다. 원시 연결은 소스와 대상 간에 필요한 핸드셰이크를 완료하지 않은 연결 요청입니다. TCP Intercept에서는 SYN 쿠키 알고리즘을 사용하여 TCP SYN 플러딩 공격을 방지합니다. SYN 플러딩 공격은 일반적으로 스푸핑된 IP 주소에서 시작되는 일련의 SYN 패킷으로 구성됩니다. SYN 패킷에 대한 지속적인 플러딩은 서버 SYN 대기열을 꽉 찬 상태로 유지하여 연결 요청에 대응하지 못하도록 합니다. 연결의 원시 연결 임계값에 도달하면 ASA는 서버의 프록시 역할을 하며 클라이언트 SYN 요청에 대한 SYN-ACK 응답을 생성합니다. ASA는 클라이언트에서 ACK를 다시 받은 후 클라이언트를 인증하고 서버에 연결하도록 허용합니다.

TCP 시퀀스 임의 설정

각 TCP 연결에는 각각 클라이언트와 서버에서 생성된 두 개의 ISN이 있습니다. ASA는 인바운드와 아웃바운드 두 방향 모두로 전달되는 TCP SYN의 ISN을 임의로 설정합니다.

보호된 호스트의 ISN을 임의로 설정하면 공격자가 새 연결을 위한 다음 ISN을 예측하지 못하며 잠재적으로 새 세션의 가로채기가 방지됩니다.

필요한 경우 TCP 초기 시퀀스 번호 임의 설정을 비활성화할 수 있습니다. 예를 들면 다음과 같습니다.

- 다른 인라인 방화벽에서도 초기 시퀀스 번호를 임의로 설정하는 경우에는 두 방화벽 모두 이 작업을 수행할 필요가 없습니다. 이는 이 작업이 트래픽에 영향을 주지 않는 경우에도 마찬가지입니다.
- ASA를 통해 eBGP 멀티 홉을 사용하는 경우 eBGP 피어는 MD5를 사용합니다. 임의 설정은 MD5 체크섬을 중단합니다.
- 연결의 시퀀스 번호를 임의 설정하지 않으려면 ASA가 필요한 WAAS 디바이스를 사용합니다.

예

다음은 **set connection** 명령을 사용하여 최대 동시 연결 수는 256으로 설정하고 TCP 시퀀스 번호 임의 설정을 비활성화하는 예입니다.

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
ciscoasa(config-pmap-c)#
```

여러 파라미터와 함께 이 명령을 입력하거나, 각 파라미터를 별도의 명령으로 입력할 수 있습니다. ASA는 실행 중인 컨피그레이션에서 명령을 한 줄로 결합합니다. 예를 들어 클래스 컨피그레이션 모드에서 다음 두 명령을 입력한 경우

```
ciscoasa(config-pmap-c)# set connection conn-max 600
ciscoasa(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map 명령의 출력에는 두 명령의 결과가 결합된 단일 명령으로 표시됩니다.

```
set connection conn-max 600 embryonic-conn-max 50
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 class-map을 지정합니다.
clear configure policy-map	모든 policy-map 컨피그레이션을 제거합니다. 단, policy-map이 service-policy 명령에서 사용 중인 경우에는 policy-map이 제거되지 않습니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
show running-config policy-map	모든 현재 policy-map 컨피그레이션을 표시합니다.
show service-policy	서비스 정책 컨피그레이션을 표시합니다. **set connection** 키워드를 사용하여 **set connection** 명령이 포함된 정책을 볼 수 있습니다.

set connection advanced-options

TCP 정규화를 사용자 지정하려면 클래스 컨피그레이션 모드에서 **set connection advanced-options** 명령을 사용합니다. TCP 정규화 옵션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

set connection advanced-options *tcp_mapname*

no set connection advanced-options *tcp_mapname*

구문 설명

tcp_mapname	**tcp-map** 명령을 통해 생성되는 TCP 맵의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

TCP 맵을 사용하여 TCP 정규화를 사용자 지정하려면 MPF(Modular Policy Framework)를 사용합니다.

1. **tcp-map** - TCP 정규화 작업을 식별합니다.
2. **class-map** - TCP 정규화 작업을 수행할 트래픽을 식별합니다.
3. **policy-map** - 클래스 맵과 연계된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **set connection advanced options** - TCP 맵을 클래스 맵에 적용합니다.
4. **service-policy** - 하나의 인터페이스 또는 전역적으로 정책 맵을 할당합니다.

예

다음 예에서는 **set connection advanced-options** 명령을 사용하여 localmap이라는 TCP 맵의 사용을 지정하는 방법을 보여 줍니다.

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config-cmap)# exit
ciscoasa(config)# tcp-map localmap
ciscoasa(config)# policy-map global_policy global
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection advanced-options localmap
ciscoasa(config-pmap-c)#
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 class-map을 지정합니다.
class-map	class-map 컨피그레이션 모드에서 일치 조건을 지정해 최대 하나(tunnel-group 및 default-inspection-traffic은 제외) 의 match 명령을 실행하여 트래픽 클래스를 구성합니다.
clear configure policy-map	모든 policy-map 컨피그레이션을 제거합니다. 단, policy-map이 service-policy 명령에서 사용 중인 경우에는 policy-map이 제거되지 않습니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
show running-config policy-map	모든 현재 policy-map 컨피그레이션을 표시합니다.
tcp-map	TCP 맵을 생성합니다.

set connection advanced-options tcp-state-bypass

TCP 상태 우회를 활성화하려면 클래스 컨피그레이션 모드에서 **set connection advanced-options** 명령을 사용합니다. 클래스 컨피그레이션 모드는 policy-map 컨피그레이션 모드에서 액세스할 수 있습니다. TCP 상태 우회를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

set connection advanced-options tcp-state-bypass

no set connection advanced-options tcp-state-bypass

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 TCP 상태 우회는 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

TCP 상태 우회를 활성화하려면 MPF(Modular Policy Framework)를 사용합니다.

1. **class-map** - TCP 상태 우회를 수행할 트래픽을 식별합니다.
2. **policy-map** - 클래스 맵과 연계된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **set connection advanced options tcp-state-bypass** - TCP 상태 우회를 클래스 맵에 적용합니다.
3. **service-policy** - 하나의 인터페이스 또는 전역적으로 정책 맵을 할당합니다.

개별 디바이스를 통한 인바운드 및 아웃바운드 흐름 허용

기본적으로 ASA를 통과하는 모든 트래픽은 ASA(Adaptive Security Algorithm)를 사용하여 검사되며, 보안 정책에 따라 통과하도록 허용되거나 삭제됩니다. ASA는 각 패킷의 상태(새 연결인지 설정된 연결인지)를 확인하고 이를 세션 관리 경로(새 연결 SYN 패킷), 빠른 경로(설정된 연결) 또는 제어 평면 경로(고급 검사)에 할당하여 방화벽 성능을 극대화합니다.

빠른 경로에 있는 기존 연결과 일치하는 TCP 패킷은 보안 정책의 모든 사항을 다시 확인하지 않고 ASA를 통과할 수 있습니다. 이 기능은 성능을 극대화합니다. 그러나 SYN 패킷을 사용하여 빠른 경로에서 세션을 설정하는 방법과 빠른 경로에서 발생하는 확인(예: TCP 시퀀스 번호)은 비동기 라우팅 솔루션을 방해할 수 있습니다. 연결의 아웃바운드 및 인바운드 흐름이 모두 동일한 ASA를 통과해야 합니다.

예를 들어 새 연결은 ASA 1로 이동합니다. SYN 패킷은 세션 관리 경로를 통과하며 연결 항목이 빠른 경로 테이블에 추가됩니다. 이 연결의 후속 패킷이 ASA 1을 통과하는 경우 이러한 패킷은 빠른 경로의 항목과 일치하므로 통과됩니다. 그러나 후속 패킷이 세션 관리 경로를 통과한 SYN 패킷이 없는 ASA 2로 이동하는 경우에는 빠른 경로에 연결을 위한 항목이 없으므로 패킷이 삭제됩니다.

업스트림 라우터에서 비동기 라우팅을 구성하고 트래픽이 두 개의 ASA 사이에서 번갈아 전송되는 경우 특정 트래픽에 대한 TCP 상태 우회를 구성할 수 있습니다. TCP 상태 우회는 빠른 경로에서 세션이 설정되는 방식을 변경하고 빠른 경로 확인을 비활성화합니다. 이 기능은 TCP 트래픽을 UDP 연결과 유사하게 처리합니다. 지정된 네트워크와 일치하는 비 SYN 패킷이 ASA로 들어올 때 빠른 경로 항목이 없는 경우에는 패킷이 세션 관리 경로를 통과하여 빠른 경로에서 연결을 설정합니다. 빠른 경로에 있게 되면 이 트래픽은 빠른 경로 확인을 우회합니다.

지원되지 않는 기능

다음 기능은 TCP 상태 우회를 사용할 때 지원되지 않습니다.

- 애플리케이션 검사 - 애플리케이션 검사를 수행하려면 인바운드 트래픽과 아웃바운드 트래픽이 모두 동일한 ASA를 통과해야 하므로 TCP 상태 우회에서는 애플리케이션 검사가 지원되지 않습니다.
- AAA 인증 세션 - 사용자가 하나의 ASA에 인증하는 경우 다른 ASA를 통해 반환되는 트래픽은 거부됩니다. 사용자가 해당 ASA에 인증하지 않았기 때문입니다.
- TCP Intercept, 최대 원시 연결 제한, TCP 시퀀스 번호 임의 설정 - ASA는 연결 상태를 추적하지 않으므로 이러한 기능은 적용되지 않습니다.
- TCP 정규화 - TCP 노멀라이저는 비활성화되어 있습니다.
- SSM IPS 기능 - IPS 또는 CSC와 같은 SSM에서 실행되는 모든 애플리케이션 및 TCP 상태 우회를 사용할 수 없습니다.

NAT 지침

변환 세션은 각 ASA에 대해 별도로 설정되기 때문에 두 ASA 모두에서 TCP 상태 우회 트래픽에 대한 상태 NAT를 구성해야 합니다. 동적 NAT를 사용하는 경우 ASA 1의 세션에 대해 선택되는 주소는 ASA 2의 세션에 대해 선택되는 주소와 다릅니다.

연결 시간 제한 지침

지정된 연결에서 2분 동안 트래픽이 없는 경우 연결 시간이 초과됩니다. **set connection timeout tcp** 명령을 사용하여 이 기본값을 재정의할 수 있습니다. 일반 TCP 연결은 기본적으로 60분 후에 시간 초과됩니다.

예

다음은 TCP 상태 우회에 대한 컨피그레이션 예입니다.

```
ciscoasa(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

ciscoasa(config)# class-map tcp_bypass
ciscoasa(config-cmap)# description "TCP traffic that bypasses stateful firewall"
ciscoasa(config-cmap)# match access-list tcp_bypass

ciscoasa(config-cmap)# policy-map tcp_bypass_policy
ciscoasa(config-pmap)# class tcp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options tcp-state-bypass

ciscoasa(config-pmap-c)# service-policy tcp_bypass_policy outside
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵을 식별합니다.
class-map	서비스 정책에서 사용할 클래스 맵을 생성합니다.
policy-map	클래스 맵과 하나 이상의 작업을 연계하는 정책 맵을 구성합니다.
service-policy	인터페이스에 정책 맵을 할당합니다.
set connection timeout	연결 시간 제한을 설정합니다.

set connection decrement-ttl

정책 맵 내에서 트래픽 클래스에 대한 TTL(Time to Live) 값을 줄이려면 클래스 컨피그레이션 모드에서 **set connection decrement-ttl** 명령을 사용합니다. TTL(Time to Live) 값을 줄이지 않으려면 이 명령의 **no** 형식을 사용합니다.

set connection decrement-ttl

no set connection decrement-ttl

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 ASA는 TTL(Time to Live) 값을 줄이지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(2)	이 명령이 도입되었습니다.

사용 지침

이 명령은 **icmp unreachable** 명령과 함께 ASA를 통한 traceroute가 ASA를 홉 중 하나로 표시하도록 허용하는 데 필요합니다.

예

다음 예에서는 TTL(Time to Live) 감소를 활성화하고 ICMP에서 연결할 수 없는 속도 제한을 설정합니다.

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
icmp unreachable	ASA를 통해 허용되는 ICMP에서 연결할 수 없는 속도를 제어합니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.
show service-policy	서비스 정책 컨피그레이션을 표시합니다.

set connection timeout

정책 맵 내에서 트래픽 클래스에 대한 연결 시간 제한을 지정하려면 클래스 컨피그레이션 모드에서 **set connection timeout** 명령을 사용합니다. 시간 제한을 제거하려면 이 명령의 **no** 형식을 사용합니다.

set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

구문 설명

dcd	DCD(Dead Connection Detection)를 활성화합니다. DCD는 여전히 트래픽을 처리할 수 있는 연결을 만료하지 않고 끊어진 연결을 감지하여 이러한 연결을 만료할 수 있도록 해줍니다. 유휴 상태이지만 유효한 연결이 유지되도록 하려는 경우에 DCD를 구성합니다. TCP 연결 시간이 초과되면 ASA에서 종단 호스트에 DCD 프로브를 보내 연결 유효성을 확인합니다. 종단 호스트 중 하나가 최대 재시도 횟수 후에도 응답하지 않으면 ASA에서 연결을 해제합니다. 두 종단 호스트 모두 연결이 유효한 것으로 응답하면 ASA에서 작업 시간 제한을 현재 시간으로 업데이트하고 그에 따라 유휴 시간 제한을 다시 예약합니다.
embryonic *hh*:*mm*:*ss*	TCP 원시(반 열린) 연결이 닫힐 때까지의 시간 제한(0:0:5~1193:0:0)을 설정합니다. 기본값은 0:0:30입니다. 이 값을 0으로 설정하여 연결 시간이 초과되지 않도록 할 수도 있습니다. 3방향 핸드셰이크가 완료되지 않은 TCP 연결이 원시 연결입니다.
half-closed *hh*:*mm*:*ss*	반 닫힌 연결이 닫힐 때까지의 유휴 시간 제한을 0:5:0(9.1(1) 이하의 경우) 또는 0:0:30(9.1(2) 이상의 경우)에서 1193:0:0 사이로 설정합니다. 기본값은 0:10:0입니다. 이 값을 0으로 설정하여 연결 시간이 초과되지 않도록 할 수도 있습니다. 반 닫힌 연결은 DCD의 영향을 받지 않습니다. 또한 ASA는 반 닫힌 연결을 해제할 때 재설정을 보내지 않습니다.
idle *hh*:*mm*:*ss*	모든 프로토콜의 설정된 연결이 닫히는 유휴 시간 제한을 설정합니다. 유효한 범위는 0:0:1~1193:0:0입니다.
max_retries	연결을 끊어진 것으로 선언하기 전에 DCD에 연속으로 실패한 재시도 횟수를 설정합니다. 최소값은 1이고 최대값은 255입니다. 기본값은 5입니다.
reset	TCP 트래픽에 한해, 유휴 연결이 제거된 후 두 종단 시스템 모두에 TCP RST 패킷을 보냅니다.
retry_interval	다른 프로브를 보내기 전에 응답하지 않는 각 DCD 프로브를 대기할 기간(*hh*:*mm*:*ss* 형식)입니다(0:0:1~24:0:0). 기본값은 0:0:15입니다.

기본값

timeout 명령을 사용하여 기본값을 전역적으로 변경하지 않는 한 기본값은 다음과 같습니다.

- 기본 **embryonic** 시간 제한은 30초입니다.
- 기본 **half-closed** 유휴 시간 제한은 10분입니다.
- 기본 **dcd** *max_retries* 값은 5입니다.
- 기본 **dcd** *retry_interval* 값은 15초입니다.
- 기본 **idle(유휴)** 시간 제한은 1시간입니다.

- 기본 **udp** 유휴 시간 제한은 2분입니다.
- 기본 **icmp** 유휴 시간 제한은 2초입니다.
- 기본 **esp** 및 **ha** 유휴 시간 제한은 30초입니다.
- 다른 프로토콜의 경우 기본 유휴 시간 제한은 2분입니다.
- 시간 제한을 없애려면 0:0:0을 입력합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.2(1)	DCD에 대한 지원이 추가되었습니다.
8.2(2)	모든 프로토콜에 대한 유휴 시간 제한을 제어하는 **idle** 키워드를 사용하기 위해 **tcp** 키워드의 사용이 중단되었습니다.
9.1(2)	최소 **half-closed** 값이 30초(0:0:30)로 낮아졌습니다.

사용 지침

모듈러 정책 프레임 워크를 사용하여 이 명령을 구성합니다. 먼저 **class-map** 명령을 사용하여 시간 제한을 적용할 트래픽을 정의합니다. 그런 다음 **policy-map** 명령을 입력하여 정책을 정의하고, **class** 명령을 입력하여 클래스 맵을 참조합니다. 클래스 컨피그레이션 모드에서 **set connection timeout** 명령을 입력할 수 있습니다. 마지막으로 **service-policy** 명령을 사용하여 정책 맵을 인터페이스에 적용합니다. 모듈러 정책 프레임 워크의 작동 방식에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.

show service-policy 명령은 DCD의 작업 양을 표시하는 카운터를 포함합니다.

예

다음 예에서는 모든 트래픽에 대한 연결 시간 제한을 설정합니다.

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# policy-map CONNS
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
ciscoasa(config-pmap-c)# service-policy CONNS interface outside
```

여러 파라미터와 함께 **set connection** 명령을 입력하거나, 각 파라미터를 별도의 명령으로 입력할 수 있습니다. ASA는 실행 중인 컨피그레이션에서 명령을 한 줄로 결합합니다. 예를 들어 클래스 컨피그레이션 모드에서 다음 두 명령을 입력한 경우

```
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0
ciscoasa(config-pmap-c)# set connection timeout embryonic 0:40:0
```

show running-config policy-map 명령의 출력에는 두 명령의 결과가 다음과 같은 결합된 단일 명령으로 표시됩니다.

```
set connection timeout tcp 2:0:0 embryonic 0:40:0
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 class-map을 지정합니다.
clear configure policy-map	모든 policy-map 컨피그레이션을 제거합니다. 단, policy-map이 service-policy 명령에서 사용 중인 경우에는 policy-map이 제거되지 않습니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
set connection	연결 값을 구성합니다.
show running-config policy-map	모든 현재 policy-map 컨피그레이션을 표시합니다.
show service-policy	DCD 및 기타 서비스 작업의 카운터를 표시합니다.

set local-preference

자동 시스템 경로의 환경 설정 값을 지정하려면 route-map 컨피그레이션 모드에서 set local-preference 명령을 사용합니다. 이 항목을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

set local-preference *number-value*

no set local-preference *number-value*

구문 설명

number-value	환경 설정 값입니다. 0~4294967295의 정수입니다.

기본값

환경 설정 값은 100입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

환경 설정은 로컬 자동 시스템의 모든 라우터로만 전송됩니다.

route-map 글로벌 컨피그레이션 명령과 match 및 set **route-map** 컨피그레이션 명령을 사용하여 라우팅 프로토콜 간의 재배포 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연계된 match 및 set 명령 목록이 있습니다. match 명령은 일치 조건(현재 **route-map** 명령에 재배포가 허용되는 조건)을 지정합니다. set 명령은 설정 작업(match 명령에서 적용하는 조건이 충족된 경우에 수행할 특정 재배포 작업)을 지정합니다. 또한 **no route-map** 명령은 경로 맵을 삭제합니다.

set **route-map** 컨피그레이션 명령은 경로 맵의 모든 일치 조건이 충족된 경우에 수행할 재배포 설정 작업을 지정합니다. 모든 일치 조건이 충족되면 모든 설정 작업이 수행됩니다.

bgp default local-preference 명령을 사용하여 기본 환경 설정 값을 변경할 수 있습니다.

예

다음 예에서는 액세스 목록 1에 포함된 모든 경로에 대한 로컬 환경 설정을 100으로 설정합니다.

```
ciscoasa(config-route-map)# route-map map-preference
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

set metric

경로 맵의 OSPF 및 기타 동적 라우팅 프로토콜에 대한 경로 메트릭 값을 설정하려면 route-map 컨피그레이션 모드에서 **set metric** 명령을 사용합니다. OSPF 및 기타 동적 라우팅 프로토콜의 기본 메트릭 값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

set metric *metric-value* | [*bandwidth delay reliability loading mtu*]

no set metric *metric-value* | [*bandwidth delay reliability loading mtu*]

구문 설명

bandwidth	경로의 EIGRP 대역폭입니다(kbps). 유효한 값의 범위는 0~4294967295입니다.
delay	EIGRP 경로 지연 시간입니다(수십 마이크로초). 유효한 값의 범위는 0~4294967295입니다.
loading	경로의 유효 EIGRP 대역폭입니다(0~255의 숫자로 표시). 값 255는 100% 로딩을 의미합니다.
metric-value	OSPF 및 기타 동적 라우팅 프로토콜(EIGRP 제외)의 경로 메트릭 값입니다(숫자로 표시). 유효한 값의 범위는 0~4294967295입니다.
mtu	EIGRP에 대한 경로의 최소 MTU 크기입니다(바이트). 유효한 값의 범위는 0~4294967295입니다.
reliability	EIGRP에 대한 성공적인 패킷 전송의 가능성입니다(0~255). 값 255는 100% 신뢰성을 의미하고, 0은 신뢰성 없음을 의미합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.2(5)	경로 맵에서 EIGRP를 지원하도록 *bandwidth*, *delay*, *reliability*, *loading* 및 *mtu* 인수가 추가되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

no set metric 명령을 사용하면 OSPF 및 기타 동적 라우팅 프로토콜의 기본 메트릭 값을 복원할 수 있습니다. 이 상황에서 *metric-value* 인수는 0~4294967295의 정수입니다.

예

다음 예에서는 OSPF 라우팅에 대한 경로 맵을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
```

다음 예에서는 경로 맵에서 EIGRP에 대한 메트릭 값을 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# access-list route-out line 1 standard permit 10.1.1.0 255.255.255.0
ciscoasa(config)# route-map rmap permit 10
ciscoasa(config-route-map)# set metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show route-map rmap
route-map rmap, permit, sequence 10
  Match clauses:
    ip address (access-lists): route-out
  Set clauses:
    metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show running-config route-map
route-map rmap permit 10
 match ip address route-out
 set metric 10000 60 100 1 1500
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에서 다음 홉이 있는 경로를 배포합니다.
match ip next-hop	지정된 액세스 목록 중 하나에 의해 전달되는 다음 홉 라우터 주소가 있는 모든 경로를 배포합니다.
route-map	라우팅 프로토콜 간에 경로를 재배포하는 조건을 정의합니다.

set metric(BGP, OSPF, RIP)

라우팅 프로토콜에 대한 메트릭 값을 설정하려면 route-map 컨피그레이션 모드에서 **set metric** 명령을 사용합니다. 기본 메트릭 값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

set metric *metric-value*

no set metric

구문 설명

metric-value	킬로비트/초 단위의 메트릭 값 또는 대역폭입니다(0~4294967295의 정수 값). 이 인수는 EIGRP(Enhanced Interior Gateway Routing Protocol)를 제외한 모든 라우팅 프로토콜에 적용됩니다.

기본값

동적으로 학습되는 메트릭 값입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

기본값을 변경하기 전에 Cisco 기술 지원 담당자에게 문의하는 것이 좋습니다.

route-map 글로벌 컨피그레이션 명령과 **match** 및 **set** route-map 컨피그레이션 명령을 사용하여 라우팅 프로토콜 간의 재배포 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연계된 **match** 및 **set** 명령 목록이 있습니다. **match** 명령은 *일치 조건*(현재 **route-map** 명령에 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 *설정 작업*(**match** 명령에서 적용하는 조건이 충족된 경우에 수행할 특정 재배포 작업)을 지정합니다. 또한 **no route-map** 명령은 경로 맵을 삭제합니다.

set route-map 컨피그레이션 명령은 경로 맵의 모든 일치 조건이 충족된 경우에 수행할 재배포 *설정 작업*을 지정합니다. 모든 일치 조건이 충족되면 모든 설정 작업이 수행됩니다.

예

다음 예에서는 라우팅 프로토콜에 대한 메트릭 값을 100으로 설정합니다.

```
ciscoasa(config-route-map)# route-map set-metric 100
ciscoasa(config-route-map)# set metric 100
```

set metric-type

OSPF 메트릭 경로 유형을 지정하려면 route-map 컨피그레이션 모드에서 **set metric-type** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

set metric-type{**type-1** | **type-2**}

no set metric-type

구문 설명

type-1	지정된 자동 시스템의 외부에 있는 OSPF 메트릭 경로의 유형을 지정합니다.
type-2	지정된 자동 시스템의 외부에 있는 OSPF 메트릭 경로의 유형을 지정합니다.

기본값

기본값은 **type-2**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

예

다음 예에서는 OSPF 라우팅에 대한 경로 맵을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# set metric-type type-2
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
ciscoasa(config-route-map)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에서 다음 홉이 있는 경로를 배포합니다.
route-map	라우팅 프로토콜 간에 경로를 재배포하는 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

set metric-type internal

외부 BGP(eBGP) 인접 라우터로 보급되는 접두사에서 MED(Multi Exit Discriminator) 값을 다음 홉의 IGP(Interior Gateway Protocol)와 일치하도록 설정하려면 route-map 컨피그레이션 모드에서 **set metric-type internal** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

set metric-type internal

no set metric-type internal

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 BGP에서 경로의 다음 홉과 연계된 IGP 메트릭에 해당하는 MED 값을 보급하도록 합니다. 이 명령은 생성된 내부 BGP(iBGP) 파생 경로 및 eBGP 파생 경로에 적용됩니다.

이 명령을 사용하면 일반 자동 시스템의 여러 BGP 스피커가 특정 접두사에 대한 서로 다른 MED 값을 보급할 수 있습니다. 또한 IGP 메트릭이 변경된 경우 BGP가 10분마다 경로를 다시 보급합니다.

route-map 글로벌 컨피그레이션 명령과 **match** 및 **set** route-map 컨피그레이션 명령을 사용하여 라우팅 프로토콜 간의 재배포 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연계된 **match** 및 **set** 명령 목록이 있습니다. **match** 명령은 *일치 조건*(현재 **route-map** 명령에 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 *설정 작업*(**match** 명령에서 적용하는 조건이 충족된 경우에 수행할 특정 재배포 작업)을 지정합니다. 또한 **no route-map** 명령은 경로 맵을 삭제합니다.

set route-map 컨피그레이션 명령은 경로 맵의 모든 일치 조건이 충족된 경우에 수행할 재배포 *설정 작업*을 지정합니다. 모든 일치 조건이 충족되면 모든 설정 작업이 수행됩니다.

참고 이 명령은 경로를 BGP(Border Gateway Protocol)로 재배포하는 경우에는 지원되지 않습니다.

예

다음 예에서는 인접 라우터 172.16.2.3으로 보급되는 모든 경로의 MED 값을 다음 홉의 해당 IGP 메트릭으로 설정합니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 172.16.0.0
ciscoasa(config-router-af)# neighbor 172.16.2.3 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.2.3 route-map setMED out
ciscoasa(config-route-map)# route-map setMED permit 10
ciscoasa(config-route-map)# match as-path as-path-acl
ciscoasa(config-route-map)# set metric-type internal
ciscoasa(config-route-map)# ip as-path access-list as-path-acl permit .*
```

set ip next-hop BGP

정책 라우팅에 대한 경로 맵의 match 절을 전달하는 패킷을 출력할 위치를 나타내려면 route-map 컨피그레이션 모드에서 **set ip next-hop** 명령을 사용합니다. 이 항목을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

set ip next-hop *ip-address* [*... ip-address*] [**peer-address]**

no set ip next-hop *ip-address* [*... ip-address*] **[peer-address]**

구문 설명

ip-address	패킷이 출력되는 다음 홉의 IP 주소입니다. 인접 라우터일 필요는 없습니다.
peer-address	(선택 사항) 다음 홉을 BGP 피어링 주소로 설정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

명령 구문에서 줄임표(...)는 명령 입력에 *ip-address* 인수의 여러 값을 포함할 수 있음을 나타냅니다.

ip policy route-map 인터페이스 컨피그레이션 명령, **route-map** 글로벌 컨피그레이션 명령, **match** 및 **set** route-map 컨피그레이션 명령을 사용하여 정책 라우팅 패킷에 대한 조건을 정의할 수 있습니다. **ip policy route-map** 명령은 경로 맵을 이름으로 식별합니다. 각 **route-map** 명령에는 연계된 **match** 및 **set** 명령 목록이 있습니다. **match** 명령은 *일치 조건*(정책 라우팅이 발생하는 조건)을 지정합니다. **set** 명령은 *설정 작업*(**match** 명령에서 적용하는 조건이 충족된 경우에 수행할 특정 라우팅 작업)을 지정합니다.

set next-hop 명령으로 지정된 첫 번째 다음 홉의 작동이 중지된 경우 선택적으로 지정된 IP 주소가 차례로 시도됩니다.

BGP 피어의 인바운드 경로 맵에서 **peer-address** 키워드와 함께 **set next-hop** 명령을 사용하면 수신된 일치하는 경로의 다음 홉이 인접 라우터 피어링 주소로 설정되어 모든 서드파티 다음 홉이 재정의됩니다. 따라서 동일한 경로 맵을 여러 BGP 피어에 적용하여 서드파티 다음 홉을 재정의할 수 있습니다.

BGP 피어의 아웃바운드 경로 맵에서 **peer-address** 키워드와 함께 **set next-hop** 명령을 사용하면 보급된 일치하는 경로의 다음 홉이 로컬 라우터의 피어링 주소로 설정되므로 다음 홉 계산이 비활성화됩니다. **set next-hop** 명령은 다른 경로는 그대로 두고 일부 경로의 다음 홉을 설정할 수 있기 때문에 인접 라우터별 **neighbor next-hop-self** 명령보다 세분성이 더 뛰어납니다. **neighbor next-hop-self** 명령은 해당 인접 라우터로 전송되는 모든 경로에 대한 다음 홉을 설정합니다.

set 절은 서로 함께 사용할 수 있으며, 다음 순서로 평가됩니다.

1. **set next-hop**
2. **set interface**
3. **set default next-hop**
4. **set default interface**

참고 반영된 경로에 대한 일반적인 컨피그레이션 오류를 방지하려면 BGP 경로 리플렉터 클라이언트에 적용할 경로 맵에서 **set next-hop** 명령을 사용하지 마십시오.

예

다음 예에는 세 개의 라우터가 동일한 LAN에 있습니다(각 IP 주소는 10.1.1.1, 10.1.1.2 및 10.1.1.3). 각 라우터는 서로 다른 자동 시스템에 있습니다. **set ip next-hop peer-address** 명령은 원격 자동 시스템 300의 라우터(10.1.1.3)에서 경로 맵과 일치하는 원격 자동 시스템 100의 라우터(10.1.1.1)에 대한 트래픽이 LAN에 대한 상호 연결을 통해 자동 시스템 100의 라우터(10.1.1.1)로 직접 전송되지 않고 라우터 bgp 200을 통과하도록 지정합니다.

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.1.1.3 remote-as 300
ciscoasa(config-router-af)# neighbor 10.1.1.3 route-map set-peer-address out
ciscoasa(config-router-af)# neighbor 10.1.1.1 remote-as 100
ciscoasa(config-route-af)# route-map set-peer-address permit 10
ciscoasa(config-route-map)# set ip next-hop peer-address
```

set origin(BGP)

BGP 원본 코드를 설정하려면 route-map 컨피그레이션 모드에서 **set origin** 명령을 사용합니다. 이 항목을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

no set origin {**igp** | **egp** *autonomous-system-number* | **incomplete**}

구문 설명

autonomous-system-number	원격 자동 시스템 번호입니다. 이 인수 값의 범위는 1에서 65535 사이의 자동 시스템 번호입니다.
egp	로컬 EGP(External Gateway Protocol) 시스템입니다.
igp	원격 IGP(Interior Gateway Protocol) 시스템입니다.
incomplete	알 수 없는 유산입니다.

기본값

경로의 원본은 주 IP 라우팅 테이블에 있는 경로의 경로 정보를 기반으로 합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

경로의 원본을 설정하려면 match 절이 있어야 합니다("모두 허용" 목록을 가리키는 경우도 포함). 이 명령을 사용하여 경로가 BGP로 재배포될 때 특정 원본을 설정할 수 있습니다. 경로가 재배포될 때 원본은 일반적으로 완료되지 않은 것으로 기록되며, 이는 BGP 테이블에서 ?로 식별됩니다.

route-map 글로벌 컨피그레이션 명령과 **match** 및 **set** route-map 컨피그레이션 명령을 사용하여 라우팅 프로토콜 간의 재배포 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연계된 **match** 및 **set** 명령 목록이 있습니다. **match** 명령은 *일치 조건*(현재 **route-map** 명령에 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 *설정 작업*(**match** 명령에서 적용하는 조건이 충족된 경우에 수행할 특정 재배포 작업)을 지정합니다. 또한 **no route-map** 명령은 경로 맵을 삭제합니다.

set route-map 컨피그레이션 명령은 경로 맵의 모든 일치 조건이 충족된 경우에 수행할 재배포 *설정 작업*을 지정합니다. 모든 일치 조건이 충족되면 모든 설정 작업이 수행됩니다.

예

다음 예에서는 경로 맵을 IGP로 전달하는 경로의 원본을 설정합니다.

```
ciscoasa(config-route-map)# route-map set_origin
ciscoasa(config-route-map)# match as-path 10
ciscoasa(config-route-map)# set origin igp
```

set weight

라우팅 테이블에 대한 BGP 가중치를 지정하려면 route-map 컨피그레이션 모드에서 **set weight** 명령을 사용합니다. 이 항목을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

set weight *number*

no set weight *number*

구문 설명

number	가중치 값입니다. 0~65535의 정수일 수 있습니다.

기본값

가중치는 지정된 경로 맵에 의해 변경되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
route-map 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

구현되는 가중치는 일치하는 첫 번째 자동 시스템 경로를 기반으로 합니다. 자동 시스템 경로가 일치하는 경우에 표시되는 가중치는 전역 **neighbor** 명령을 통해 할당되는 가중치를 재정의합니다. 즉, **set weight** route-map 컨피그레이션 명령을 통해 할당된 가중치가 **neighbor weight** 명령을 사용하여 할당된 가중치를 재정의합니다.

예

다음 예에서는 자동 시스템 경로 액세스 목록과 일치하는 경로의 BGP 가중치를 200으로 설정합니다.

```
ciscoasa(config-route-map)# route-map set-weight
ciscoasa(config-route-map)# match as-path as_path_acl
iscoasa(config-route-map)# set weight 200
```

setup

인터랙티브 프롬프트를 사용하여 ASA에 대한 최소 컨피그레이션을 설정하려면 글로벌 컨피그레이션 모드에서 **setup** 명령을 입력합니다.

setup

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.4(1)	ASA 5510 이상에 대한 라우팅 모드에서 구성된 인터페이스는 이제 "내부" 인터페이스가 아니라 관리 *슬롯/포트* 인터페이스입니다. ASA 5505의 경우 구성된 인터페이스는 "내부"가 아니라 VLAN 1 인터페이스입니다.
9.0(1)	기본 컨피그레이션 프롬프트가 변경되었으며, 설정 프로세스를 종료하는 Ctrl+Z가 활성화되었습니다.

사용 지침

설정 프롬프트는 플래시 메모리에 시작 컨피그레이션이 없는 경우 부팅 시 자동으로 표시됩니다.

setup 명령은 ASDM 연결을 설정하는 최소 컨피그레이션을 안내합니다. 이 명령은 컨피그레이션이 없거나 일부 컨피그레이션만 있는 디바이스용으로 설계되었습니다. 모델이 공장 기본 컨피그레이션을 지원하는 경우 **setup** 명령 대신 공장 기본 컨피그레이션을 사용하는 것이 좋습니다(기본 컨피그레이션을 복원하려면 **configure factory-default** 명령 사용).

setup 명령에는 "management"라는 이미 명명된 인터페이스가 필요합니다.

setup 명령을 입력하면 표 1-1의 정보를 묻는 프롬프트가 나타납니다. 나열된 파라미터에 대한 컨피그레이션이 이미 있는 경우에는 대괄호 안에 해당 컨피그레이션이 표시되므로 이를 기본값으로 적용하거나 새 값을 입력하여 재정의할 수 있습니다. 정확한 프롬프트는 모델에 따라 다를 수 있습니다. 시스템 **setup** 명령은 이러한 프롬프트의 하위 집합을 포함합니다.

표 1-1 설정 프롬프트

프롬프트	설명
`Pre-configure Firewall now through interactive prompts [yes]?`	**yes** 또는 **no**를 입력합니다. **yes**를 입력하면 설정이 계속됩니다. **no**를 입력하면 설정이 중지되고 글로벌 컨피그레이션 프롬프트(ciscoasa(config)#)가 표시됩니다.
`Firewall Mode [Routed]:`	**routed** 또는 **transparent**를 입력합니다.
`Enable password:`	enable 비밀번호를 입력합니다. 비밀번호는 3자 이상이어야 합니다.
`Allow password recovery [yes]?`	**yes** 또는 **no** 를 입력합니다 .
`Clock (UTC):`	이 필드에는 아무 것도 입력할 수 없습니다. UTC 시간이 기본적으로 사용됩니다.
`Year:`	네 자리 연도(예: 2005)를 입력합니다. 연도 범위는 1993~2035입니다.
`Month:`	이름 첫 세 자(예: 9월 경우 **Sep**)를 사용하여 월을 입력합니다.
`Day:`	날짜(1~31)를 입력합니다.
`Time:`	24시간 형식(예: 오후 8시 54분 44초의 경우 **20:54:44**)으로 시, 분, 초를 입력합니다.
`Host name:`	커맨드 라인 프롬프트에 표시할 호스트 이름을 입력합니다.
`Domain name:`	ASA가 실행되는 네트워크의 도메인 이름을 입력합니다.
`IP address of host running Device Manager:`	ASDM에 액세스하는 데 필요한 호스트의 IP 주소를 입력합니다.
`Use this configuration and save to flash (yes)?`	**yes** 또는 **no**를 입력합니다. **yes**를 입력하면 내부 인터페이스가 활성화되고 요청된 컨피그레이션이 플래시 파티션에 작성됩니다. **no**를 입력하면 설정 프롬프트가 첫 번째 질문부터 반복됩니다. `Pre-configure Firewall now through interactive prompts [yes]?` 설정을 종료하려면 **Ctrl + Z**를 입력하고 프롬프트를 반복하려면 **yes**를 입력합니다.

예

다음 예에서는 **setup** 명령을 완료하는 방법을 보여 줍니다.

```
ciscoasa(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1
```

```
The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

관련 명령

명령	설명
configure factory-default	기본 컨피그레이션을 복원합니다.

sfr

트래픽을 ASA FirePOWER 모듈로 리디렉션하려면 클래스 컨피그레이션 모드에서 **sfr** 명령을 사용합니다. 리디렉션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

sfr {**fail-close** | **fail-open**} [**monitor-only**]

no sfr {**fail-close** | **fail-open**} [**monitor-only**]

구문 설명

fail-close	모듈을 사용할 수 없는 경우 트래픽을 차단하도록 ASA를 설정합니다.
fail-open	모듈을 사용할 수 없는 경우 ASA 정책만 적용하여 트래픽 통과를 허용하도록 ASA를 설정합니다.
monitor-only	트래픽의 읽기 전용 복사본을 모듈로 보냅니다(즉, 패시브 모드). 키워드를 포함하지 않으면 트래픽이 인라인 모드로 전송됩니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

먼저 policy-map 명령을 입력하여 클래스 컨피그레이션 모드에 액세스할 수 있습니다.

ASA에서 **sfr** 명령을 구성하기 이전 또는 이후에 FireSIGHT Management Center를 사용하여 보안 정책을 구성합니다.

sfr 명령을 구성하려면 먼저 **class-map** 명령, **policy-map** 명령 및 **class** 명령을 구성해야 합니다.

트래픽 흐름

ASA FirePOWER 모듈은 ASA와 별개의 애플리케이션을 실행합니다. 그러나 이 모듈은 ASA 트래픽 흐름에 통합됩니다. ASA에서 트래픽 클래스에 대한 **sfr** 명령을 적용한 경우 트래픽은 다음과 같은 방식으로 ASA 및 모듈을 통과합니다.

1. 트래픽이 ASA로 들어갑니다.
2. 들어오는 VPN 트래픽의 암호가 해독됩니다.
3. 방화벽 정책이 적용됩니다.
4. 트래픽이 백플레인을 통해 ASA FirePOWER 모듈로 전송됩니다.

5. 모듈이 트래픽에 보안 정책을 적용하고 적절한 조치를 취합니다.
6. 인라인 모드에서 유효한 트래픽이 백플레인을 통해 ASA로 다시 전송됩니다. ASA FirePOWER 모듈은 해당 보안 정책에 따라 일부 트래픽을 차단할 수 있으며, 이 트래픽은 전달되지 않습니다. 패시브 모드에서는 아무 트래픽도 반환되지 않으므로 모듈에서 트래픽을 차단할 수 있습니다.
7. 나가는 VPN 트래픽이 암호화됩니다.
8. 트래픽이 ASA에서 나갑니다.

ASA 기능과의 호환성

ASA에는 HTTP 검사를 포함하여 다양한 고급 애플리케이션 검사 기능이 포함되어 있습니다. 그러나 ASA FirePOWER 모듈은 애플리케이션 사용 현황 모니터링 및 제어를 포함하여 다른 애플리케이션에 대한 추가 기능과 함께 ASA보다 더 고급 HTTP 검사 기능을 제공합니다.

ASA FirePOWER 모듈의 기능을 완벽하게 활용하려면 ASA FirePOWER 모듈로 보내는 트래픽에 대한 다음 지침을 참고하십시오.

- HTTP 트래픽에 대한 ASA 검사를 구성하지 마십시오.
- Cloud Web Security(ScanSafe)를 구성하지 마십시오. 동일한 트래픽에 대해 ASA FirePOWER 검사와 Cloud Web Security 검사를 둘 다 구성한 경우에는 ASA에서 ASA FirePOWER 검사만 수행합니다.
- ASA의 다른 애플리케이션 검사는 기본 검사를 포함하여 ASA FirePOWER 모듈과 호환됩니다.
- MUS(Mobile User Security) 서버를 활성화하지 마십시오. ASA FirePOWER 모듈과 호환되지 않습니다.
- 대체작동을 활성화한 경우 ASA가 대체작동되면 모든 기존 ASA FirePOWER 흐름이 새 ASA로 전송됩니다. 새 ASA의 ASA FirePOWER 모듈은 해당 시점부터 트래픽을 검사하기 시작합니다. 이전 검사 상태는 전송되지 않습니다.

모니터링 전용 모드

모니터링 전용 모드의 트래픽 흐름은 인라인 모드와 동일합니다. 유일한 차이점은 ASA FirePOWER 모듈은 트래픽을 ASA로 다시 전달하지 않는다는 점입니다. 대신, 보안 정책을 트래픽에 적용하여 인라인 모드에서 작동할 경우 수행되는 작업을 알려 줍니다. 예를 들어 트래픽이 이벤트에서 "would have dropped"로 표시될 수 있습니다. 트래픽 분석에 이 정보를 사용하여 인라인 모드가 바람직한지 결정할 수 있습니다.

참고 ASA에서 모니터링 전용 모드와 인라인 모드 둘 다를 동시에 구성할 수는 없습니다. 한 가지 유형의 보안 정책만 허용됩니다. 다중 상황 모드에서는 상황에 따라 모니터링 전용 모드 또는 일반 인라인 모드를 구성할 수 없습니다.

예 다음 예에서는 모든 HTTP 트래픽을 ASA FirePOWER 모듈로 전달하며, 이 모듈에서 장애가 발생한 경우 모든 HTTP 트래픽을 차단합니다.

```
ciscoasa(config)# access-list ASASFR permit tcp any any eq port 80
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list ASASFR
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-close
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

다음 예에서는 10.1.1.0 네트워크 및 10.2.1.0 네트워크를 대상으로 하는 모든 IP 트래픽을 ASA FirePOWER 모듈로 전달하며, 이 모듈에서 장애가 발생한 경우 모든 트래픽 통과를 허용합니다.

```
ciscoasa(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list my-sfr-acl
ciscoasa(config)# class-map my-sfr-class2
ciscoasa(config-cmap)# match access-list my-sfr-acl2
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap)# class my-sfr-class2
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)# service-policy my-sfr-policy interface outside
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
class-map	정책 맵에서 사용할 트래픽을 식별합니다.
hw-module module reload	모듈을 다시 로드합니다.
hw-module module reset	재설정을 수행한 다음 모듈을 다시 로드합니다.
hw-module module shutdown	모듈을 종료합니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
show asp table classify domain sfr	트래픽을 ASA FirePOWER 모듈로 전송하기 위해 생성된 NP 규칙을 표시합니다.
show module	모듈 상태를 표시합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.
show service-policy	서비스 정책 통계를 표시합니다.
sw-module module sfr reload	소프트웨어 모듈을 다시 로드합니다.
sw-module module sfr reset	소프트웨어 모듈을 재설정합니다.
sw-module module sfr recover	소프트웨어 모듈 부트 이미지를 설치합니다.
sw-module module sfr shutdown	소프트웨어 모듈을 종료합니다.

shape

QoS 트래픽 셰이핑을 활성화하려면 클래스 컨피그레이션 모드에서 **shape** 명령을 사용합니다. 고속 이더넷이 포함된 ASA와 같이 패킷을 고속으로 전송하는 디바이스가 있는 경우 이 디바이스를 케이블 모뎀과 같은 저속 디바이스에 연결하면 케이블 모뎀에서 병목 현상이 발생하여 패킷이 자주 삭제됩니다. 회선 속도가 서로 다른 네트워크를 관리하려면 고정된 느린 속도로 패킷을 전송하도록 ASA를 구성하면 됩니다. 이를 *트래픽 셰이핑*이라고 합니다. 이 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

참고 트래픽 셰이핑은 ASA 5505, 5510, 5520, 5540 및 5550에서만 지원됩니다. 멀티 코어 모델(예: ASA 5500-X)은 셰이핑을 지원하지 않습니다.

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

구문 설명

average *rate*	지정된 기간 동안의 평균 트래픽 속도(비트/초)를 설정합니다(64000~154400000). 8000의 배수 값을 지정합니다. 기간을 계산하는 방법에 대한 자세한 내용은 "사용 지침" 섹션을 참고하십시오.
burst_size	지정된 기간 동안 전송할 수 있는 평균 버스트 크기(비트)를 설정합니다(2048~154400000). 128의 배수 값을 지정합니다. *burst_size*를 지정하지 않은 경우 기본값은 지정된 평균 속도에서 4밀리초 트래픽으로 설정됩니다. 예를 들어 평균 속도가 1000000bps인 경우 4ms = 1000000 * 4/1000 = 4000입니다.

기본값

*burst_size*를 지정하지 않은 경우 기본값은 지정된 평균 속도에서 4밀리초 트래픽으로 설정됩니다. 예를 들어 평균 속도가 1000000bps인 경우 4ms = 1000000 * 4/1000 = 4000입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(4)/8.0(4)	이 명령이 도입되었습니다.

사용 지침

트래픽 셰이핑을 활성화하려면 MPF(Modular Policy Framework)를 사용합니다.

1. **policy-map** - **class-default** 클래스 맵과 연계된 작업을 식별합니다.
   a. **class class-default** - 작업을 수행할 **class-default** 클래스 맵을 식별합니다.
   b. **shape** - 클래스 맵에 트래픽 셰이핑을 적용합니다.
   c. (선택 사항) **service-policy** - 셰이핑된 트래픽의 하위 집합에 우선순위 대기열 처리를 적용할 수 있도록 **priority** 명령을 구성한 다른 정책 맵을 호출합니다.
2. **service-policy** - 하나의 인터페이스 또는 전역적으로 정책 맵을 할당합니다.

트래픽 셰이핑 개요

트래픽 셰이핑은 디바이스 및 링크 속도를 일치시켜 지터 및 지연을 일으킬 수 있는 패킷 손실, 가변 지연 및 링크 포화를 제어하는 데 사용됩니다.

- 물리적 인터페이스 또는 VLAN(ASA 5505의 경우)의 모든 나가는 트래픽에 트래픽 셰이핑을 적용해야 합니다. 특정 유형의 트래픽에 대한 트래픽 셰이핑을 구성할 수 없습니다.
- 트래픽 셰이핑은 패킷이 인터페이스에서 전송될 준비가 완료된 경우에 구현되므로 속도 계산은 IPsec 헤더 및 L2 헤더와 같은 가능한 모든 오버헤드를 포함하여 전송될 패킷의 실제 크기를 기반으로 수행됩니다.
- 셰이핑된 트래픽에는 through-the-box 트래픽과 from-the-box 트래픽이 모두 포함됩니다.
- 셰이핑 속도 계산은 표준 토큰 버킷 알고리즘을 기반으로 합니다. 토큰 버킷 크기는 버스트 크기 값의 두 배입니다. 토큰 버킷에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.
- 버스트 트래픽이 지정된 셰이핑 속도를 초과하는 경우에는 패킷이 대기열에 있다가 나중에 전송됩니다. 다음은 셰이핑 대기열에 대한 몇 가지 특성입니다(계층적 우선순위 대기열 처리에 대한 자세한 내용은 **priority** 명령 참고).
  - 대기열 크기는 셰이핑 속도를 기반으로 계산됩니다. 대기열은 1500바이트 패킷을 가정할 경우 200밀리초의 셰이핑 속도에 해당하는 트래픽을 유지할 수 있습니다. 최소 대기열 크기는 64입니다.
  - 대기열 제한에 도달하면 패킷이 종단 삭제(tail-drop)됩니다.
  - OSPF Hello 패킷과 같은 중요한 특정 연결 유지 패킷은 삭제되지 않습니다.
  - 시간 간격은 *time_interval* = *burst_size* / *average_rate*로 계산됩니다. 시간 간격이 클수록 셰이핑된 트래픽이 급증하고 링크 유휴 시간이 길어질 수 있습니다. 다음과 같은 과장된 예를 통해 효과를 가장 잘 이해할 수 있습니다.

    평균 속도 = 1000000

    버스트 크기 = 1000000

    위 예에서 시간 간격이 1초이면, 100Mbps FE 링크에서 1초 간격의 첫 번째 10밀리초 이내에 1Mbps의 트래픽이 버스트되고, 나머지 990밀리초는 다음 시간 간격까지 패킷을 보낼 수 없도록 유휴 상태로 유지됩니다. 따라서 음성 트래픽과 같은 지연에 민감한 트래픽이 있는 경우 평균 속도에 비해 버스트 크기를 줄여 시간 간격을 줄여야 합니다.

QoS 기능의 상호 작동 방식

각 QoS 기능은 ASA에 바람직한 경우에만 구성할 수 있습니다. 따라서 ASA에서 여러 QoS 기능을 구성할 수 있지만, 예를 들어 일부 트래픽의 우선순위를 지정하여 다른 트래픽이 대역폭 문제를 일으키지 않도록 할 수 있습니다.

인터페이스별로 지원되는 다음 기능 조합을 참고하십시오.

- 표준 우선순위 대기열 처리(특정 트래픽) + 정책 적용(나머지 트래픽)

  동일한 트래픽 집합에 대해 우선순위 대기열 처리와 정책 적용을 구성할 수 없습니다.
- 트래픽 셰이핑(인터페이스의 모든 트래픽) + 계층적 우선순위 대기열 처리(트래픽의 하위 집합)

동일한 인터페이스에 대해 트래픽 셰이핑과 표준 우선순위 대기열 처리를 구성할 수 없으며, 계층적 우선순위 대기열 처리만 허용됩니다. 예를 들어 전역 정책에 대해 표준 우선순위 대기열 처리를 구성한 다음 특정 인터페이스에 대해 트래픽 셰이핑을 구성한 경우 전역 정책이 인터페이스 정책을 중첩하므로 마지막에 구성한 기능은 거부됩니다.

트래픽 셰이핑을 활성화한 경우에는 동일한 트래픽에 대해 정책 적용을 활성화하지 않는 것이 일반적입니다(ASA에서 이 컨피그레이션을 제한하는 것은 아님).

예

다음 예에서는 외부 인터페이스의 모든 트래픽에 대한 트래픽 셰이핑을 활성화하고 VPN tunnel-grp1 내에서 DSCP 비트가 ef로 설정된 트래픽의 우선순위를 지정합니다.

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef

ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

ciscoasa(config-pmap-c)# service-policy shape_policy interface outside
```

관련 명령

명령	설명
class	정책 맵에서 작업을 수행할 클래스 맵을 식별합니다.
police	QoS 정책 적용을 활성화합니다.
policy-map	서비스 정책의 트래픽에 적용할 작업을 식별합니다.
priority	QoS 우선순위 대기열 처리를 활성화합니다.
service-policy(class)	계층적 정책 맵을 적용합니다.
service-policy(global)	인터페이스에 서비스 정책을 적용합니다.
show service-policy	QoS 통계를 표시합니다.

2 장

show aaa kerberos through show asdm sessions 명령

show aaa kerberos

ASA에서 캐시된 모든 Kerberos 티켓을 표시하려면 webvpn 컨피그레이션 모드에서 **show aaa kerberos** 명령을 사용합니다.

show aaa kerberos [**username** *user* | **host** *ip* | *hostname*]

구문 설명

host	보려는 특정 호스트를 지정합니다.
hostname	호스트 이름을 지정합니다.
ip	호스트의 IP 주소를 지정합니다.
username	보려는 특정 사용자를 지정합니다.

기본값

이 명령에는 기본값이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

사용 지침

webvpn 컨피그레이션 모드에서 **show aaa kerberos** 명령을 사용하여 ASA에서 캐시된 모든 Kerberos 티켓을 볼 수 있습니다. 특정 사용자 또는 호스트의 Kerberos 티켓을 보려면 **username** 및 **host** 키워드를 사용합니다.

예

다음 예에서는 **show aaa kerberos** 명령의 사용법을 보여 줍니다.

```
ciscoasa(config)# show aaa kerberos

Default Principal      Valid Starting Expires        Service Principal
kcduser@example.com    06/29/10 17:33:00 06/30/10 17:33:00 asa$/mycompany.com@example.com
kcduser@example.com    06/29/10 17:33:00 06/30/10 17:33:00
http/owa.mycompany.com@example.com
```

관련 명령

명령	설명
clear aaa kerberos	ASA에서 캐시된 모든 Kerberos 티켓을 지웁니다.
clear configure aaa-server	컨피그레이션에서 모든 AAA 명령문을 제거합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내의 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

show aaa local user

현재 잠긴 사용자 이름 목록을 표시하거나, 사용자 이름에 대한 세부사항을 표시하려면 글로벌 컨피그레이션 모드에서 show **aaa local user** 명령을 사용합니다.

show aaa local user [**locked**]

구문 설명

locked	(선택 사항) 현재 잠긴 사용자 이름 목록을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

선택적 키워드 **locked**를 생략하면 ASA에 모든 AAA 로컬 사용자에 대한 실패한 시도 및 잠금 상태 세부사항이 표시됩니다.

username 옵션을 사용하여 단일 사용자를 지정하거나 **all** 옵션을 사용하여 모든 사용자를 지정할 수 있습니다.

이 명령은 잠긴 사용자의 상태에만 영향을 줍니다.

관리자가 디바이스에서 잠글 수 없습니다.

예

다음 예에서는 **show aaa local user** 명령을 사용하여 모든 사용자 이름의 잠금 상태를 표시하는 방법을 보여 줍니다.

이 예에서는 **show aaa local user** 명령을 사용하여 제한이 5로 설정된 후 모든 AAA 로컬 사용자에 대한 실패한 인증 시도 횟수 및 잠금 상태 세부사항을 표시합니다.

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
    -                   2       N       mona
    -                   1       N       cisco
    -                   4       N       newuser
ciscoasa(config)#
```

이 예에서는 **lockout** 키워드와 함께 **show aaa local user** 명령을 사용하여 제한이 5로 설정된 후 모든 잠긴 AAA 사용자에 대한 실패한 인증 시도 횟수 및 잠금 상태 세부사항만 표시합니다.

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
ciscoasa(config)#
```

관련 명령

명령	설명
aaa local authentication attempts max-fail	사용자가 잠기기 전에 잘못된 비밀번호를 입력할 수 있는 최대 횟수를 구성합니다.
clear aaa local user fail-attempts	잠금 상태를 수정하지 않고 실패한 시도 횟수를 0으로 재설정합니다.
clear aaa local user lockout	지정된 사용자 또는 모든 사용자의 잠금 상태를 지우고 실패한 시도 횟수를 0으로 설정합니다.

show aaa-server

AAA 서버에 대한 AAA 서버 통계를 표시하려면 특권 EXEC 모드에서 **show aaa-server** 명령을 사용합니다.

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

구문 설명

LOCAL	(선택 사항) 로컬 사용자 데이터베이스에 대한 통계를 표시합니다.
groupname	(선택 사항) 그룹의 서버에 대한 통계를 표시합니다.
host *hostname*	(선택 사항) 그룹의 특정 서버에 대한 통계를 표시합니다.
protocol *protocol*	(선택 사항) 지정된 다음 프로토콜의 서버에 대한 통계를 표시합니다. • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

기본값

기본적으로 모든 AAA 서버 통계가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.1(1)	HTTP 형식 프로토콜이 추가되었습니다.
8.0(2)	**aaa-server active** 명령 또는 **fail** 명령을 사용하여 상태를 수동으로 변경한 경우에 서버 상태가 표시됩니다.

예

다음은 **show aaa-server** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

다음 표에는 **show aaa-server** 명령에 대한 필드 설명이 나와 있습니다.

필드	설명
Server Group	**aaa-server** 명령에 지정된 서버 그룹 이름입니다.
Server Protocol	**aaa-server** 명령에 지정된 서버 그룹의 서버 프로토콜입니다.
Server Address	AAA 서버의 IP 주소입니다.
Server port	ASA 및 AAA 서버에서 사용하는 통신 포트입니다. **authentication-port** 명령을 사용하여 RADIUS 인증 포트를 지정할 수 있습니다. **accounting-port** 명령을 사용하여 RADIUS 계정 관리 포트를 지정할 수 있습니다. 비 RADIUS 서버의 경우 포트는 **server-port** 명령을 통해 설정됩니다.
Server status	서버의 상태입니다. 다음 값 중 하나가 표시됩니다. • ACTIVE - ASA가 이 AAA 서버와 통신합니다. • FAILED - ASA가 AAA 서버와 통신할 수 없습니다. 이 상태의 서버는 구성된 정책에 따라 일정 기간 동안 이 상태로 유지된 후 다시 활성화됩니다. 상태 뒤에 “(admin initiated)”가 있으면 **aaa-server active** 명령 또는 **fail** 명령을 사용하여 서버를 수동으로 실패하게 만들거나 재활성화한 것입니다. 마지막 트랜잭션의 날짜 및 시간은 다음 형식으로 표시됩니다. **Last transaction ({success | failure}) at** *time timezone date* ASA가 서버와 통신한 적이 없는 경우에는 메시지가 다음과 같이 표시됩니다. **Last transaction at Unknown**
Number of pending requests	여전히 진행 중인 요청 수입니다.
Average round trip time	서버와의 트랜잭션을 완료하는 데 걸리는 평균 시간입니다.

필드	설명
Number of authentication requests	ASA에서 보낸 인증 요청 수입니다. 시간 초과 이후의 재전송은 이 값에 포함되지 않습니다.
Number of authorization requests	권한 부여 요청 수입니다. 이 값은 명령 권한 부여 또는 through-the-box 트래픽(TACACS+ 서버의 경우)으로 인한 권한 부여 요청이나 터널 그룹에 대해 활성화된 WebVPN 및 IPsec 권한 부여 기능에 대한 권한 부여 요청을 나타냅니다. 시간 초과 이후의 재전송은 이 값에 포함되지 않습니다.
Number of accounting requests	계정 관리 요청 수입니다. 시간 초과 이후의 재전송은 이 값에 포함되지 않습니다.
Number of retransmissions	내부 시간 초과 후 메시지가 재전송된 횟수입니다. 이 값은 Kerberos 및 RADIUS 서버(UDP)에만 적용됩니다.
Number of accepts	성공적인 인증 요청 수입니다.
Number of rejects	거부된 요청 수입니다. 이 값에는 오류 조건 및 AAA 서버의 실제 자격 증명 거부가 포함됩니다.
Number of challenges	AAA 서버가 초기 사용자 이름 및 비밀번호 정보를 받은 후 사용자에게 추가 정보를 요청한 횟수입니다.
Number of malformed responses	해당 없음. 이후 사용을 위해 예약되었습니다.
Number of bad authenticators	다음 중 하나가 발생한 횟수입니다. • RADIUS 패킷의 “authenticator” 문자열이 손상되었습니다(드문 경우). • ASA의 공유 비밀 키가 RADIUS 서버의 공유 비밀 키와 일치하지 않습니다. 이 문제를 해결하려면 올바른 서버 키를 입력하십시오. 이 값은 RADIUS에만 적용됩니다.
Number of timeouts	ASA에서 AAA 서버가 응답하지 않거나 잘못 동작하는 것을 감지하고 이 서버를 오프라인으로 선언한 횟수입니다.
Number of unrecognized responses	ASA가 AAA 서버로부터 인식할 수 없거나 지원하지 않는 응답을 받은 횟수입니다. 예를 들어 서버의 RADIUS 패킷 코드가 알 수 없는 유형이거나 알려진 유형(“access-accept”, “access-reject”, “access-challenge” 또는 “accounting-response”)과 다른 유형인 경우가 여기에 해당합니다. 일반적으로 이는 서버의 RADIUS 응답 패킷이 손상되었음을 의미하며, 이러한 경우는 드물게 발생합니다.

관련 명령

명령	설명
show running-config aaa-server	지정된 서버 그룹의 모든 서버 또는 특정 서버에 대한 통계를 표시합니다.
clear aaa-server statistics	AAA 서버 통계를 지웁니다.

show access-list

액세스 목록에 대한 적중 횟수 및 타임스탬프 값을 표시하려면 특권 EXEC 모드에서 **show access-list** 명령을 사용합니다.

show access-list *id_1* [...[*id_2*]] [**brief**]

구문 설명

brief	(선택 사항) 액세스 목록 식별자, 적중 횟수 및 마지막 규칙 적중의 타임스탬프를 모두 16진수 형식으로 표시합니다.
id_1	기존 액세스 목록을 식별하는 이름 또는 문자 집합입니다.
id_2	(선택 사항) 기존 액세스 목록을 식별하는 이름 또는 문자 집합입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	**brief** 키워드에 대한 지원이 도입되었습니다.
8.3(1)	ACL 타임스탬프를 표시하는 ACE 표시 패턴이 수정되었습니다.

사용 지침

하나의 명령에 액세스 목록 식별자를 입력하여 여러 액세스 목록을 한 번에 표시할 수 있습니다.

액세스 목록 적중 횟수, 식별자 및 타임스탬프 정보를 16진수 형식으로 표시하는 **brief** 키워드를 지정할 수 있습니다. 16진수 형식으로 표시되는 컨피그레이션 식별자는 세 열에 표시되며, syslog 106023 및 106100에서 사용되는 식별자와 동일합니다.

클러스터링 지침

ASA 클러스터링을 사용할 때 단일 디바이스에서 트래픽을 받은 경우 클러스터링 디렉터 논리로 인해 나머지 디바이스에서 ACL에 대한 적중 횟수를 계속 표시할 수 있습니다. 이는 예상된 동작입니다. 클라이언트에서 직접 패킷을 받지 않은 디바이스는 소유자 요청에 대해 클러스터 제어 링크를 통해 전달된 패킷을 받을 수 있기 때문에 수신 디바이스로 패킷을 다시 보내기 전에 ACL을 확인할 수 있습니다. 따라서 디바이스에서 트래픽을 전달하지 않은 경우에도 ACL 적중 횟수가 증가합니다.

예

다음 예에서는 16진수 형식으로 지정된 액세스 정책(적중 횟수가 0이 아닌 ACE)에 대한 간략한 정보를 보여 줍니다. 처음 두 열에는 16진수 형식의 식별자가 표시되고, 세 번째 열에는 적중 횟수가 나열되며, 네 번째 열에는 16진수 형식의 타임스탬프 값이 표시됩니다. 적중 횟수 값은 트래픽에 의해 규칙이 적중된 횟수를 나타냅니다. 타임스탬프 값은 마지막 적중 시간을 보고합니다. 적중 횟수가 0인 경우에는 아무 정보도 표시되지 않습니다.

다음은 **show access-list** 명령의 샘플 출력이며, "IN" 방향의 외부 인터페이스에 적용되는 "test"라는 액세스 목록을 보여 줍니다.

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq telnet (hitcnt=1) 0xca10ca21
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq ssh(hitcnt=1) 0x5b704158
```

다음은 **object-group-search** 그룹이 활성화되지 않은 경우 **show access-list** 명령의 샘플 출력입니다.

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group
BLK-LAN 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
14.14.14.0 255.255.255.0 (hitcnt=2) 0xce8596ec
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

다음은 **object-group-search** 그룹이 활성화된 경우 **show access-list** 명령의 샘플 출력입니다.

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

다음은 텔넷 트래픽 전달되는 경우 **show access-list brief** 명령의 샘플 출력입니다.

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
```

다음은 SSH 트래픽 전달되는 경우 **show access-list brief** 명령의 샘플 출력입니다.

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
5b704158 44ae5901 00000001 4a68aaa9
```

다음은 **show access-list** 명령의 샘플 출력이며, ACL 최적화가 활성화된 경우 "IN" 방향의 외부 인터페이스에 적용되는 "test"라는 액세스 목록을 보여 줍니다.

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1
object-group D1 0x44ae5901
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq
telnet (hitcnt=1) 0x7b1c1660
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq ssh
(hitcnt=1) 0x3666f922
```

다음은 텔넷 트래픽 전달되는 경우 **show access-list brief** 명령의 샘플 출력입니다.

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

다음은 SSH 트래픽 전달되는 경우 **show access-list brief** 명령의 샘플 출력입니다.

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

관련 명령

명령	설명
access-list ethertype	해당 EtherType에 따라 트래픽을 제어하는 액세스 목록을 구성합니다.
access-list extended	액세스 목록을 컨피그레이션에 추가하고, 방화벽을 통과하는 IP 트래픽에 대한 정책을 구성합니다.
clear access-list	액세스 목록 카운터를 지웁니다.
clear configure access-list	실행 중인 컨피그레이션에서 액세스 목록을 지웁니다.
show running-config access-list	현재 실행 중인 access-list 컨피그레이션을 표시합니다.

show activation-key

영구 라이센스, 활성 시간 기반 라이센스 및 실행 중인 라이센스(영구 라이센스와 활성 시간 기준 라이센스의 조합)를 표시하려면 특권 EXEC 모드에서 **show activation-key** 명령을 사용합니다. 대체작동 디바이스의 경우 이 명령은 기본 디바이스와 보조 디바이스의 조합된 키인 "대체작동 클러스터" 라이센스도 표시합니다.

show activation-key [detail]

구문 설명

detail	비활성 시간 기반 라이센스를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.0(4)	**detail** 키워드가 추가되었습니다.
8.2(1)	추가 라이센싱 정보를 포함하도록 출력이 수정되었습니다.
8.3(1)	이제 출력에 기능에서 영구 키를 사용할지 또는 시간 기반 키를 사용할지 여부 및 사용 중인 시간 기반 키의 기간이 포함됩니다. 또한 설치된 모든 시간 기반 키(활성 및 비활성)가 표시됩니다.
8.4(1)	No Payload Encryption 모델을 지원합니다.

사용 지침

일부 영구 라이센스의 경우 활성화한 후 ASA를 다시 로드해야 합니다. 표 2-1에 다시 로드해야 하는 라이센스가 나와 있습니다.

표 2-1 영구 라이센스 다시 로드 요건

모델	다시 로드해야 하는 라이센스 작업
모든 모델	암호화 라이센스 다운그레이드
ASAv	vCPU 라이센스 다운그레이드

다시 로드해야 하는 경우 **show activation-key** 출력은 다음과 같습니다.

```
The flash activation key is DIFFERENT from the running key.

The flash activation key takes effect after the next reload.
```

No Payload Encryption 모델이 있는 경우에는 라이센스를 볼 때 VPN 및 유니파이드 커뮤니케이션 라이센스가 나열되지 않습니다.

예

예 2-1 독립형 디바이스에 대한 show activation-key 명령 출력

다음은 독립형 디바이스에 대한 **show activation-key** 명령의 샘플 출력으로, 실행 중인 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)와 각 활성 시간 기반 라이센스를 보여 줍니다.

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

예 2-2 독립형 디바이스에 대한 show activation-key detail 명령 출력

다음은 독립형 디바이스에 대한 **show activation-key detail** 명령의 샘플 출력으로, 실행 중인 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)와 영구 라이센스 및 설치된 각 시간 기반 라이센스(활성 및 비활성)를 보여 줍니다.

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5505 Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days
```

```
Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

예 2-3 대체작동 쌍의 기본 디바이스에 대한 show activation-key detail 출력

다음은 기본 대체작동 디바이스에 대한 **show activation-key detail** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 기본 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "대체작동 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 기본 디바이스 영구 라이센스
- 기본 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성)

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
```

```
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2               perpetual
AnyConnect Essentials             : Disabled        perpetual
Other VPN Peers                   : 750             perpetual
Total VPN Peers                   : 750             perpetual
Shared License                    : Disabled         perpetual
AnyConnect for Mobile             : Disabled        perpetual
AnyConnect for Cisco VPN Phone    : Disabled        perpetual
Advanced Endpoint Assessment      : Disabled        perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                  : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

예 2-4 대체작동 쌍의 보조 디바이스에 대한 show activation-key detail 출력

다음은 보조 대체작동 디바이스에 대한 **show activation-key detail** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 보조 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "대체작동 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 보조 디바이스 영구 라이센스
- 보조 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성) 이 디바이스에는 시간 기반 라이센스가 없으므로 이 샘플 출력에는 none이 표시됩니다.

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
```

```
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

예 2-5 라이센스 없는 ASAv 에 대한 독립형 디바이스의 show activation-key 출력

배포된 vCPU ASAv 1개에 대한 다음 출력은 빈 액티베이션 키, 라이센스 없음 상태 및 vCPU 라이센스 1개 설치 메시지를 보여 줍니다.

참고 명령 출력에 “This platform has an ASAv VPN Premium license”가 표시됩니다. 이 메시지는 ASAv에서 페이로드 암호화를 수행할 수 있음을 지정합니다. ASAv Standard 및 Premium 라이센스를 나타내는 것은 아닙니다.

```
ciscoasa# show activation-key
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs                      : 0              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

예 2-6 vCPU Standard 라이센스 4 개가 있는 ASAv 에 대한 독립형 디바이스의 show activation-key 출력

참고 명령 출력에 “This platform has an ASAv VPN Premium license”가 표시됩니다. 이 메시지는 ASAv에서 페이로드 암호화를 수행할 수 있음을 지정합니다. ASAv Standard 및 Premium 라이센스를 나타내는 것은 아닙니다.

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
```

예 2-7 vCPU Premium 라이센스 4 개가 있는 ASAv 에 대한 독립형 디바이스의 show activation-key 출력

참고 명령 출력에 “This platform has an ASAv VPN Premium license”가 표시됩니다. 이 메시지는 ASAv에서 페이로드 암호화를 수행할 수 있음을 지정합니다. ASAv Standard 및 Premium 라이센스를 나타내는 것은 아닙니다.

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82

ASAv Platform License State: Compliant

Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
```

```
Maximum VLANs                   : 200           perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Standby perpetual
Encryption-DES                  : Enabled       perpetual
Encryption-3DES-AES             : Enabled       perpetual
Security Contexts               : 0             perpetual
GTP/GPRS                        : Enabled       perpetual
AnyConnect Premium Peers        : 750           perpetual
AnyConnect Essentials           : Disabled      perpetual
Other VPN Peers                 : 750           perpetual
Total VPN Peers                 : 750           perpetual
Shared License                  : Disabled      perpetual
AnyConnect for Mobile           : Enabled       perpetual
AnyConnect for Cisco VPN Phone  : Enabled       perpetual
Advanced Endpoint Assessment    : Enabled       perpetual
UC Phone Proxy Sessions         : 1000          perpetual
Total UC Proxy Sessions         : 1000          perpetual
Botnet Traffic Filter           : Enabled       perpetual
Intercompany Media Engine       : Enabled       perpetual
Cluster                         : Disabled      perpetual

This platform has an ASAv VPN Premium license.

The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

예 2-8 대체작동 쌍의 ASA 서비스 모듈에 대한 기본 디바이스의 show activation-key 출력

다음은 기본 대체작동 디바이스에 대한 **show activation-key** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 기본 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "대체작동 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 기본 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성)

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces              : 1024          perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active  perpetual
DES                             : Enabled       perpetual
3DES-AES                        : Enabled       perpetual
Security Contexts               : 25            perpetual
GTP/GPRS                        : Enabled       perpetual
Botnet Traffic Filter           : Enabled       330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces              : 1024          perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active  perpetual
```

```
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

예 2-9 대체작동 쌍의 ASA 서비스 모듈에 대한 보조 디바이스의 show activation-key 출력

다음은 보조 대체작동 디바이스에 대한 **show activation-key** 명령의 샘플 출력으로, 다음 항목이 표시됩니다.

- 보조 디바이스 라이센스(영구 라이센스와 시간 기반 라이센스의 조합)
- 기본 디바이스와 보조 디바이스의 라이센스가 조합된 "대체작동 클러스터" 라이센스. 이는 ASA에서 실제로 실행 중인 라이센스입니다. 기본 라이센스와 보조 라이센스의 조합을 반영하는 이 라이센스의 값은 굵게 표시됩니다.
- 보조 디바이스의 설치된 시간 기반 라이센스(활성 및 비활성) 이 디바이스에는 시간 기반 라이센스가 없으므로 이 샘플 출력에는 none이 표시됩니다.

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.
```

예 2-10 클러스터에 대한 show activation-key 출력

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 The flash permanent activation key is the SAME as the running permanent key.
```

관련 명령

명령	설명
activation-key	액티베이션 키를 변경합니다.

show ad-groups

Active Directory 서버에 나열된 그룹을 표시하려면 특권 EXEC 모드에서 **show ad-groups** 명령을 사용합니다.

show ad-groups *name* **[filter** *string***]**

구문 설명

name	쿼리할 Active Directory 서버 그룹의 이름입니다.
string	검색할 전체 또는 일부 그룹 이름을 지정하는 따옴표 내의 문자열입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.

사용 지침

show ad-groups 명령은 LDAP 프로토콜을 사용하여 그룹을 검색하는 Active Directory 서버에만 적용됩니다. 이 명령을 사용하여 동적 액세스 정책 AAA 선택 조건에 사용할 수 있는 AD 그룹을 표시할 수 있습니다.

LDAP 특성 유형이 LDAP인 경우 ASA가 서버의 응답을 기다리는 기본 시간은 10초입니다. aaa-server host 컨피그레이션 모드에서 **group-search-timeout** 명령을 사용하여 이 시간을 조정할 수 있습니다.

참고 Active Directory 서버에 많은 그룹이 있는 경우에는 서버가 응답 패킷에 포함할 수 있는 데이터 양에 대한 제한에 따라 **show ad-groups** 명령이 잘릴 수도 있습니다. 이 문제를 방지하려면 **filter** 옵션을 사용하여 서버에서 보고되는 그룹 수를 줄이십시오.

예

```
ciscoasa# show ad-groups LDAP-AD17
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     46
Account Operators
Administrators
APP-SSL-VPN CIO Users
Backup Operators
Cert Publishers
CERTSVC_DCOM_ACCESS
Cisco-Eng
DHCP Administrators
DHCP Users
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Doctors
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Employees
Engineering
Engineering1
Engineering2
Enterprise Admins
Group Policy Creator Owners
Guests
HelpServicesGroup
```

다음 예에서는 **filter** 옵션을 사용하는 동일한 명령을 보여 줍니다.

```
ciscoasa(config)# show ad-groups LDAP-AD17 filter "Eng"
.
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     4
Cisco-Eng
Engineering
Engineering1
Engineering2
```

관련 명령

명령	설명
ldap-group-base-dn	Active Directory 계층에서 서버가 동적 그룹 정책에서 사용되는 그룹의 검색을 시작할 수준을 지정합니다.
group-search-timeout	ASA가 그룹 목록에 대한 Active Directory 서버의 응답을 기다리는 시간을 조정합니다.

show admin-context

현재 관리 상황으로 할당된 상황 이름을 표시하려면 특권 EXEC 모드에서 **show admin-context** 명령을 사용합니다.

show admin-context

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show admin-context** 명령의 샘플 출력입니다. 다음 예에서는 플래시의 루트 디렉토리에 저장된 “admin”이라는 관리 상황을 보여 줍니다.

```
ciscoasa# show admin-context
Admin: admin flash:/admin.cfg
```

관련 명령

명령	설명
admin-context	관리 상황을 설정합니다.
changeto	상황 또는 시스템 실행 공간 간의 변경 사항입니다.
clear configure context	모든 상황을 제거합니다.
mode	상황 모드를 단일 모드 또는 다중 모드로 설정합니다.
show context	상황 목록(시스템 실행 공간) 또는 현재 상황에 대한 정보를 표시합니다.

show arp

ARP 테이블을 보려면 특권 EXEC 모드에서 **show arp** 명령을 사용합니다.

show arp

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(8)/7.2(4)/8.0(4)	표시할 동적 ARP 기간이 추가되었습니다.

사용 지침

화면 출력은 동적, 정적 및 프록시 ARP 항목이 표시됩니다. 동적 ARP 항목은 ARP 항목의 기간(초)을 포함합니다. 정적 ARP 항목은 기간 대신 대시(-)를 포함하며, 프록시 ARP 항목은 "별칭"을 나타냅니다.

예

다음은 **show arp** 명령의 샘플 출력입니다. 첫 번째 항목은 2초가 지난 동적 항목입니다. 두 번째 항목은 정적 항목이고, 세 번째 항목은 프록시 ARP의 항목입니다.

```
ciscoasa# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

관련 명령

명령	설명
arp	정적 ARP 항목을 추가합니다.
arp-inspection	투명 방화벽 모드에서 ARP 스푸핑을 방지하기 위해 ARP 패킷을 검사합니다.
clear arp statistics	ARP 통계를 지웁니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config arp	ARP의 현재 시간 제한 컨피그레이션을 표시합니다.

show arp-inspection

각 인터페이스에 대한 ARP 검사 설정을 보려면 특권 EXEC 모드에서 **show arp-inspection** 명령을 사용합니다.

show arp-inspection

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show arp-inspection** 명령의 샘플 출력입니다.

```
ciscoasa# show arp-inspection
interface               arp-inspection         miss
-----------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 열은 ARP 검사가 활성화된 경우 일치하지 않는 패킷에 대해 수행할 기본 작업(“flood” 또는 “no-flood”)을 표시합니다.

관련 명령

명령	설명
arp	정적 ARP 항목을 추가합니다.
arp-inspection	투명 방화벽 모드에서 ARP 스푸핑을 방지하기 위해 ARP 패킷을 검사합니다.
clear arp statistics	ARP 통계를 지웁니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config arp	ARP의 현재 시간 제한 컨피그레이션을 표시합니다.

show arp statistics

ARP 통계를 보려면 특권 EXEC 모드에서 show arp statistics 명령을 사용합니다.

show arp statistics

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show arp statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

표 2에 각 필드에 대한 설명이 나와 있습니다.

표 2-2 show arp statistics 필드

필드	설명
Number of ARP entries	ARP 테이블 항목의 총 개수입니다.
Dropped blocks in ARP	IP 주소를 해당 하드웨어 주소에 대해 확인하는 동안 삭제된 블록 수입니다.
Maximum queued blocks	IP 주소를 확인할 때까지 기다리는 동안 ARP 모듈에서 대기 중이었던 최대 블록 수입니다.

표 2-2 show arp statistics 필드(계속)

필드	설명
Queued blocks	ARP 모듈에서 현재 대기 중인 블록 수입니다.
Interface collision ARPs received	ASA 인터페이스와 동일한 IP 주소에서 모든 ASA 인터페이스에 수신된 ARP 패킷 수입니다.
ARP-defense gratuitous ARPs sent	ARP-Defense 메커니즘의 일부로 ASA에서 보낸 여분의 ARP 수입니다.
Total ARP retries	첫 번째 ARP 요청에 대한 응답에서 주소가 확인되지 않은 경우 ARP 모듈에서 보낸 총 ARP 요청 수입니다.
Unresolved hosts	ARP 모듈에서 ARP 요청을 여전히 전송 중인 확인되지 않은 호스트의 개수입니다.
Maximum unresolved hosts	마지막으로 지워졌거나 ASA가 부팅한 이후에 ARP 모듈에 있던 확인되지 않은 호스트의 최대 개수입니다.

관련 명령

명령	설명
arp-inspection	투명 방화벽 모드에서 ARP 스푸핑을 방지하기 위해 ARP 패킷을 검사합니다.
clear arp statistics	ARP 통계를 지우고 값을 0으로 재설정합니다.
show arp	ARP 테이블을 표시합니다.
show running-config arp	ARP의 현재 시간 제한 컨피그레이션을 표시합니다.

show asdm history

ASDM 기록 버퍼의 내용을 표시하려면 특권 EXEC 모드에서 **show asdm history** 명령을 사용합니다.

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

구문 설명

asdmclient	(선택 사항) ASDM 클라이언트에 맞게 형식이 지정된 ASDM 기록 데이터를 표시합니다.
feature *feature*	(선택 사항) 기록 표시를 지정된 기능으로 제한합니다. 다음은 *feature* 인수의 유효한 값입니다. • **all** - 모든 기능에 대한 기록을 표시합니다(기본값). • **blocks** - 시스템 버퍼에 대한 기록을 표시합니다. • **cpu** - CPU 사용에 대한 기록을 표시합니다. • **failover** - 대체작동에 대한 기록을 표시합니다. • **ids** - IDS에 대한 기록을 표시합니다. • **interface** *if_name* - 지정된 인터페이스에 대한 기록을 표시합니다. *if_name* 인수는 **nameif** 명령에 지정된 인터페이스의 이름입니다. • **memory** - 메모리 사용 기록을 표시합니다. • **perfmon** - 성능 기록을 표시합니다. • **sas** - 보안 연계에 대한 기록을 표시합니다. • **tunnels** - 터널에 대한 기록을 표시합니다. • **xlates** - 변환 슬롯 기록을 표시합니다.
snapshot	(선택 사항) 마지막 ASDM 기록 데이터 포인트만 표시합니다.
view *timeframe*	(선택 사항) 기록 표시를 지정된 기간으로 제한합니다. *timeframe* 인수의 유효한 값은 다음과 같습니다. • **all** - 기록 버퍼의 모든 내용을 표시합니다(기본값). • **12h** - 12시간 • **5d** - 5일 • **60m** - 60분 • **10m** - 10분

기본값

인수 또는 키워드를 지정하지 않으면 모든 기능에 대한 모든 기록 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 **show pdm history** 명령에서 **show asdm history** 명령으로 변경되었습니다.

사용 지침

show asdm history 명령은 ASDM 기록 버퍼의 내용을 표시합니다. ASDM 기록 정보를 보려면 먼저 **asdm history enable** 명령을 사용하여 ASDM 기록 추적을 활성화해야 합니다.

예

다음은 **show asdm history** 명령의 샘플 출력입니다. 이 명령은 지난 10분 동안 수집된 외부 인터페이스에 대한 데이터로 출력을 제한합니다.

```
ciscoasa# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
```

```
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
ciscoasa#
```

다음은 **show asdm history** 명령의 샘플 출력입니다. 이 명령은 위 예와 마찬가지로 지난 10분 동안 수집된 외부 인터페이스에 대한 데이터로 출력을 제한합니다. 그러나 이 예에서는 ASDM 클라이언트에 맞게 출력의 형식이 지정됩니다.

```
ciscoasa# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|6
2469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|6
2553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|6
2636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|6
2723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|25025|2
5026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091|25096|2
5102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|25161|25165|2
5169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|25367|25371|25375|2
5381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750|750
|750|750|750|750|750|750|750|750|750|750|750|751|751|751|751|751|751|751|751|751|751|751|7
51|751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|753|753|753|753
|753|753|753|753|753|753|753|
MH|OPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|55|55|55|55|55|55|55|55|55|55|5
5|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|5
5|55|55|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|3979|4
381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|4847|4292|5
401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|6309|5969|4472|
2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|4698
|5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3343|3349
|5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|3931|3298|33
49|5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6|9|5
|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|7|6|9|7|
6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|0|0|
1|1|0|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|1|28|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|IERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
```

```
MH|NB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|374874|374911|374943|374967|3750
10|375038|375073|375113|375140|375160|375181|375211|375243|375289|375316|375350|375373|375
395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|375738|375761|37
5794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115|376147|376168|3
76200|376224|376253|376289|376315|376365|376400|376436|376463|376508|376530|376553|376583|
376614|376668|376714|376749|
MH|RNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|GNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|CRC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|FRM|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCOLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|RST|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DEF|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|1
28|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|
MH|SIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|SOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
ciscoasa#
```

다음은 **snapshot** 키워드를 사용한 **show asdm history** 명령의 샘플 출력입니다.

```
ciscoasa# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
```

```
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
```

```
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
```

```
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPsec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
ciscoasa#
```

관련 명령

명령	설명
asdm history enable	ASDM 기록 추적을 활성화합니다.

show asdm image

현재 ASDM 소프트웨어 이미지 파일을 보려면 특권 EXEC 모드에서 **asdm image** 명령을 표시합니다.

show asdm image

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 **show pdm image** 명령에서 **show asdm image** 명령으로 변경되었습니다.

예

다음은 **show asdm image** 명령의 샘플 출력입니다.

```
ciscoasa# show asdm image

Device Manager image file, flash:/ASDM
```

관련 명령

명령	설명
asdm image	현재 ASDM 이미지 파일을 지정합니다.

show asdm log_sessions

활성 ASDM 로깅 세션 및 연계된 해당 세션 ID 목록을 표시하려면 특권 EXEC 모드에서 **show asdm log_sessions** 명령을 사용합니다.

show asdm log_sessions

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

각 활성 ASDM 세션에 하나 이상의 연계된 ASDM 로깅 세션이 있습니다. ASDM에서는 로깅 세션을 사용하여 ASA에서 syslog 메시지를 검색합니다. 각 ASDM 로깅 세션에는 고유한 세션 ID가 할당됩니다. **asdm disconnect log_session** 명령에서 이 세션 ID를 사용하여 지정된 세션을 종료할 수 있습니다.

참고 각 ASDM 세션에 하나 이상의 ASDM 로깅 세션이 있으므로 **show asdm sessions**와 **show asdm log_sessions**의 출력이 동일하게 표시될 수도 있습니다.

예

다음은 **show asdm log_sessions** 명령의 샘플 출력입니다.

```
ciscoasa# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

관련 명령

명령	설명
asdm disconnect log_session	활성 ASDM 로깅 세션을 종료합니다.

show asdm sessions

활성 ASDM 세션 및 연계된 해당 세션 ID 목록을 표시하려면 특권 EXEC 모드에서 **show asdm sessions** 명령을 사용합니다.

show asdm sessions

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 **show pdm sessions** 명령에서 **show asdm sessions** 명령으로 변경되었습니다.

사용 지침

각 활성 ASDM 세션에는 고유한 세션 ID가 할당됩니다. **asdm disconnect** 명령에서 이 세션 ID를 사용하여 지정된 세션을 종료할 수 있습니다.

예

다음은 **show asdm sessions** 명령의 샘플 출력입니다.

```
ciscoasa# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

관련 명령

명령	설명
asdm disconnect	활성 ASDM 세션을 종료합니다.

3 장

show as-path-access-list through show auto-update 명령

show as-path-access-list

모든 현재 AS(자동 시스템) 경로 액세스 목록의 내용을 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show as-path-access-list** 명령을 사용합니다.

show as-path-access-list [*name*]

구문 설명

name	(선택 사항) AS 경로 액세스 목록 이름을 지정합니다.

기본값

name 인수를 지정하지 않으면 모든 AS 경로 액세스 목록에 대한 명령 출력이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 **show as-path-access-list** 명령의 샘플 출력입니다.

```
ciscoasa# show as-path-access-list
AS path access list as-path-acl-1
    deny RTR$
AS path access list as-path-acl-2
    permit 100$
```

표 3-1에는 각 필드에 대한 설명이 나와 있습니다.

표 3-1 show as-path-access-list 필드

필드	설명
AS path access list	AS 경로 액세스 목록 이름을 나타냅니다.
deny	정규식을 경로의 AS 경로 표현과 일치시키는 데 실패한 이후에 거부된 패킷 수를 ASCII 문자열로 나타냅니다.
permit	정규식을 경로의 AS 경로 표현과 일치시킨 이후에 전달된 패킷 수를 ASCII 문자열로 나타냅니다.

show asp cluster counter

클러스터링 환경에서 전역 또는 상황별 정보를 디버깅하려면 특권 EXEC 모드에서 **show asp cluster counter** 명령을 사용합니다.

show asp cluster counter

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show asp cluster counter 명령은 문제 해결에 도움이 될 수 있는 전역 및 상황별 DP 카운터를 표시합니다. 이 정보는 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp cluster counter** 명령의 샘플 출력입니다.

```
ciscoasa# show asp cluster counter

Global dp-counters:

Context specific dp-counters:

MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

관련 명령

명령	설명
show asp drop	삭제된 패킷에 대한 가속화된 보안 경로 카운터를 표시합니다.

show asp drop

가속화된 보안 경로에 의해 삭제된 패킷 또는 연결을 디버깅하려면 특권 EXEC 모드에서 **show asp drop** 명령을 사용합니다.

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

구문 설명

flow [*flow_drop_reason*]	(선택 사항) 삭제된 흐름(연결)을 표시합니다. *flow_drop_reason* 인수를 사용하여 특정 사유를 지정할 수 있습니다. *flow_drop_reason* 인수의 유효한 값은 "사용 지침" 섹션에 나와 있습니다.
frame [*frame_drop_reason*]	(선택 사항) 삭제된 패킷을 표시합니다. *frame_drop_reason* 인수를 사용하여 특정 사유를 지정할 수 있습니다. *frame_drop_reason* 인수의 유효한 값은 "사용 지침" 섹션에 나와 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.0(8)/7.2(4)/8.0(4)	카운터가 마지막으로 지워진 시점을 나타내는 타임스탬프가 출력에 포함됩니다(**clear asp drop** 명령 참고). 또한 설명 옆에 삭제 사유 키워드가 표시되므로 연계된 키워드와 함께 **capture asp-drop** 명령을 쉽게 사용할 수 있습니다.

사용 지침

show asp drop 명령은 가속화된 보안 경로에 의해 삭제된 패킷 또는 연결을 표시하여 문제 해결을 도와줍니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이 정보는 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음 섹션에는 권장 사항을 포함하여 각 삭제 사유의 이름과 설명이 나와 있습니다.

- 3-5 페이지의 프레임 삭제 사유
- 3-64 페이지의 Flow Drop Reasons

프레임 삭제 사유

```
-------------------------------------------------------------------
Name: natt-keepalive
NAT-T keepalive message:
    This counter will increment when the appliance receives an IPsec NAT-T keepalive
message. NAT-T keepalive messages are sent from the IPsec peer to the appliance to keep
NAT/PAT flow information current in network devices between the NAT-T IPsec peer and the
appliance.

 Recommendation:
    If you have configured IPsec NAT-T on your appliance, this indication is normal and
doesn't indicate a problem. If NAT-T is not configured on your appliance, analyze your
network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


-------------------------------------------------------------------
Name: ipsecudp-keepalive
IPSEC/UDP keepalive message:
    This counter will increment when the appliance receives an IPsec over UDP keepalive
message. IPsec over UDP keepalive messages are sent from the IPsec peer to the appliance
to keep NAT/PAT flow information current in network devices between the IPsec over UDP
peer and the appliance. Note - These are not industry standard NAT-T keepalive messages
which are also carried over UDP and addressed to UDP port 4500.
 Recommendation:
    If you have configured IPsec over UDP on your appliance, this indication is normal and
doesn't indicate a problem. If IPsec over UDP is not configured on your appliance, analyze
your network traffic to determine the source of the IPsec over UDP traffic.

 Syslogs:
    None


-------------------------------------------------------------------
Name: bad-ipsec-prot
IPsec not AH or ESP:
    This counter will increment when the appliance receives a packet on an IPsec
connection which is not an AH or ESP protocol. This is not a normal condition.

 Recommendation:
    If you are receiving many IPsec not AH or ESP indications on your appliance, analyze
your network traffic to determine the source of the traffic.

 Syslogs:
    402115


-------------------------------------------------------------------
Name: ipsec-ipv6
IPsec via IPV6:
    This counter will increment when the appliance receives an IPsec ESP packet, IPsec
NAT-T ESP packet or an IPsec over UDP ESP packet encapsulated in an IP version 6 header.
The appliance does not currently support any IPsec sessions encapsulated in IP version 6.

 Recommendation:
    None

 Syslogs:
    None
```

```
----------------------------------------------------------------
Name: bad-ipsec-natt
Bad IPsec NATT packet:
    This counter will increment when the appliance receives a packet on an IPsec
connection which has negotiated NAT-T but the packet is not addressed to the NAT-T UDP
destination port of 4500 or had an invalid payload length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: bad-ipsec-udp
Bad IPsec UDP packet:
    This counter will increment when the appliance receives a packet on an IPsec
connection that has negotiated IPsec over UDP, but the packet has an invalid payload
length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


----------------------------------------------------------------
Name: inspect-srtp-encrypt-failed
Inspect SRTP Encryption failed:
    This counter will increment when SRTP encryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP encryption is
failing in the hardware crypto accelerator.

Syslogs:
    337001.


----------------------------------------------------------------
Name: inspect-srtp-decrypt-failed
Inspect SRTP Decryption failed:
    This counter will increment when SRTP decryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP decryption is
failing in the hardware crypto accelerator.

Syslogs:
    337002.


----------------------------------------------------------------
Name: inspect-srtp-validate-authtag-failed
Inspect SRTP Authentication tag validation failed:
    This counter will increment when SRTP authentication tag validation fails.

Recommendation:
    No action is required. If error persists SRTP packets arriving at the firewall are
being tampered with and the administrator has to identify the cause.

Syslogs:
```

```
    337003.


----------------------------------------------------------------
Name: inspect-srtp-generate-authtag-failed
Inspect SRTP Authentication tag generation failed:
    This counter will increment when SRTP authentication tag generation fails.

Recommendation:
    No action is required.

Syslogs:
    337004.


----------------------------------------------------------------
Name: inspect-srtp-no-output-flow
Inspect SRTP failed to find output flow:
    This counter will increment when the flow from the Phone proxy could not be created or
if the flow has been torn down

Recommendation:
    No action is required. The flow creation could have failed because of low memory
conditions.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-setup-srtp-failed
Inspect SRTP setup in CTM failed:
    This counter will increment when SRTP setup in the CTM fails.

Recommendation:
    No action is required. If error persists call TAC to see why the CTM calls are
failing.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-one-part-no-key
Inspect SRTP failed to find keys for both parties:
    This counter will increment when Inspect SRTP finds only one party's keys populated in
the media session.

Recommendation:
    No action is required. This counter could increment in the beginning phase of the call
but eventually when the call signaling exchange completes both parties should know their
respective keys.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-no-media-session
Inspect SRTP Media session lookup failed:
    This counter will increment when SRTP media session lookup fails.

Recommendation:
```

```
    No action is required. The media session is created by Inspect SIP or Skinny when the
IP address is parsed as part of the signaling exchange. Debug the signaling messages to
figure out the cause.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-no-remote-phone-proxy-ip
Inspect SRTP Remote Phone Proxy IP not populated:
    This counter will increment when remote phone proxy IP is not populated

Recommendation:
    No action is required. The remote phone proxy IP address is populated from the
signaling exchange. If error persists debug the signaling messages to figure out if ASA is
seeing all the signaling messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-client-port-not-present
Inspect SRTP client port wildcarded in media session:
    This counter will increment when client port is not populated in media session

Recommendation:
    No action is required. The client port is populated dynamically when the media stream
comes in from the client. Capture the media packets to see if the client is sending media
packets.

Syslogs:
    None.


----------------------------------------------------------------
Name: ipsec-need-sa
IPsec SA not negotiated yet:
    This counter will increment when the appliance receives a packet which requires
encryption but has no established IPsec security association. This is generally a normal
condition for LAN-to-LAN IPsec configurations. This indication will cause the appliance to
begin ISAKMP negotiations with the destination peer.

 Recommendation:
    If you have configured IPsec LAN-to-LAN on your appliance, this indication is normal
and doesn't indicate a problem. However, if this counter increments rapidly it may
indicate a crypto configuration error or network error preventing the ISAKMP negotiation
from completing. Verify that you can communicate with the destination peer and verify your
crypto configuration via the 'show running-config' command.

 Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-spoof
IsSec spoof detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not. The packet matched the inner header security policy check of a
configured and established IPsec connection on the appliance but was received unencrypted.
This is a security issue.

 Recommendation:
```

```
    Analyze your network traffic to determine the source of the spoofed IPsec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
Name: ipsec-clearpkt-notun
IPsec Clear Pkt w/no tunnel:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not. The packet matched the inner header security policy check of a
configured and established IPsec connection on the appliance but was received unencrypted.
This is a security issue.

 Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPsec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
Name: ipsec-tun-down
IPsec tunnel is down:
    This counter will increment when the appliance receives a packet associated with an
IPsec connection which is in the process of being deleted.

 Recommendation:
    This is a normal condition when the IPsec tunnel is torn down for any reason.

 Syslogs:
    None


----------------------------------------------------------------
Name: mp-svc-delete-in-progress
SVC Module received data while connection was being deleted:
    This counter will increment when the security appliance receives a packet associated
with an SVC connection that is in the process of being deleted.

Recommendation:
    This is a normal condition when the SVC connection is torn down for any reason. If
this error occurs repeatedly or in large numbers, it could indicate that clients are
having network connectivity issues.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-bad-framing
SVC Module received badly framed data:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software that it is unable to decode.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
```

```
Name: mp-svc-bad-length
SVC Module received bad data length:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software where the calculated and specified lengths do not match.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
Name: mp-svc-unknown-type
SVC Module received unknown data frame:
    This counter will increment when the security appliance receives a packet from an SVC
where the data type is unknown.

Recommendation:
    Validate that the SVC being used by the client is compatible with the version of
security appliance software.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-addr-renew-response
SVC Module received address renew response data frame:
    This counter will increment when the security appliance receives an Address Renew
Response message from an SVC. The SVC should not be sending this message.

Recommendation:
    This indicates that an SVC software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-prepend
SVC Module does not have enough space to insert header:
    This counter will increment when there is not enough space before the packet data to
prepend a MAC header in order to put the packet onto the network.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-channel
SVC Module does not have a channel for reinjection:
    This counter will increment when the interface that the encrypted data was received
upon cannot be found in order to inject the decrypted data.

Recommendation:
    If an interface is shut down during a connection, this could happen; re-enable/check
the interface. Otherwise, this indicates that a software error should be reported to the
Cisco TAC.
```

```
Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-session
SVC Module does not have a session:
    This counter will increment when the security appliance cannot determine the SVC
session that this data should be transmitted over.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-session-lock-failure
SVC Module failed to acquire the session lock:
    This counter will increment when the security appliance cannot grab the lock for the
SVC session that this data should be transmitted over.

Recommendation:
    This condition should never be encountered during normal operation and     may
indicate a software problem with the appliance.  Contact the Cisco Technical Assistance
Center (TAC) if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-decompres-error
SVC Module decompression error:
    This counter will increment when the security appliance encounters an error during
decompression of data from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-compress-error
SVC Module compression error:
    This counter will increment when the security appliance encounters an error during
compression of data to an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-no-mac
SVC Module unable to find L2 data for frame:
```

```
    This counter will increment when the security appliance is unable to find an L2 MAC
header for data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac
SVC Module found invalid L2 data in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
header attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac-len
SVC Module found invalid L2 data length in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
length attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-flow-control
SVC Session is in flow control:
    This counter will increment when the security appliance needs to drop data because an
SVC is temporarily not accepting any more data.

Recommendation:
    This indicates that the client is unable to accept more data. The client should reduce
the amount of traffic it is attempting to receive.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-fragment
SVC Module unable to fragment packet:
    This counter is incremented when a packet to be sent to the SVC is not permitted to be
fragmented or when there are not enough data buffers to fragment the packet.

Recommendation:
    Increase the MTU of the SVC to reduce fragmentation. Avoid using applications that do
not permit fragmentation. Decrease the load on the device to increase available data
buffers.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: vpn-handle-error
VPN Handle Error:
    This counter is incremented when the appliances is unable to create a VPN handle
because the VPN handle already exists.

 Recommendation:
    It is possible to see this counter increment as part of normal operation However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

 Syslogs:
    None.


----------------------------------------------------------------
Name: ipsec-lock-error
IPsec locking error:
    This counter is incremented when an IPsec operation is attempted but fails due to an
internal locking error.

Recommendation:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Technical Assistance Center (TAC)
if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: vpn-handle-mismatch
VPN Handle Mismatch:
    This counter is incremented when the appliance wants to forward a block and the flow
referred to by the VPN Handle is different than the flow associated with the block.

 Recommendation:
    This is not a normal occurrence. Please enter the show console-output command and
forward that output to CISCO TAC for further analysis.

 Syslogs:
    None.


----------------------------------------------------------------
Name: vpn-reclassify-failed
VPN Reclassify Failed:
    This counter is incremented when a packet for a VPN flow is dropped due to the flow
failing to be reclassified after a VPN state change.

 Recommendation:
    This counter is incremented when a packet for a VPN flow arrives that requires
reclassification due to VPN CLI or Tunnel state changes. If the flow no longer matches the
existing policies, then the flow is freed and the packet dropped.

 Syslogs:
    No new syslogs accompany this event.


----------------------------------------------------------------
Name: punt-rate-limit
Punt rate limit exceeded:
```

```
    This counter will increment when the appliance attempts to forward a layer-2 packet to
a rate-limited control point service routine and the rate limit (per/second) is now being
exceeded. Currently, the only layer-2 packets destined for a control point service routine
which are rate limited are ARP packets. The ARP packet rate limit is 500 ARPs per second
per interface.

Recommendation:
    Analyze your network traffic to determine the reason behind the high rate of ARP
packets.

 Syslogs:
    322002, 322003


----------------------------------------------------------------
Name: punt-no-mem
Punt no memory:
    This counter is incremented and the packet is dropped when there is no memory to
create data structure for punting a packet to Control Point.

Recommendation:
    No action needs to be taken if this condition is transient. If this condition persists
due to low memory, then system upgrade might be necessary.

Syslogs:
    None


----------------------------------------------------------------
Name: punt-queue-limit
Punt queue limit exceeded:
    This counter is incremented and the packet is dropped when punt queue limit is
exceeded, an indication that a bottle-neck is forming at Control Point.

Recommendation:
    No action needs to be taken. This is a design limitation.

Syslogs:
    None


----------------------------------------------------------------
Name: flow-being-freed
Flow is being freed:
    This counter is incremented when the flow is being freed and all packets queued for
inspection are dropped.

Recommendation:
    No action needs to be taken.

Syslogs:
    None


----------------------------------------------------------------
Name: invalid-encap
Invalid Encapsulation:
    This counter is incremented when the security appliance receives a frame belonging to
an unsupported link-level protocol or if the L3type specified in the frame is not
supported by the appliance. The packet is dropped.

Recommendation:
    Verify that directly connected hosts have proper link-level protocol settings.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ip-header
Invalid IP header:
    This counter is incremented and the packet is dropped when the appliance receives an
IP packet whose computed checksum of the IP header does not match the recorded checksum in
the header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a peer is sending corrupted packets and an attack is in progress. Please use the
packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: unsupported-ip-version
Unsupported IP version:
    This counter is incremented when the security appliance receives an IP packet that has
an unsupported version in version field of IP header. Specifically, if the packet does not
belong to version 4 or version 6. The packet is dropped.

Recommendation:
    Verify that other devices on connected network are configured to send IP packets
belonging to versions 4 or 6 only.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ip-length
Invalid IP Length:
    This counter is incremented when the security appliance receives an IPv4 or IPv6
packet in which the header length or total length fields in IP header are not valid or do
not conform to the received packet length.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ethertype
Invalid Ethertype:
    This counter is incremented when the fragmentation module on the security appliance
receives or tries to send a fragmented packet that does not belong IP version 4 or version
6. The packet is dropped.

Recommendation:
    Verify mtu of device and other devices on connected network to determine why the
device is processing such fragments.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: invalid-tcp-hdr-length
Invalid TCP Length:
    This counter is incremented when the security appliance receives a TCP packet whose
size is smaller than minimum-allowed header length or does not conform to the received
packet length.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.
Investigate the traffic from source in the following syslog.

Syslogs:
    500003.


----------------------------------------------------------------
Name: invalid-udp-length
Invalid UDP Length:
    This counter is incremented when the security appliance receives a UDP packet whose
size as calculated from the fields in header is different from the measured size of packet
as received from the network.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
    This counter is incremented when the security appliance has tried to obtain an
adjacency and could not obtain mac-address for next hop. The packet is dropped.

Recommendation:
    Configure a capture for this drop reason and check if a host with specified
destination address exists on connected network or is routable from the device.

Syslogs:
   None.


----------------------------------------------------------------
Name: unexpected-packet
Unexpected packet:
    This counter is incremented when the appliance in transparent mode receives a non-IP
packet, destined to its MAC address, but there is no corresponding service running on the
appliance to process the packet.

Recommendation:
    Verify if the appliance is under attack. If there are no suspicious packets, or the
device is not in transparent mode, this counter is most likely being incremented due to a
software error. Attempt to capture the traffic that is causing the counter to increment
and contact the Cisco TAC.

Syslogs:
    None


----------------------------------------------------------------
Name: no-route
No route to host:
```

```
    This counter is incremented when the security appliance tries to send a packet out of
an interface and does not find a route for it in routing table.

Recommendation:
    Verify that a route exists for the destination address obtained from the generated
syslog.

Syslogs:
   110002, 110003.


----------------------------------------------------------------
Name: rpf-violated
Reverse-path verify failed:
    This counter is incremented when ip-verify is configured on an interface and the
security appliance receives a packet for which the route lookup of source-ip did not yield
the same interface as the one on which the packet was received.

Recommendation:
    Trace the source of traffic based on source-ip printed in syslog below and investigate
why it is sending spoofed traffic.

Syslogs:
    106021.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by configured rule:
    This counter is incremented when a drop rule is hit by the packet and gets dropped.
This rule could be a default rule created when the box comes up, when various features are
turned on or off, when an acl is applied to interface or any other feature etc. Apart from
default rule drops, a packet could be dropped because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface

Recommendation:
    Note if one of ACLs listed below are fired.

Syslogs:
    106023, 106100, 106004


----------------------------------------------------------------
Name: unable-to-create-flow
Flow denied due to resource limitation:
    This counter is incremented and the packet is dropped when flow creation fails due to
a system resource limitation. The resource limit may be either:
       1) system memory
       2) packet block extension memory
       3) system connection limit
    Causes 1 and 2 will occur simultaneously with flow drop reason "No memory to complete
flow".

Recommendation:
    - Observe if free system memory is low.
    - Observe if flow drop reason "No memory to complete flow" occurs.
    - Observe if connection count reaches the system connection limit with the command
"show resource usage".

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: unable-to-add-flow
Flow hash full:
    This counter is incremented when a newly created flow is inserted into flow hash table
and the insertion failed because the hash table was full. The flow and the packet are
dropped. This is different from counter that gets incremented when maximum connection
limit is reached.

Recommendation:
    This message signifies lack of resources on the device to support an operation that
should have been successful. Please check if the connections in the 'show conn' output
have exceeded their configured idle timeout values. If so, contact the Cisco Technical
Assistance Center (TAC).

Syslogs:
    None.


----------------------------------------------------------------
Name: np-sp-invalid-spi
Invalid SPI:
    This counter will increment when the appliance receives an IPsec ESP packet addressed
to the appliance which specifies a SPI (security parameter index) not currently known by
the appliance.

 Recommendation:
    Occasional invalid SPI indications are common, especially during rekey processing.
Many invalid SPI indications may suggest a problem or DoS attack. If you are experiencing
a high rate of invalid SPI indications, analyze your network traffic to determine the
source of the ESP traffic.

 Syslogs:
    402114


----------------------------------------------------------------
Name: unsupport-ipv6-hdr
Unsupported IPv6 header:
    This counter is incremented and the packet is dropped if an IPv6 packet is received
with an unsupported IPv6 extension header. The supported IPv6 extension headers are: TCP,
UDP, ICMPv6, ESP, AH, Hop Options, Destination Options, and Fragment. The IPv6 routing
extension header is not supported, and any extension header not listed above is not
supported.  IPv6 ESP and AH headers are supported only if the packet is through-the-box.
To-the-box IPv6 ESP and AH packets are not supported and will be dropped.

Recommendation:
    This error may be due to a misconfigured host. If this error occurs repeatedly or in
large numbers, it could also indicate spurious or malicious activity such as an attempted
DoS attack.

Syslogs:
    None.


----------------------------------------------------------------
Name: tcp-not-syn
First TCP packet not SYN:
    Received a non SYN packet as the first packet of a non intercepted and non nailed
connection.

Recommendation:
```

```
    Under normal conditions, this may be seen when the appliance has already closed a
connection, and the client or server still believe the connection is open, and continue to
transmit data.  Some examples where this may occur is just after a 'clear local-host' or
'clear xlate' is issued. Also, if connections have not been recently removed, and the
counter is incrementing rapidly, the appliance may be under attack. Capture a sniffer
trace to help isolate the cause.

Syslogs:
    6106015


----------------------------------------------------------------
Name: bad-tcp-cksum
Bad TCP checksum:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet whose computed TCP checksum does not match the recorded checksum in TCP header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet. To allow
packets with incorrect TCP checksum disable checksum-verification feature under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: bad-tcp-flags
Bad TCP flags:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with invalid TCP flags in TCP header. Example a packet with SYN and FIN TCP
flags set will be dropped.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-reserved-set
TCP reserved flags set:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with reserved flags set in TCP header.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet. To allow such
TCP packets or clear reserved flags and then pass the packet use reserved-bits
configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-bad-option-list
TCP option list invalid:
```

```
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with a non-standard TCP header option.

Recommendations:
    To allow such TCP packets or clear non-standard TCP header options and then allow the
packet, use tcp-options configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-mss-exceeded
TCP data exceeded MSS:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with data length greater than the MSS advertised by peer TCP endpoint.

Recommendations:
    To allow such TCP packets use exceed-mss configuration under tcp-map

Syslogs:
    4419001


----------------------------------------------------------------
Name: tcp-synack-data
TCP SYNACK with data:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN-ACK packet with data.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-syn-data
TCP SYN with data:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN packet with data.

Recommendations:
    To allow such TCP packets use syn-data configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dual-open
TCP Dual open denied:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN packet from the server, when an embryonic TCP connection is already open.

Recommendations:
    None

Syslogs:
    None
```

```
------------------------------------------------------------------
Name: tcp-data-past-fin
TCP data send after FIN:
    This counter is incremented and the packet is dropped when the appliance receives new
TCP data packet from an endpoint which had sent a FIN to close the connection.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-3whs-failed
TCP failed 3 way handshake:
    This counter is incremented and the packet is dropped when appliance receives an
invalid TCP packet during three-way-handshake. Example SYN-ACK from client will be dropped
for this reason.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-rstfin-ooo
TCP RST/FIN out of order:
    This counter is incremented and the packet is dropped when appliance receives a RST or
a FIN packet with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-seq-syn-diff
TCP SEQ in SYN/SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a SYN or
SYN-ACK packet during three-way-handshake with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-ack-syn-diff
TCP ACK in SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a
SYN-ACK packet during three-way-handshake with incorrect TCP acknowledgement number.

Recommendations:
    None

Syslogs:
```

```
    None


----------------------------------------------------------------
Name: tcp-syn-ooo
TCP SYN on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-synack-ooo
TCP SYNACK on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN-ACK packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-seq-past-win
TCP packet SEQ past window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
data packet with sequence number beyond the window allowed by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-invalid-ack
TCP invalid ACK:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with acknowledgment number greater than data sent by peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-fo-drop
TCP replicated flow pak drop:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with control flag like SYN, FIN or RST on an established connection just after the
appliance has taken over as active unit.

Recommendations:
    None
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: tcp-discarded-ooo
TCP ACK in 3 way handshake invalid:
    This counter is incremented and the packet is dropped when appliance receives a TCP
ACK packet from client during three-way-handshake and the sequence number is not next
expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-full
TCP Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when appliance receives an
out-of-order TCP packet on a connection and there is no buffer space to store this packet.
Typically TCP packets are put into order on connections that are inspected by the
appliance or when packets are sent to SSM for inspection. There is a default queue size
and when packets in excess of this default queue size are received they will be dropped.

Recommendations:
    On ASA platforms the queue size could be increased using queue-limit configuration
under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-global-buffer-full
TCP global Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when the security appliance
receives an out-of-order TCP packet on a connection and there are no more global buffers
available. Typically TCP packets are put into order on connections that are inspected by
the security appliance or when packets are sent to the SSM for inspection. When the global
Out-of-Order buffer queue is full, the packet will be dropped and this counter will
increment.

Recommendations:
    This is a temporary condition when all global buffers are used. If this counter is
constantly incrementing, then please check your network for large amounts of Out-of-Order
traffic, which could be caused by traffic of the same flow taking different routes through
the network.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-timeout
TCP Out-of-Order packet buffer timeout:
    This counter is incremented and the packet is dropped when a queued out of order TCP
packet has been held in the buffer for too long.Typically, TCP packets are put into order
on connections that are inspected by the security appliance or when packets are sent to
the SSM for inspection. When the next expected TCP packet does not arrive within a certain
period, the queued out of order packet is dropped.
```

```
Recommendations:
    The next expected TCP packet may not arrive due to congestion in the network which is
normal in a busy network. The TCP retransmission mechanism in the end host will retransmit
the packet and the session will continue.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-rst-syn-in-win
TCP RST/SYN in window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN or TCP RST packet on an established connection with sequence number within window but
not next expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-acked
TCP DUP and has been ACKed:
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet and the data has been acknowledged by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dup-in-queue
TCP dup of packet in Out-of-Order queue:
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet that is already in our out of order packet queue.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-paws-fail
TCP packet failed PAWS test:
    This counter is incremented and the packet is dropped when TCP packet with timestamp
header option fails the PAWS (Protect Against Wrapped Sequences) test.

Recommendations:
    To allow such connections to proceed, use tcp-options configuration under tcp-map to
clear timestamp option.

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: tcp-conn-limit
TCP connection limit reached:
    This reason is given for dropping a TCP packet during TCP connection establishment
phase when the connection limit has been exceeded. The connection limit is configured via
the 'set connection conn-max' action command.

Recommendation:
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached. The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


----------------------------------------------------------------
Name: conn-limit
Connection limit reached:
    This reason is given for dropping a packet when the connection limit or host
connection limit has been exceeded. If this is a TCP packet which is dropped during TCP
connection establishment phase due to connection limit, the drop reason 'TCP connection
limit reached' is also reported.

Recommendation:
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached. The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


----------------------------------------------------------------
Name: tcp_xmit_partial
TCP retransmission partial:
    This counter is incremented and the packet is dropped when check-retransmission
feature is enabled and a partial TCP retransmission was received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This counter is incremented and the packet is dropped when check-retransmission
feature is enabled and a TCP retransmission with different data from the original packet
was received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
```

```
    This counter is incremented and the packet is dropped when window size advertised by
TCP endpoint is drastically changed without accepting that much data.

Recommendations:
    In order to allow such packet, use the window-variation configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: rate-exceeded
QoS rate exceeded:
    This counter is incremented when rate-limiting (policing) is configured on an
egress/ingress interface and the egress/ingress traffic rate exceeds the burst rate
configured. The counter is incremented for each packet dropped.

Recommendation:
    Investigate and determine why the rate of traffic leaving/entering the interface is
higher than the configured rate. This may be normal, or could be an indication of virus or
attempted attack.

Syslogs:
    None.


----------------------------------------------------------------
Name: queue-removed
Rate-limiter queued packet dropped:
    When QoS config is changed or removed, the existing packets in the output queues
awaiting transmission are dropped and this counter is incremented.

Recommendation:
    Under normal conditions, this may be seen when the QoS configuration has been changed
by the user. If this occurs when no changes to QoS config were performed, please contact
Cisco Technical Assistance Center (TAC).

Syslogs:
   None.


----------------------------------------------------------------
Name: bad-crypto
Bad crypto return in packet:
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails. This is not a normal condition and could
indicate possible software or hardware problems with the appliance

 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.
You should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors. You can also check the error counter in the global IPsec statistics with
the 'show ipsec stats' CLI command. If the IPsec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be useful in
diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: ctm-error
CTM returned error:
```

```
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails. This is not a normal condition and could
indicate possible software or hardware problems with the appliance.

 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.
You should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors. You can also check the error counter in the global IPsec statistics with
the 'show ipsec stats' CLI command. If the IPsec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be useful in
diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: send-ctm-error
Send to CTM returned error:
    This counter is obsolete in the appliance and should never increment.

 Recommendation:
    None

 Syslogs:
    None


----------------------------------------------------------------
Name: security-failed
Early security checks failed:
    This counter is incremented and packet is dropped when the security appliance :
    - receives an IPv4 multicast packet when the packets multicast MAC address doesn't
match the packets multicast destination IP address
    - receives an IPv6 or IPv4 teardrop fragment containing either small offset or
fragment overlapping
    - receives an IPv4 packet that matches an IP audit (IPS) signature

Recommendation:
    Contact the remote peer administrator or escalate this issue according to your
security policy
    For detailed description and syslogs for IP audit attack checks please refer the ip
audit signature section of command reference guide

Syslogs:
    106020
    400xx in case of ip audit checks


----------------------------------------------------------------
Name: sp-security-failed
Slowpath security checks failed:
    This counter is incremented and packet is dropped when the security appliance is:
    1) In routed mode receives a through-the-box:
       - L2 broadcast packet
       - IPv4 packet with destination IP address equal to 0.0.0.0
       - IPv4 packet with source IP address equal to 0.0.0.0
    2) In routed or transparent mode and receives a through-the-box IPv4 packet with:
       - first octet of the source IP address equal to zero
       - source IP address equal to the loopback IP address
       - network part of source IP address equal to all 0's
       - network part of source IP address equal to all 1's
       - source IP address host part equal to all 0's or all 1's
```

```
    3) In routed or transparent mode and receives an IPv4 or IPv6 packet with same source
and destination IP addresses

Recommendation:
    1 and 2) Determine if an external user is trying to compromise the protected network.
Check for misconfigured clients.
    3) If this message counter is incrementing rapidly, an attack may be in progress. Use
the packet capture feature to capture type asp packets, and check the source MAC address
in the packet to see where they are coming from.

Syslogs:
    1 and 2) 106016
    3) 106017


-------------------------------------------------------------------
Name: ipv6_sp-security-failed
IPv6 slowpath security checks failed:
    This counter is incremented and the packet is dropped for one of the following
reasons:
1) IPv6 through-the-box packet with identical source and destination address.
2) IPv6 through-the-box packet with linklocal source or destination address.
3) IPv6 through-the-box packet with multicast destination address.

Recommendation:
    These packets could indicate malicious activity, or could be the result of a
misconfigured IPv6 host.  Use the packet capture feature to capture type asp packets, and
use the source MAC address to identify the source.

Syslogs:
    For identical source and destination address, syslog 106016, else none.


-------------------------------------------------------------------
Name: invalid-ip-option
IP option drop:
    This counter is incremented when any unicast packet with ip options or a multicast
packet with ip-options that have not been configured to be accepted, is received by the
security appliance. The packet is dropped.

Recommendation:
    Investigate why a packet with ip options is being sent by the sender.

Syslogs:
    None.


-------------------------------------------------------------------
Name: lu-invalid-pkt
Invalid LU packet:
    Standby unit received a corrupted Logical Update packet.

Recommendation:
    The packet corruption could be caused by a bad cable, interface card, line noise, or
software defect. If the interface appears to be functioning properly, then report the
problem to Cisco TAC.

Syslogs:
    None


-------------------------------------------------------------------
Name: fo-standby
Dropped by standby unit:
```

```
    If a through-the-box packet arrives at an appliance or context in a Standby state and
a flow is created, the packet is dropped and the flow removed. This counter will increment
each time a packet is dropped in this manner.

Recommendation:
    This counter should never be incrementing on the Active appliance or context. However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: dst-l2_lookup-fail
Dst MAC L2 Lookup Failed:
    This counter will increment when the appliance is configured for transparent mode and
the appliance does a Layer 2 destination MAC address lookup which fails. Upon the lookup
failure, the appliance will begin the destination MAC discovery process and attempt to
find the location of the host via ARP and/or ICMP messages.

 Recommendation:
    This is a normal condition when the appliance is configured for transparent mode. You
can also execute (show mac-address-table) to list the L2 MAC address locations currently
discovered by the appliance.

 Syslogs:
    None


----------------------------------------------------------------
Name: l2_same-lan-port
L2 Src/Dst same LAN port:
    This counter will increment when the appliance/context is configured for transparent
mode and the appliance determines that the destination interface's L2 MAC address is the
same as its ingress interface.

 Recommendation:
    This is a normal condition when the appliance/context is configured for transparent
mode.  Since the appliance interface is operating in promiscuous mode, the
appliance/context receives all packets on the local LAN seqment.

 Syslogs:
    None


----------------------------------------------------------------
Name: flow-expired
Expired flow:
    This counter is incremented when the security appliance tries to inject a new or
cached packet belonging to a flow that has already expired.It is also incremented when the
appliance attempts to send an rst on a tcp flow that has already expired or when a packet
returns from IDS blade but the flow had already expired. The packet is dropped

Recommendation:
    If valid applications are getting pre-empted, investigate if a longer timeout is
needed.

Syslogs:
   None.


----------------------------------------------------------------
Name: inspect-icmp-out-of-app-id
ICMP Inspect out of App ID:
```

```
    This counter will increment when the ICMP inspection engine fails to allocate an 'App
ID' data structure. The structure is used to store the sequence number of the ICMP packet.

Recommendation:
    Check the system memory usage. This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmp-bad-code
ICMP Inspect bad icmp code:
    This counter will increment when the ICMP code in the ICMP echo request or reply
message is non-zero.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313009.


----------------------------------------------------------------
Name: inspect-icmp-seq-num-not-matched
ICMP Inspect seq num not matched:
    This counter will increment when the sequence number in the ICMP echo reply message
does not match any ICMP echo message that passed across the appliance earlier on the same
connection.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004


----------------------------------------------------------------
Name: inspect-icmp-error-no-existing-conn
ICMP Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMP error message.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-error-nat64-error
ICMP NAT64 Error Inspect XLATE Error:
    This counter will increment when the appliance is unable to translate ICMP error
messages between IPv6 and IPv4.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.
```

```
Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-nat64-frag
ICMP NAT64 Inspect Fragmentation Error:
    This counter will increment when the appliance is unable to translate ICMP messages
between IPv6 and IPv4 due to fragmentation.  Per RFC-6145, ICMP packet fragments will not
be translated.

Recommendation:
    No action required.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-error-different-embedded-conn
ICMP Error Inspect different embedded conn:
    This counter will increment when the frame embedded in the ICMP error message does not
match the established connection that has been identified when the ICMP connection is
created.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmpv6-error-invalid-pak
ICMPv6 Error Inspect invalid packet:
    This counter will increment when the appliance detects an invalid frame embedded in
the ICMPv6 packet. This check is the same as that on IPv6 packets. Examples: Incomplete
IPv6 header; malformed IPv6 Next Header; etc.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmpv6-error-no-existing-conn
ICMPv6 Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMPv6 error message.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-dns-invalid-pak
DNS Inspect invalid packet:
```

```
    This counter will increment when the appliance detects an invalid DNS packet.
Examples: A DNS packet with no DNS header; the number of DNS resource records not matching
the counter in the header; etc.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-invalid-domain-label
DNS Inspect invalid domain label:
    This counter will increment when the appliance detects an invalid DNS domain name or
label. DNS domain name and label is checked per RFC 1035.

Recommendation:
    No action required. If the domain name and label check is not desired, disable the
protocol-enforcement parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-pak-too-long
DNS Inspect packet too long:
    This counter is incremented when the length of the DNS message exceeds the configured
maximum allowed value.

Recommendation:
    No action required.  If DNS message length checking is not desired, enable DNS
inspection without the 'maximum-length' option, or disable the 'message-length maximum'
parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    410001


----------------------------------------------------------------
Name: inspect-dns-out-of-app-id
DNS Inspect out of App ID:
    This counter will increment when the DNS inspection engine fails to allocate a data
structure to store the identification of the DNS message.
Recommendation:
    Check the system memory usage. This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-id-not-matched
DNS Inspect ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
```

```
    None.


----------------------------------------------------------------
Name: dns-guard-out-of-app-id
DNS Guard out of App ID:
    This counter will increment when the DNS Guard function fails to allocate a data
structure to store the identification of the DNS message.

Recommendation:
    Check the system memory usage. This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: dns-guard-id-not-matched
DNS Guard ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.
This counter will increment by the DNS Guard function.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-length
Invalid RTP Packet length:
    This counter will increment when the UDP packet length is less than the size of the
RTP header.

Recommendation:
    No action required. A capture can be used to figure out which RTP source is sending
the incorrect packets and you can deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-version
Invalid RTP Version field:
    This counter will increment when the RTP version field contains a version other than
2.

Recommendation:
    The RTP source in your network does not seem to be sending RTP packets conformant with
the RFC 1889. The reason for this has to be identified and you can deny the host using
ACLs if required.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-invalid-payload-type
Invalid RTP Payload type field:
```

```
    This counter will increment when the RTP payload type field does not contain an audio
payload type when the signalling channel negotiated an audio media type for this RTP
secondary connection. The counter increments similarly for the video payload type.

Recommendation:
    The RTP source in your network is using the audio RTP secondary connection to send
video  or vice versa. If you wish to prevent this you can deny the host using ACLs.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-ssrc-mismatch
Invalid RTP Synchronization Source field:
    This counter will increment when the RTP SSRC field in the packet does not match the
SSRC which the inspect has been seeing from this RTP source in all the RTP packets.

Recommendation:
    This could be because the RTP source in your network is rebooting and hence changing
the SSRC or it could be because of another host on your network trying to use the opened
secondary RTP connections on the firewall to send RTP packets. This should be investigated
further to confirm if there is a problem.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-sequence-num-outofrange
RTP Sequence number out of range:
    This counter will increment when the RTP sequence number in the packet is not in the
range expected by the inspect.

Recommendation:
    No action is required because the inspect tries to recover and start tracking from a
new sequence number after a lapse in the sequence numbers from the RTP source.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-max-outofseq-paks-probation
RTP out of sequence packets in probation period:
    This counter will increment when the out of sequence packets when the RTP source is
being validated exceeds 20. During the probation period, the inspect looks for 5
in-sequence packets to consider the source validated.

Recommendation:
    Check the RTP source to see why the first few packets do not come in sequence and
correct it.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-length
Invalid RTCP Packet length:
    This counter will increment when the UDP packet length is less than the size of the
RTCP header.

Recommendation:
```

```
    No action required. A capture can be used to figure out which RTP source is sending
the incorrect packets and you can deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-version
Invalid RTCP Version field:
    This counter will increment when the RTCP version field contains a version other than
2.

Recommendation:
    The RTP source in your network does not seem to be sending RTCP packets conformant
with the RFC 1889. The reason for this has to be identified and you can deny the host
using ACLs if required.

Syslogs:
    431002.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-payload-type
Invalid RTCP Payload type field:
    This counter will increment when the RTCP payload type field does not contain the
values 200 to 204.

Recommendation:
    The RTP source should be validated to see why it is sending payload types outside of
the range recommended by the RFC 1889.

Syslogs:
    431002.


----------------------------------------------------------------
Name: cxsc-request
Flow terminated by CXSC:
This reason is given for terminating a flow as requested by CXSC module. Recommendations:
Check syslogs and alerts on CXSC module.
Syslogs: 429002


----------------------------------------------------------------
Name: cxsc-fail
CXSC config removed for connection:
    This counter is incremented and the packet is dropped when CXSC configuration is not
found for a particular connection.

Recommendations:
   check if any configuration changes have been done for CXSC.

Syslogs:
   None


----------------------------------------------------------------
Name: cxsc-fail-close
CXSC fail-close:
    This reason is given for terminating a flow since CXSC card is down and fail-close
option was used with CXSC action.

Recommendations:
```

```
    Check and bring up CXSC card.

Syslogs:
    429001


----------------------------------------------------------------
Name: cxsc-bad-tlv-received
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by CXSC module when
the packet has bad TLV's.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-ha-request
CXSC HA replication drop:
    This counter is incremented when the security appliance receives a CXSC HA request
packet, but could not process it and the packet is dropped.

Recommendation:
    This could happen occasionally when CXSC does not have the latest ASA HA state, like
right after ASA HA state change. If the counter is constantly increasing however, then it
can be because CXSC and ASA are out of sync. If that happens, contact Cisco TAC for
assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-invalid-encap
CXSC invalid header drop:
    This counter is incremented when the security appliance receives a CXSC packet with
invalid messsage header, and the packet is dropped.

Recommendation:
    This should not happen. Contact Cisco TAC for assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-malformed-packet
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by CXSC module when
the packet is malformed.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: ips-request
IPS Module requested drop:
```

```
    This counter is incremented and the packet is dropped as requested by IPS module when
the packet matches a signature on the IPS engine.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002


----------------------------------------------------------------
Name: ips-fail-close
IPS card is down:
    This counter is incremented and the packet is dropped when IPS card is down and
fail-close option was used in IPS inspection.

Recommendations:
    Check and bring up the IPS card.

Syslogs:
    420001


----------------------------------------------------------------
Name: ips-fail
IPS config removed for connection:
    This counter is incremented and the packet is dropped when IPS configuration is not
found for a particular connection.

Recommendations:
   check if any configuration changes have been done for IPS.

Syslogs:
   None


----------------------------------------------------------------
Name: ips-no-ipv6
Executing IPS software does not support IPv6:
    This counter is incremented when an IPv6 packet, configured to be directed toward IPS
SSM, is discarded since the software executing on IPS SSM card does not support IPv6.

Recommendations:
   Upgrade the IPS software to version 6.2 or later.

Syslogs:
   None


----------------------------------------------------------------
Name: l2_acl
FP L2 rule drop:
    This counter will increment when the appliance denies a packet due to a layer-2 ACL.
By default, in routed mode the appliance will PERMIT:
    1) IPv4 packets
    2) IPv6 packets
    3) ARP packets
    4) L2 Destination MAC of FFFF:FFFF:FFFF (broadcast)
    5) IPv4 MCAST packet with destination L2 of 0100:5E00:0000-0100:5EFE:FFFF
    6) IPv6 MCAST packet with destination L2 of 3333:0000:0000-3333:FFFF:FFFF

    By default, in Transparent mode permits the routed mode ACL and PERMITS:

    1) BPDU packets with destination L2 of 0100:0CCC:CCCD
```

```
    2) Appletalk packets with destination L2 of 0900:0700:0000-0900:07FF:FFFF

    The user can also configure ethertype ACL(s) and apply them to an interface to permit
other types of L2 traffic.

    The default L2 ACL can be seen in routed and transparent mode with the show asp table
classify domain permit command.

    Note - Packets permitted by L2 ACLs may still be dropped by L3-L4 ACLs.

 Recommendation:
    If your running the appliance/context in transparent mode and your non-IP packets are
dropped by the appliance, you can configure an ethertype ACL and apply the ACL to an
access group. Note - the appliance ethertype CLI only supports protocol types and not L2
destination MAC addresses.

 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: intercept-unexpected
Intercept unexpected packet:
    Either received data from client while waiting for SYNACK from server or received a
packet which cannot be handled in a particular state of TCP intercept.

Recommendation:
    If this drop is causing the connection to fail, please have a sniffer trace of the
client and server side of the connection while reporting the issue. The box could be under
attack and the sniffer traces or capture would help narrowing down the culprit.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-mcast-entry
FP no mcast entry:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    A multicast entry change has been detected after a packet was punted to the CP, and
the NP can no longer forward the packet since no entry is present.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: no-mcast-intrf
FP no mcast output intrf:
    All output interfaces have been removed from the multicast entry.
    - OR -
    The multicast packet could not be forwarded.

Recommendation:
    Verify that there are no longer any receivers for this group.
    - OR -
    Verify that a flow exists for this packet.
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: fragment-reassembly-failed
Fragment reassembly failed:
    This counter is incremented when the appliance fails to reassemble a chain of
fragmented packets into a single packet. All the fragment packets in the chain are
dropped. This is most probably because of failure while allocating memory for the
reassembled packet.

Recommendation:
    Use the show blocks command to monitor the current block memory.

Syslogs:
    None


----------------------------------------------------------------
Name: ifc-classify
Virtual firewall classification failed:
    A packet arrived on a shared interface, but failed to classify to any specific context
interface.

Recommendation:
    For software versions without customizable mac-address support, use the "global" or
"static" command to specify the IPv4 addresses that belong to each context interface.  For
software versions with customizable mac-address support, enable "mac-address auto" in
system context.  Alternatively, configure unique MAC addresses for each context interfaces
residing over a shared interface with "mac-address" command under each context interface
submode.

Syslogs:
    None.


----------------------------------------------------------------
Name: connection-lock
Connection locking failed:
    While the packet was waiting for processing, the flow that would be usedwas destroyed.

Recommendation:
    The message could occur from user interface command to remove connection in an device
that is actively processing packet.  Otherwise, investigate flow drop counter.  This
message may occur if the flow are forced dropped from error.

Syslogs:
    None.


----------------------------------------------------------------
Name: interface-down
Interface is down:
    This counter will increment for each packet received on an interface that is shutdown
via the 'shutdown' interface sub-mode command. For ingress traffic, the packet is dropped
after security context classification and if the interface associated with the context is
shut down. For egress traffic, the packet is dropped when the egress interface is shut
down.

Recommendation:
    No action required.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-app-length
Invalid App length:
    This counter will increment when the appliance detects an invalid length of the Layer
7 payload in the packet. Currently, it counts the drops by the DNS Guard function only.
Example: Incomplete DNS header.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: loopback-buffer-full
Loopback buffer full:
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared interface and there is no
buffer space in loopback queue.

Recommendations:
    Check system CPU to make sure it is not overloaded.

Syslogs:
    None


----------------------------------------------------------------
Name: non-ip-pkt-in-routed-mode
Non-IP packet received in routed mode:
    This counter will increment when the appliance receives a packet which is not IPv4,
IPv6 or ARP and the appliance/context is configured for routed mode. In normal operation
such packets should be dropped by the default L2 ACL configuration.

 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: host-move-pkt
FP host move packet:
    This counter will increment when the appliance/context is configured for transparent
and source interface of a known L2 MAC address is detected on a different interface.

 Recommendation:
    This indicates that a host has been moved from one interface (i.e. LAN segment) to
another. This condition is normal while in transparent mode if the host has in fact been
moved. However, if the host move toggles back and forth between interfaces, a network loop
may be present.

 Syslogs:
    412001, 412002, 322001


----------------------------------------------------------------
Name: tfw-no-mgmt-ip-config
```

```
No management IP address configured for TFW:
    This counter is incremented when the security appliance receives an IP packet in
transparent mode and has no management IP address defined. The packet is dropped.

Recommendation:
    Configure the device with management IP address and mask values.

Syslogs:
    322004


----------------------------------------------------------------
Name: shunned
Packet shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.

Recommendation:
    No action required.

Syslogs:
    401004


----------------------------------------------------------------
Name: rm-conn-limit
RM connection limit reached:
    This counter is incremented when the maximum number of connections for a context or
the system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-conn-rate-limit
RM connection rate limit reached:
    This counter is incremented when the maximum connection rate for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002


----------------------------------------------------------------
Name: np-socket-closed
Dropped pending packets in a closed socket:
    If a socket is abruptly closed, by the user or software, then any pending packets in
the pipeline for that socket are also dropped. This counter is incremented for each packet
in the pipeline that is dropped.

Recommendation:
```

```
    It is common to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-pf-queue-full
Port Forwarding Queue Is Full:
       This counter is incremented when the Port Forwarding application's internal queue
is full and it receives another packet  for transmission.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-dpp-invalid
Invalid packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the security appliance receives a packet from the internal data plane
interface but could not find the proper driver to parse it.

Recommendation:
    The data plane driver is dynamically registered depending on the type of SSM installed
in the system. So this could happen if data plane packets arrive before the security
appliance is fully initialized. This counter is usually 0. You should not be concerned if
there are a few drops. However, if this counter keeps rising when system is up and
running, it may indicate a problem. Please contact Cisco Technical Assistance Center (TAC)
if you suspect it affects the normal operation of your the security appliance.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-asdp-invalid
Invalid ASDP packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the security appliance receives an ASA SSM Dataplane Protocol (ASDP)
packet from the internal data plane interface, but the driver encountered a problem when
parsing the packet. ASDP is a protocol used by the security appliance to communicate with
certain types of SSMs, like the CSC-SSM. This could happen for various reasons, for
example ASDP protocol version is not compatible between the security appliance and SSM, in
which case the card manager process in the control plane issues system messages and CLI
warnings to inform you of the proper version of images that need to be installed; the ASDP
packet belongs to a connection that has already been terminated on the security appliance;
the security appliance has switched to the standby state (if failover is enable) in which
case it can no longer pass traffic; or any unexpected value when parsing the ASDP header
and payload.

Recommendation:
    The counter is usually 0 or a very small number. But user should not be concerned if
the counter slowly increases over the time, especially when there has been a failover, or
you have manually cleared connections on the security appliance via CLI. If the counter
increases drastically during normal operation, please contact Cisco Technical Assistance
Center (TAC).
```

```
Syslogs:
    421003
    421004


----------------------------------------------------------------
Name: ssm-app-request
Service module requested drop:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the application running on the SSM requests the security appliance to
drop a packet.

Recommendation:
    More information could be obtained by querying the incident report or system messages
generated by the SSM itself. Please consult the documentation that comes with your SSM for
instructions.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-app-fail
Service module is down:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a packet to be inspected by the SSM is dropped because the SSM has become
unavailable. Some examples of this are: software or hardware failure, software or
signature upgrade, or the module being shut down.

Recommendation:
    The card manager process running in the security appliance control plane would have
issued system messages and CLI warning to inform you of the failure. Please consult the
documentation that comes with the SSM to trouble shoot the SSM failure. Contact Cisco
Technical Assistance Center (TAC) if needed.

Syslog:
    None.


----------------------------------------------------------------
Name: wccp-return-no-route
No route to host for WCCP returned packet:
    This counter is incremented when a packet is returned from the Cache Engine and the
security appliance does not find a route for the original source of the packet.

Recommendation:
    Verify that a route exists for the source ip address of the packet returned from Cache
Engine.

Syslogs:
    None.


----------------------------------------------------------------
Name: wccp-redirect-no-route
No route to Cache Engine:
    This counter is incremented when the security appliance tries to redirect a packet and
does not find a route to the Cache Engine.

Recommendation:
    Verify that a route exists for Cache Engine.

Syslogs:
   None.
```

```
------------------------------------------------------------------
Name: telnet-not-permitted
Telnet not permitted on least secure interface:
    This counter is incremented and packet is dropped when the appliance receives a TCP
SYN packet attempting to establish a TELNET session to the appliance and that packet was
received on the least secure interface.

 Recommendation:
    To establish a Telnet session to the appliance via the least secure interface, first
establish an IPsec tunnel to that interface and then connect the Telnet session over that
tunnel.

 Syslogs:
    402117


------------------------------------------------------------------
Name: ipv6-sp-security-failed
IPv6 slowpath security checks failed:
    This counter is incremented and the packet is dropped for one of the following
reasons:
1) IPv6 through-the-box packet with identical source and destination address.
2) IPv6 through-the-box packet with linklocal source or destination address.
3) IPv6 through-the-box packet with multicast destination address.

Recommendation:
    These packets could indicate malicious activity, or could be the result of a
misconfigured IPv6 host.  Use the packet capture feature to capture type asp packets, and
use the source MAC address to identify the source.
Syslogs:
    For identical source and destination address, syslog 106016, else none.


------------------------------------------------------------------
Name: ipv6-eh-inspect-failed
IPv6 extension header is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet but extension header could not be inspected due to memory allocation failed.

 Recommendation:
Also check 'show memory' output to make sure appliance has enough memory to operate.

 Syslogs:
    None


------------------------------------------------------------------
Name: ipv6-bad-eh
Bad IPv6 extension header is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with bad extension header.

 Recommendation:
Check 'verify-header type' of 'parameters' in 'policy-map type ipv6'. Remove
'verify-header type' if the header conformance can be skipped.

 Syslogs:
    325005


------------------------------------------------------------------
Name: ipv6-bad-eh-order
```

```
IPv6 extension headers not in proper order is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with extension headers not in proper order.

 Recommendation:
Check 'verify-header order' of 'parameters' in 'policy-map type ipv6'. Remove
'verify-header order' if the header order can be arbitrary.

 Syslogs:
    325005


----------------------------------------------------------------
Name: ipv6-mobility-denied
IPv6 mobility extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with mobility extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header mobility' in 'policy-map type ipv6'. Remove action
'drop' if mobility should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-mobility-type-denied
IPv6 mobility type extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with mobility type extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header mobility type' in 'policy-map type ipv6'. Remove action
'drop' if mobility should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-fragment-denied
IPv6 fragmentation extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with fragmentation extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header fragmentation' in 'policy-map type ipv6'. Remove action
'drop' if fragmentation should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-routing-address-denied
IPv6 routing extension header exceeding configured maximum routing addresses is denied:
routing count is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with too many routing addresses in routing extension header whichis denied by the
user configuration rule.

 Recommendation:
```

```
    Check action of 'match header routing-address count' in 'policy-map type ipv6'. Remove
action 'drop' or increase <count> if <count> routing addresses should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-routing-type-denied
routing type is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with routing type extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header routing-type' in 'policy-map type ipv6'. Remove action
'drop' if routing-type should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-eh-count-denied
IPv6 extension headers exceeding configured maximum extension headers is denied:
extension header count is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with fragmentation extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header fragmentation' in 'policy-map type ipv6'. Remove action
'drop' if fragmentation should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-dest-option-denied
destination-option is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with destination-option extension header which is denied by the user configuration
rule.

 Recommendation:
    Check action of 'match header destination-option' in 'policy-map type ipv6'. Remove
action 'drop' if destination-option should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-hop-by-hop-denied
IPv6 hop-by-hp extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with hop-by-hop extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header hop-by-hop' in 'policy-map type ipv6'. Remove action
'drop' if hop-by-hop should be allowed.

 Syslogs:
    325004
```

```
-------------------------------------------------------------------
Name: ipv6-esp-denied
ESP is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with ESP extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header esp' in 'policy-map type ipv6'. Remove action 'drop' if
ESP should be allowed.

 Syslogs:
    325004


-------------------------------------------------------------------
Name: ipv6-ah-denied
AH is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with AH extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header ah' in 'policy-map type ipv6'. Remove action 'drop' if
AH should be allowed.

 Syslogs:
    325004


-------------------------------------------------------------------
Name: channel-closed
Data path channel closed:
    This counter is incremented when the data path channel has been closed before the
packet attempts to be sent out through this channel.

Recommendation:
    It is normal in multi-processor system when one processor closes the channel (e.g.,
via CLI), and another processor tries to send a packet through the channel.

 Syslogs:
    None


-------------------------------------------------------------------
Name: dispatch-decode-err
Diapatch decode error:
    This counter is incremented when the packet dispatch module finds an error when
decoding the frame.  An example is an unsupported packet frame.
Recommendation:
    Verify the packet format with a capture tool.

 Syslogs:
    None


-------------------------------------------------------------------
Name: cp-event-queue-error
CP event queue error:
    This counter is incremented when a CP event queue enqueue attempt has failed due to
queue length exceeded. This queue is used by the data-path to punt packets to the
control-point for additional processing. This condition is only possible in a
multi-processor enviroment. The module that attempted to enqueue the packet may issue its
own packet specific drop in response to this error.
```

```
Recommendation:
    While this error does indicate a failure to completely process a packet, it may not
adversely affect the connection. If the condition persists or connections are adversely
affected contact the Cisco Technical Assistance Center (TAC).

Syslogs:
    None


----------------------------------------------------------------
Name: host-limit
Host limit exceeded:
    This counter is incremented when the licensed host limit is exceeded.

Recommendation:
    None.

Syslogs:
    450001


----------------------------------------------------------------
Name: cp-syslog-event-queue-error
CP syslog event queue error:
    This counter is incremented when a CP syslog event queue enqueue attempt has failed
due to queue length exceeded. This queue is used by the data-path to punt logging events
to the control-point when logging destinations other than to a UDP server are configured.
This condition is only possible in a multi-processor environment.

Recommendation:
    While this error does indicate a failure to completely process a logging event,
logging to UDP servers should not be affected. If the condition persists consider lowering
the logging level and/or removing logging destinations or contact the Cisco Technical
Assistance Center (TAC).

Syslogs:
    None


----------------------------------------------------------------
Name: dispatch-block-alloc
Dispatch block unavailable:
     This counter is incremented and the packet is dropped when the appliance could not
allocate a core local block to process the packet that was received by the interface
driver.

Recommendation:
    This may be due to packets being queued for later processing or a block leak. Core
local blocks may also not be available if they are not replenished on time by the free
resource rebalancing logic. Please use "show blocks core" to further diagnose the problem.

Syslogs:
    None


----------------------------------------------------------------
Name: async-lock-queue-limit
Async lock queue limit exceeded:
    Each async lock working queue has a limit of 1000. When more SIP packets are attempted
to be dispatch to the work queue, packet will be dropped.

Recommendation:
```

```
    Only SIP traffic may be dropped. When SIP packets have the same parent lock and they
can be queued into the same async lock queue, thus may result into blocks depletion,
becasue only single core is handling all the media. If a SIP packet attempts to be queued
when the size of the async lock queue exceeds the limit, the packet will be dropped.

Syslogs:
    None.


----------------------------------------------------------------
Name: loopback-lock-failed
Loopback lock failed
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared intrface and the loopback
queue has failed to acquire a lock.

Recommendations:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Techncial Assistance Center (TAC)
if this error occurs.

Syslogs:
    None

----------------------------------------------------------------
Name: loopback-ifc-not-found
Loopback output interface not found
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared interface, and the output
interface is not found by the loopback queue.

Recommendations:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Techncial Assistance Center (TAC)
if this error occurs.

Syslogs:
    None


----------------------------------------------------------------
Name: loopback-count-exceeded
Loopback count exceeded
    This counter is incremented and the packet is dropped when a packet is sent from one
context of the appliance to another context through a shared interface, but this packet
has exceeded the number of times it is allowed to queue to the loopback queue.

Recommendations:
    Check the context configuration for each context. The packet is entering a loop in the
context configurations so that it is stuck between contexts, and is repeatedly put into
the loopback queue.

Syslogs:
    None


----------------------------------------------------------------
Name: ips-license-disabled-fail-close
IPS module license disabled
    The IPS module license has been disabled and when the fail-close mode is configured,
all traffic destined for the IPS module will be dropped. The status of the license can be
checked using the "show activation-key" command.

Recommendation:
```

```
    Please apply an activation key using the "activation-key" command that has the IPS
license enabled.

Syslogs:
    420008


------------------------------------------------------------------
Name: backplane-channel-null
Backplane channel null:
The card backplane channel was NULL. This may happen because the channel
was not initialized correctly and had to be closed. ASA will drop the packet.
Recommendation:
    This should not happen. Contact Cisco TAC for assistance.

Syslogs:
    None.


------------------------------------------------------------------
Name: svc-conn-timer-cb-fail
SVC connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: svc-udp-conn-timer-cb-fail
SVC UDP connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: nat64/46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in coversion of IPv6 traffic to IPv4 or
vice-versa.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-cflow-clu-closed
Cluster flow with CLU closed on owner:
    Director/backup unit received a cluster flow clu delete message from the owner unit
and terminated the flow.
```

```
Recommendation:
    This counter should increment for every replicated clu that is torn down on the owner
unit.

Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-cflow-clu-timeout
Cluster flow with CLU removed from due to idle timeout:
    A cluster flow with CLU is considered idle if the director/backup unit no longer
receives periodic updates from the owner, which is supposed to happen at fixed intervals
when the flow is alive.

Recommendation:
    This counter is informational.

Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-redirect
Flow matched a cluster redirect classify rule:
    A stub forwarding flow will thereafter forward packets to the cluster unit that owns
the flow.

Recommendations:
    This counter is informational and the behavior expected. The packet was forwarded to
the owner over the Cluster Control Link.

Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-drop-on-slave
Flow matched a cluster drop-on-slave classify rule:
    This is for cases that the packets from L3 subnet are seen by all units and only
master unit need to process them.

Recommendations:
    This counter is informational and the behavior expected. The packet is processed by
master.

Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-director-change
The flow director changed due to a cluster join event:
    A new unit joined the cluster and is now the director for the flow. The old
director/backup has removed it's flow and the flow owner will update the new director.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


-------------------------------------------------------------------
```

```
Name: cluster-mcast-owner-change
The multicast flow owner changed due to a cluster join or leave event:
     This flow gets created on a new owner unit.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-convert-to-dirbak
Forwarding or redirect flow converted to director or backup flow:
    Forwarding or redirect flow is removed, so that director or  backup flow can be
created.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-scansafe-server-not-reachable
Scansafe server is not configured or the cloud is down:
    Either the scansafe server IP is not specified in the scansafe general options or the
scansafe server is not reachable.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-scansafe-public_key_not_configured
Scansafe public key not configured:
    This counter is incremented when the scansafe public key is not configured. The packet
is dropped and the connection isclosed.

Recommendation:
    Verify if the configured scansafe public key is configured on the security appliance.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-license-key-not-configured
Scansafe license key not configured:
    This counter is incremented when the scansafe licnese key is not configured. The
packet is dropped and the connection isclosed.

Recommendation:
    Verify if the configured scansafe license key is configured on the security appliance.

Syslogs:
    775002.


----------------------------------------------------------------
```

```
Name: inspect-scansafe-encoding-failed
Inspect  scansafe header encoding failed :
    This counter is incremented when the base64 encoding of user and group name is failed.
The packet is dropped and connection is closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-hdr-encryption-failed
Inspect  scansafe header encryption failed:
    This counter is incremented when the encryption of scansafe header is failed. The
packet is dropped and connection is closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-max-conn-reached
Inspect  scansafe max allowed connections reached:
    This counter is incremented when we get a new connection and the maximum allowed
concurrent scansafe connection for the platform is already reached. The packet is dropped
and connection is closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: inspect-scansafe-duplicate-conn
Inspect scansafe duplicate connection:
     This counter is incremented when duplicate connection with the same source ip address
and port. This packet will be dropped and connection will be closed.

Syslogs:
    775002.


----------------------------------------------------------------
Name: cluster-director-closed
Flow removed due to director flow closed:
    Owner unit received a cluster flow clu delete message from the director unit and
terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the
director unit.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-pinhole-master-change
Master only pinhole flow removed at bulk sync due to master change:
    Master only pinhole flow is removed during bulk sync becase cluster master has
changed.

Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
```

```
    302014


----------------------------------------------------------------
Name: np-socket-lock-failure
Dropped pending packets due to a failed attempt to get an internal socket lock:
    This error occurs if an attempt to grab an internal socket lock fails.

Recommendation:
    This condition should never be encountered during normal operation and     may
indicate a software problem with the appliance.  Contact the Cisco     Technical
Assistance Center (TAC) if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-service-inject-failed
SERVICE Module failed to inject a packet:
    This error occurs if an attempt to inject a packet via the SERVICE     Module fails.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: nat-64-or-46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in coversion of     IPv6 traffic to IPv4
or vice-versa.

Recommendation:
    Verify if the NAT64 or NAT46 policies are configured properly.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-not-owner
Cluster not owner:
    A Cluster data packet was received without a flow.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ccl-cfull-sent
CLU FULL sent:
    A Cluster data packet was received over CCL and full flow is built on a new owner.
This packet is no longer needed.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
```

```
Name: cluster-ccl-backup
Cluster CCL backup:
    A Cluster data packet was received over CCL on a backup unit, when it should have been
received on the owner+director unit.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-ccl-unknown-stub
Cluster CCL unknown stub:
    A Cluster data packet was received over CCL and a matching stub flow found, but unit
has unknown role.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-stub-to-full
Cluster stub to full flow:
    A Cluster packet was received on director, stub flow was converted to full flow. Drop
this packet and wait for retransmission.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-ccl-unknown
Cluster CCL unknown role:
    A Cluster data packet was received over CCL and no matching flow is found, and unit
has unknown role.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-owner-update
Cluster owner update:
    A Cluster data packet was received updating the flow owner.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
Name: cluster-invalid-pkt
Cluster rcvd invalid packet:
    An invalid cluster packet was received.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------
```

```
Name: cluster-no-msgp
Cluster unit is out of message descriptor:
    Cluster unit is out of message descriptor.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-slave-ignored
Flow matched a cluster drop-on-slave classify rule:
    A multicast routing packet was received on a L3 cluster     interface when the unit
was a slave. Only a master unit     is permitted to process these packets.
Recommendation:
    This counter is informational and the behavior expected. The packet is    processed by
master.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-non-owner-ignored
Flow matched a cluster drop-on-non-owner classify rule:
    A multicast data packet was received on a L3 cluster     interface when the unit was
not an elected owner unit.     Only an elected owner unit is permitted to process
these packets.
Recommendation:
    This counter is informational and the behavior expected. The packet is    processed by
one elected owner unit.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat-xlate-failed
NAT failed:
    Failed to create an xlate to translate an IP or transport header.

Recommendation:
    If NAT is not desired, disable "nat-control".  Otherwise, use the "static", "nat" or
"global" command to configure NAT policy for the dropped flow.  For dynamic NAT, ensure
that each "nat" command is paired with at least one "global" command.  Use "show nat" and
"debug pix process" to verify NAT rules.

Syslogs:
    305005, 305006, 305009, 305010, 305011, 305012


----------------------------------------------------------------
Name: nat-rpf-failed
NAT reverse path failed:
    Rejected attempt to connect to a translated host using the translated host's real
address.

Recommendation:
    When not on the same interface as the host undergoing NAT, use the mapped address
instead of the real address to connect to the host. Also, enable the appropriate inspect
command if the application embeds IP address.

Syslogs:
    305005
```

```
----------------------------------------------------------------
Name: nat-cluster-input
NAT invalid input:
    An input value for clustering communication contains an unexpected or invalid value.
Recommendation:
    This could be an internal software error.  Contact Cisco Systems.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat-no-xlate-to-pat-pool
NAT no xlate to pat pool:
    No pre-existing xlate found for a connection with a destination matching a mapped
address in a PAT pool.
Recommendation:
    Configure static PAT is access is desired.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat--xlate-create-failed
NAT xlate creation failed:
    Creation of a PAT xlate failed.
Recommendation:
    Check system memory. Configure at least one backup PAT address. Configure a NAT
address to translate non-overload IP address. Only TCP, UDP, ICMP echo, and PPTP GRE
overloadable.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-peer-mcast-ignored
Flow matched a cluster peer mcast data traffic classify rule:
    A multicast data packet was received on a L3 cluster interface when it is from a
cluster peer unit corresponding interface. This is a packet flooded back from L3 subnet.
Recommendation:
    This counter is informational and the behavior expected. The packet has been forwarded
out of the cluster and should be ignored by cluster.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dispatch-queue-fail
Cluster failed to enqueue into global dispatch work queue:
    A forwarded data packet failed to enqueue into global dispatch work queue.
Recommendation:
    This could be an internal software error.  Contact Cisco Systems.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dir-flow-create-fail
Cluster director failed to create director flow:
    Director is trying to create a stub flow but failed due to resource     limitation.
The resource limit may be either:
       1) system memory
       2) packet block extension memory
       3) system connection limit
```

```
    Causes 1 and 2 will occur simultaneously with flow drop reason "No     memory to
complete flow".
Recommendation:
    - Observe if free system memory is low.
    - Observe if flow drop reason "No memory to complete flow" occurs.
    - Observe if connection count reaches the system connection limit with     the command
"show resource usage".
Syslogs:
    None


----------------------------------------------------------------
Name: cluster-early-sec-chk-fail
Cluster early security check has failed:
    Director applied early security check has failed due to ACL, WCCP     redirect,
TCP-intercept or IP option.
Recommendation:
    This counter is informational and the behavior expected. The packet will     be
dropped.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-queued-ccl-unknown
Cluster CCL unknown stub:
    A queued cluster data packet received over ccl was processed but unit has     unknown
role.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dir-nat-changed
Cluster director NAT action changed:
    Cluster director NAT action has changed due to NAT policy change, update     or
expiration before queued ccl data packet can be processed.Recommendation:
    This counter is informational and the behavior expected. The packet will     be
dropped.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-dir-invalid-ifc
Cluster director has packet with invalid ingress/egress interface:
    Cluster director has processed a previously queued packet with invalid     ingress
and/or egress interface. This is a result of interface removal     (through CLI) before
the packet can be processed.
Recommendation:
    This counter is informational and the behavior expected. The packet will     be
dropped.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-parent-owner-left
Flow removed at bulk sync becasue parent flow is gone:
    Flow is removed during bulk sync because the parent flow's owner has left the cluster.

Recommendation:
```

```
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-ctp-punt-channel-missing
Flow removed at bulk sync becasue CTP punt channel is missing:
    Flow is removed during bulk sync because CTP punt channel is missing in cluster
restored flow.

Recommendation:
    The cluster master may have just left the cluster, and there might be packet drops on
the Cluster Control Link.

Syslogs:
    302014


----------------------------------------------------------------
Name: ike-sa-rate-limit
IKE need SA indication per SA rule rate limit exceeded:
     This counter will increment when the appliance attempts to send a message,indicating
that a new SA is needed for a rate-limited control point service routine and the rate
limit (per/second) is now being exceeded. The current rate is one message every two
seconds.

Recommendation:
     This counter is informational and the behavior expected. The packet will be dropped.

Syslogs:
     None


----------------------------------------------------------------
Name: ike-sa-global-rate-limit
IKE new SA global limit exceeded:
     This counter will increment when the appliance attempts to send a message,indicating
that a new SA is needed for a rate-limited control point service routine and the global
rate limit (per/second) is now being exceeded. The current rate is ten messages per
second.

Recommendation:
     This counter is informational and the behavior expected. The packet will be dropped.

Syslogs:
     None


----------------------------------------------------------------
Name: nat-cluster-invalid-unxlate-redirect
Cluster member dropped an invalid NAT untranslate redirect packet from peer:
    Cluster member received a NAT untranslate packet from peer. However this member does
not own the NAT address pool the packet belongs to.

Recommendation:
    This counter is a temporal condition after a cluster member failure. However, if this
counter is incremented continuously, it could be an internal software error. Contact Cisco
TAC in this case.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: nat-cluster-pool-update-fail
Cluster master failed to send NAT pool update to slave:
    Cluster master has failed to send NAT pool update to slave unit. This drop will
increase if system resources is low.

Recommendation:
    - Observe if free system memory is low.
    - Observe if "SEC_NAT_SEND_NO_BUFFER" counter is increasing.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-forward-error
Cluster member failed to send data packet over CCL:
    Cluster member failed to transmit control packet over the CCL link.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-tp-version-incompatible
The packet contains an incompatible transport protocol:
    The transport protocol of the packet contains a transport protocol that is not
compatible.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ip-version-error
IP version mismatch between layer-2 and layer-3 headers:
    The IP protocol versions in layer-2 and layer-3 headers mismatch.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-tp-sender-myself
DP message over CCL from a unit with same ID as myself:
    The sender information in the transport header indicates that the sender is myself,
which could happen if two clusters (with overlapping IDs) exist on the same network
segment.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ttl-expired
TTL of the packet has expired:
    Maximum TTL value has exceeded for this packet.
Recommendation:
    None.
```

```
Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-ttl-invalid
TTL of the packet is invalid:
    The TTL value of the packet is not a valid value.
Recommendation:
    None.
Syslogs:
    None.
-------------------------------------------------------------------
Name: cluster-non-ip-pkt
Layer 3 protocol of the packet is not IP:
    The packet is not IPv4, IPv6 or an ARP packet.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-bad-tp-pkt
Failed to fetch the transport layer header of the packet:
    Fetching the transport layer header of the packet failed.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-bad-trailer
Failed to fetch the trailer of the packet:
    Fetching the trailer of the packet failed.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-frag-owner-query-error
Cluster fragment failed to query flow director for flow owner:
    A failure either when forwarding first fragment to flow director or     fragment chain
reinsert failure.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: cluster-frag-error
The fragment is not formatted correctly:
    The fragment is not formatted correctly and cannot be processed or     forwarding to
the Fragment Owner failed.
Recommendation:
    None.
Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-bad-ifc-goid-in-trailer
Failed to find ifc from goid in the trailer:
    The goid extracted from the trailer does not yield a     valid real ifc.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: platform-unlicensed
ASAv platform is unlicensed:
    The ASAv is not licensed. All data traffic traversing the appliance will be
dropped until the ASAv is licensed.
Recommendation:
    Check the platform license state with "show activation-key" and install the
appropriate ASAv platform license.
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-bad-tlv-received
Received a packet from SFR without a Policy ID TLV:
    The ASA received a packet from SFR without a Policy ID TLV. This TLV must be present
in non-control packets if it does not have the Standby/Active bit set in the actions
field.
Recommendation:
    None
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-request
Frame was requested to be dropped by SFR:
    The frame was requested to be dropped by SFR due a policy on SFR whereby SFR would set
the actions to Deny Source, Deny Destination, or Deny Pkt.
Recommendation:
    Review SFR policies for any such rule denying the flow.
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-fail-close
Packet was dropped:
    The packet was dropped because the card is not up and the policy configured was
'fail-close' (rather than 'fail-open,' which allows packets through even if the card was
down).
Recommendation:
    Check card status and attempt to restart services or reboot it.
Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-fail
SFR configuration was removed for an existing flow:
    The SFR configuration was removed for an existing flow and we are not able to process
it through SFR, so it will be dropped. This is very unlikely to occur.
Recommendation:
    Review SFR policies for any such rule denying the flow.
```

```
Syslogs:
    None.


-------------------------------------------------------------------
Name: sfr-malformed-packet
Packet from SFR contains an invalid header:
    The packet from SFR contains an invalid header. For instance, the header length may
not be correct.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: sfr-ha-request
Security appliance received a SFR HA request packet:
    This counter is incremented when the security appliance received a SFR HA request
packet, but could not process it and the packet is dropped.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: sfr-invalid-encap
Security appliance received a SFR packet with invalid message header:
    This counter is incremented when the security appliance received a SFR packet with
invalid message header and the packet is dropped.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: sfr-bad-handle-received
Received Bad flow handle in a packet from SFR Module:
    Received Bad flow handle in a packet from SFR Module, thus dropping flow. This counter
is incremented; flow and packet are dropped on ASA as the handle for SFR flow has changed
in flow duration.
Recommendation:
    None.
Syslogs:
    None.


-------------------------------------------------------------------
Name: sfr-rx-monitor-only
Security appliance received a SFR packet when in monitor-only mode:
    This counter is incremented when the security appliance receives a SFR packet when in
monitor-only mode, and the packet is dropped.
Recommendation:
    Remove "monitor-only" keyword in class configuration if not intentional.
Syslogs:
    None.


-------------------------------------------------------------------
```

Flow Drop Reasons

```
----------------------------------------------------------------
Name: tunnel-torn-down
Tunnel has been torn down:
    This counter will increment when the appliance receives a packet associated with an
established flow whose IPsec security association is in the process of being deleted.

Recommendation:
    This is a normal condition when the IPsec tunnel is torn down for any reason.
Syslogs:
    None


----------------------------------------------------------------
Name: no-ipv6-ipsec
IPsec over IPv6 unsupported:
    This counter will increment when the appliance receives an IPsec ESP packet, IPsec
NAT-T ESP packet or an IPsec over UDP ESP packet encapsulated in an IP version 6 header.
The appliance does not currently support any IPsec sessions encapsulated in IP version 6.

Recommendation:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tunnel-pending
Tunnel being brought up or torn down:
    This counter will increment when the appliance receives a packet matching an entry in
the security policy database (i.e. crypto map) but the security association is in the
process of being negotiated; it’s not complete yet.

    This counter will also increment when the appliance receives a packet matching an
entry in the security policy database but the security association has been or is in the
process of being deleted. The difference between this indication and the 'Tunnel has been
torn down' indication is that the 'Tunnel has been torn down' indication is for
established flows.

Recommendation:
    This is a normal condition when the IPsec tunnel is in the process of being negotiated
or deleted.

Syslogs:
    None


----------------------------------------------------------------
Name: need-ike
Need to start IKE negotiation:
    This counter will increment when the appliance receives a packet which requires
encryption but has no established IPsec security association. This is generally a normal
condition for LAN-to-LAN IPsec configurations. This indication will cause the appliance to
begin ISAKMP negotiations  with the destination peer.

Recommendation:
    If you have configured IPsec LAN-to-LAN on your appliance, this indication is normal
and does not indicate a problem.  However, if this counter increments rapidly it may
indicate a crypto configuration error or network error preventing the ISAKMP negotiation
from completing.
```

```
    Verify that you can communicate with the destination peer and verify your crypto
configuration via the 'show running-config' command.

Syslogs:
    None


----------------------------------------------------------------
Name: vpn-handle-error
VPN handle error:
    This counter is incremented when the appliance is unable to create a VPN handle
because the VPN handle already exists.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-error
    show asp table classify crypto
    show asp table vpn-context detail

Syslogs:
    None


----------------------------------------------------------------
Name: vpn-handle-not-found
VPN handle not found:
    This counter is incremented when a datagram hits an encrypt or decrypt rule, and no
VPN handle is found for the flow the datagram is on.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-not-found
    show asp table classify crypto
    show asp table vpn-context detail

Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-spoof-detect
IPsec spoof packet detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not. The packet matched the inner header security policy check of a
configured and established IPsec connection on the appliance but was received unencrypted.
This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPsec traffic.

Syslogs:
    402117
```

```
----------------------------------------------------------------
Name: svc-spoof-detect
SVC spoof packet detected:
    This counter will increment when the security appliance receives a packet which should
have been encrypted but was not. The packet matched the inner header security policy check
of a configured and established SVC connection on the security appliance but was received
unencrypted. This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed SVC traffic.

Syslogs:
    None


----------------------------------------------------------------
Name: svc-failover
An SVC socket connection is being disconnected on the standby unit:
    This counter is incremented for each new SVC socket connection that is disconnected
when the active unit is transitioning into standby state as part of a failover transition.

Recommendation:
    None. This is part of a normal cleanup of a SVC connection when the current device is
transitioning from active to standby. Existing SVC connections on the device are no longer
valid and need to be removed.

Syslogs:
    None.


----------------------------------------------------------------
Name: svc-replacement-conn
SVC replacement connection established:
    This counter is incremented when an SVC connection is replaced by a new connection.

Recommendation:
    None. This may indicate that users are having difficulty maintaining connections to
the ASA. Users should evaluate the quality of their home network and Internet connection.

Syslog:
    722032


----------------------------------------------------------------
Name: ipsec-selector-failure
IPsec VPN inner policy selector mismatch detected:
    This counter is incremented when an IPsec packet is received with an inner IP header
that does not match the configured policy for the tunnel.

 Recommendation:
    Verify that the crypto ACLs for the tunnel are correct and that all acceptable packets
are included in the tunnel identity. Verify that the box is not under attack if this
message is repeatedly seen.

 Syslogs:
    402116


----------------------------------------------------------------
Name: vpn-context-expired
Expired VPN context:
    This counter will increment when the security appliance receives a packet that
requires encryption or decryption, and the ASP VPN context required to perform the
operation is no longer valid.
```

```
 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

 Syslogs:
    None


----------------------------------------------------------------
Name: vpn-lock-error
IPsec locking error:
  This counter is incremented when VPN flow cannot be created due to an internal locking
error.

Recommendation:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Technical Assistance Center (TAC)
if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: out-of-memory
No memory to complete flow:
    This counter is incremented when the appliance is unable to create a flow because of
insufficient memory.

Recommendation:
    Verify that the box is not under attack by checking the current connections. Also
verify if the configured timeout values are too large resulting in idle flows residing in
memory longer. Check the free memory available by issuing 'show memory'. If free memory is
low, issue the command 'show processes memory' to determine which processes are utilizing
most of the memory.

Syslogs:
    None


----------------------------------------------------------------
Name: parent-closed
Parent flow is closed:
    When the parent flow of a subordinating flow is closed, the subordinating flow is also
closed. For example, an FTP data flow (subordinating flow) will be closed with this
specific reason when its control flow (parent flow) is terminated. This reason is also
given when a secondary flow (pin-hole) is closed by its controlling application. For
example, when the BYE messaged is received, the SIP inspection engine (controlling
application) will close the corresponding SIP RTP flows (secondary flow).

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: closed-by-inspection
Flow closed by inspection:
    This reason is given for closing a flow due to an error detected during application
inspection. For example, if an error is detected during inspecting an H323 message, the
corresponding H323 flow is closed with this reason.
```

```
Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: fo-primary-closed
Failover primary closed:
    Standby unit received a flow delete message from the active unit and terminated the
flow.

Recommendation:
    If the appliance is running stateful failover, then this counter should increment for
every replicated connection that is torn down on the standby appliance.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo-standby
Flow closed by failover standby:
    If a through-the-box packet arrives at an appliance or context is in a Standby state,
and a flow is created, the packet is dropped and the flow removed. This counter will
increment each time a flow is removed in this manner.

Recommendation:
    This counter should never be incrementing on the Active appliance or context. However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo_rep_err
Standby flow replication error:
    Standby unit failed to replicate a flow.

Recommendation:
    If appliance is processing VPN traffic, then this counter could be constantly
increasing on the standby unit because of the flow could be replicated before the IKE SA
info. No action is required in this case. If the appliance is not processing VPN traffic,
then this indicate a software detect, turn on the debug: "debug fover fail" on the standby
unit, collect the debug output, and report the problem to Cisco TAC.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: loopback
Flow is a loopback:
    This reason is given for closing a flow due to the following conditions: 1) when
U-turn traffic is present on the flow, and, 2) 'same-security-traffic permit
intra-interface' is not configured.

Recommendation:
    To allow U-turn traffic on an interface, configure the interface with
'same-security-traffic permit intra-interface'.

Syslogs:
```

```
    None.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by access rule:
     This counter is incremented when a drop rule is hit by the packet and flow creation
is denied. This rule could be a default rule created when the box comes up, when various
features are turned on or off, when an acl is applied to interface or any other feature
etc. Apart from default rule drops, a flow could be denied because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface
     5) Implicity deny 'ip any any' at the end of an ACL

Recommendation:
    Observe if one of syslogs related to packet drop are fired. Flow drop results in the
corresponding packet-drop that would fire requisite syslog.

Syslogs:
    None.


----------------------------------------------------------------
Name: pinhole-timeout
Pinhole timeout:
    This counter is incremented to report that the appliance opened a secondary flow, but
no packets passed through this flow within the timeout interval, and hence it was removed.
An example of a secondary flow is the FTP data channel that is created after successful
negotiation on the FTP control channel.

Recommendation:
    No action required.

Syslogs:
    302014, 302016


----------------------------------------------------------------
Name: host-removed
Host is removed:
    Flow removed in response to "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002


----------------------------------------------------------------
Name: xlate-removed
Xlate Clear:
    Flow removed in response to "clear xlate" or "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002


----------------------------------------------------------------
```

```
Name: connection-timeout
Connection timeout:
    This counter is incremented when a flow is closed because of the expiration of it's
inactivity timer.

Recommendation:
    No action required.

Syslogs:
    302014, 302016, 302018, 302021


----------------------------------------------------------------
Name: conn-limit-exceeded
Connection limit exceeded:
    This reason is given for closing a flow when the connection limit has been exceeded.
The connection limit is configured via the 'set connection conn-max' action command.

Recommendation:
    None.

Syslogs:
    201011


----------------------------------------------------------------
Name: tcp-fins
TCP FINs:
    This reason is given for closing a TCP flow when TCP FIN packets are received.

Recommendations:
    This counter will increment for each TCP connection that is terminated normally with
FINs.

Syslogs:
    302014


----------------------------------------------------------------
Name: syn-timeout
SYN Timeout:
    This reason is given for closing a TCP flow due to expiry of embryonic timer.

Recommendations:
    If these are valid session which take longer to establish a connection increase the
embryonic timeout.

Syslogs:
    302014


----------------------------------------------------------------
Name: fin-timeout
FIN Timeout:
    This reason is given for closing a TCP flow due to expiry of half-closed timer.

Recommendations:
    If these are valid session which take longer to close a TCP flow, increase the
half-closed timeout.

Syslogs:
    302014
```

```
----------------------------------------------------------------
Name: reset-in
TCP Reset-I:
    This reason is given for closing an outbound flow (from a low-security interface to a
same- or high-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-out
TCP Reset-O:
    This reason is given for closing an inbound flow (from a high-security interface to
low-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-appliance
TCP Reset-APPLIANCE:
    This reason is given for closing a flow when a TCP reset is generated by appliance.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: recurse
Close recursive flow:
    A flow was recursively freed. This reason applies to pair flows, multicast slave
flows, and syslog flows to prevent syslogs being issued for each of these subordinate
flows.

Recommendation:
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intecept-no-response
TCP intercept, no response from server:
    SYN retransmission timeout after trying three times, once every second. Server
unreachable, tearing down connection.

Recommendation:
    Check if the server is reachable from the ASA.

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: tcp-intercept-unexpected
TCP intercept unexpected state:
    Logic error in TCP intercept module, this should never happen.

Recommendation:
    Indicates memory corruption or some other logic error in the TCP intercept module.

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This reason is given for closing a TCP flow when check-retransmission feature is
enabled and the TCP endpoint sent a retransmission with different data from the original
packet.

Recommendations:
    The TCP endpoint maybe attacking by sending different data in TCP retransmits. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    302014


----------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
    This reason is given for closing a TCP flow when window size advertised by TCP
endpoint is drastically changed without accepting that much data.

Recommendations:
    In order to allow this connection, use the window-variation configuration under
tcp-map.

Syslogs:
    302014


----------------------------------------------------------------
Name: tcpnorm-invalid-syn
TCP invalid SYN:
    This reason is given for closing a TCP flow when the SYN packet is invalid.

Recommendations:
    SYN packet could be invalid for number of reasons, like invalid checksum, invalid TCP
header. Please use the packet capture feature to understand why the SYN packet is invalid.
If you would like to allow these connection use tcp-map configurations to bypass checks.

Syslogs:
    302014


----------------------------------------------------------------
Name: mcast-intrf-removed
Multicast interface removed:
    An output interface has been removed from the multicast entry.
    - OR -
    All output interfaces have been removed from the multicast entry.

Recommendation:
```

```
    No action required.
    - OR -
    Verify that there are no longer any receivers for this group.

Syslogs:
    None


----------------------------------------------------------------
Name: mcast-entry-removed
Multicast entry removed:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    The multicast entry has been deleted so the flow is being cleaned up, but the packet
will be reinjected into the data path.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intercept-kill
Flow terminated by TCP Intercept:
    TCP intercept would tear down a connection if this is the first SYN, a connection is
created for the SYN, and TCP intercept replied with a SYN cookie, or after seeing a valid
ACK from client, when TCP intercept sends a SYN to server, server replies with a RST.

Recommendation:
    TCP intercept normally does not create a connection for first SYN, except when there
are nailed rules or the packet comes over a VPN tunnel or the next hop gateway address to
reach the client is not resolved. So for the first SYN this indicates that a connection
got created. When TCP intercept receives a RST from server, its likely the corresponding
port is closed on the server.

Syslogs:
    None


----------------------------------------------------------------
Name: audit-failure
Audit failure:
    A flow was freed after matching an "ip audit" signature that had reset as the
associated action.

Recommendation:
    If removing the flow is not the desired outcome of matching this signature, then
remove the reset action from the "ip audit" command.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-request
Flow terminated by CXSC:
    This reason is given for terminating a flow as requested by CXSC module.

Recommendations:
```

```
    Check syslogs and alerts on CXSC module.

Syslogs:
    429002


----------------------------------------------------------------
Name: cxsc-fail-close
CXSC fail-close:
    This reason is given for terminating a flow since CXSC card is down and fail-close
option was used with CXSC action.

Recommendations:
    Check and bring up CXSC card.

Syslogs:
    429001


----------------------------------------------------------------
Name: reset-by-cx
Flow reset by CXSC:
    This reason is given for terminating a TCP flow as requested by the CXSC module.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    429003


----------------------------------------------------------------
Name: ips-request
Flow terminated by IPS:
    This reason is given for terminating a flow as requested by IPS module.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002


----------------------------------------------------------------
Name: cxsc-request
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet matches a signature on the CXSC engine.

Recommendations:
    Check syslogs and alerts on the CXSC module.

Syslogs:
    429002


----------------------------------------------------------------
Name: cxsc-bad-tlv-received
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet has bad TLVs.

Recommendations:
    Check syslogs and alerts on the CXSC module.
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-malformed-packet
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet is malformed.

Recommendations:
    Check syslogs and alerts on the CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-fail
CXSC config removed for connection:
    This counter is incremented and the packet is dropped when the CXSC configuration is
not found for a particular connection.

Recommendations:
    Check if any configuration changes have been made for CXSC.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-ha-request
CXSC HA replication drop:
    This counter is incremented when the security appliance receives a CXSC HA request
packet, but could not process it and the packet is dropped.

Recommendation:
    This could happen occasionally when CXSC does not have the latest ASA HA state, such
as right after an ASA HA state change. If the counter is constantly increasing however, it
may be because CXSC and ASA are out of sync. If that happens, contact Cisco TAC for
assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-invalid-encap
CXSC invalid header drop:
    This counter is incremented when the security appliance receives a CXSC packet with an
invalid messsage header, and the packet is dropped.

Recommendation: This should not happen. Contact Cisco TAC for assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: ips-fail-close
IPS fail-close:
    This reason is given for terminating a flow since IPS card is down and fail-close
option was used with IPS inspection.
```

```
Recommendations:
    Check and bring up IPS card.

Syslogs:
    420001


----------------------------------------------------------------
Name: reinject-punt
Flow terminated by punt action:
    This counter is incremented when a packet is punted to the exception-path for
processing by one of the enhanced services such as inspect, aaa etc and the servicing
routine, having detected a violation in the traffic flowing on the flow, requests that the
flow be dropped. The flow is immediately dropped.

Recommendation:
    Please watch for syslogs fired by servicing routine for more information. Flow drop
terminates the corresponding connection.

Syslogs:
    None.


----------------------------------------------------------------
Name: shunned
Flow shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.  When a shun command is applied, it will be
incremented for each existing flow that matches the shun command.

Recommendation:
    No action required.

Syslogs:
    401004


----------------------------------------------------------------
Name: host-limit
host-limit

----------------------------------------------------------------
Name: nat-failed
NAT failed:
    Failed to create an xlate to translate an IP or transport header.

Recommendation:
    If NAT is not desired, disable "nat-control". Otherwise, use the "static", "nat" or
"global" command to configure NAT policy for the dropped flow. For dynamic NAT, ensure
that each "nat" command is paired with at least one "global" command.  Use "show nat" and
"debug pix process" to verify NAT rules.

Syslogs:
    305005, 305006, 305009, 305010, 305011, 305012


----------------------------------------------------------------
Name: nat-rpf-failed
NAT reverse path failed:
    Rejected attempt to connect to a translated host using the translated host's real
address.

Recommendation:
```

```
    When not on the same interface as the host undergoing NAT, use the mapped address
instead of the real address to connect to the host. Also, enable the appropriate inspect
command if the application embeds IP address.

Syslogs:
    305005


----------------------------------------------------------------
Name: inspect-fail
Inspection failure:
    This counter will increment when the appliance fails to enable protocol inspection
carried out by the NP for the connection. The cause could be memory allocation failure, or
for ICMP error message, the appliance not being able to find any established connection
related to the frame embedded in the ICMP error message.

Recommendation:
    Check system memory usage. For ICMP error message, if the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004 for ICMP error.


----------------------------------------------------------------
Name: no-inspect
Failed to allocate inspection:
    This counter will increment when the security appliance fails to allocate a run-time
inspection data structure upon connection creation. The connection will be dropped.

Recommendation:
    This error condition is caused when the security appliance runs out of system memory.
Please check the current available free memory by executing the "show memory" command.

Syslogs:
    None


----------------------------------------------------------------
Name: reset-by-ips
Flow reset by IPS:
    This reason is given for terminating a TCP flow as requested by IPS module.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420003


----------------------------------------------------------------
Name: flow-reclaimed
Non-tcp/udp flow reclaimed for new request:
    This counter is incremented when a reclaimable flow is removed to make room for a new
flow. This occurs only when the number of flows through the appliance equals the maximum
number permitted by the software imposed limit, and a new flow request is received. When
this occurs, if the number of reclaimable flows exceeds the number of VPN tunnels
permitted by the appliance, then the oldest reclaimable flow is removed to make room for
the new flow. All flows except the following are deemed to be reclaimable:
    1. TCP, UDP, GRE and Failover flows
    2. ICMP flows if ICMP stateful inspection is enabled
    3. ESP flows to the appliance

Recommendation:
```

```
    No action is required if this counter is incrementing slowly. If this counter is
incrementing rapidly, it could mean that the appliance is under attack and the appliance
is spending more time reclaiming and rebuilding flows.

Syslogs
    302021


----------------------------------------------------------------
Name: non_tcp_syn
non-syn TCP:
    This reason is given for terminating a TCP flow when the first packet is not a SYN
packet.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: rm-xlate-limit
RM xlate limit reached:
    This counter is incremented when the maximum number of xlates for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-host-limit
RM host limit reached:
    This counter is incremented when the maximum number of hosts for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-inspect-rate-limit
RM inspect rate limit reached:
    This counter is incremented when the maximum inspection rate for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002
```

```
----------------------------------------------------------------
Name: tcpmod-connect-clash
A TCP connect socket clashes with an existing listen connection. This is an internal
system error.  Contact TAC.

----------------------------------------------------------------
Name: ssm-app-request
Flow terminated by service module:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the application running on the SSM requests the security appliance to
terminate a connection.

Recommendation:
    You can obtain more information by querying the incident report or system messages
generated by the SSM itself. Please consult the documentation that comes with comes with
the SSM for instructions.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-app-fail
Service module failed:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a connection that is being inspected by the SSM is terminated because the
SSM has failed.

Recommendation:
    The card manager process running in the security appliance control plane issued system
messages and CLI warning to inform you of the failure. Please consult the documentation
that comes with the SSM to trouble shoot the SSM failure. Contact Cisco Technical
Assistance Center (TAC) if needed.

Syslog:
    421001.


----------------------------------------------------------------
Name: ssm-app-incompetent
Service module incompetent:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a connection is supposed to be inspected by the SSM, but the SSM is not
able to inspect it. This counter is reserved for future use. It should always be 0 in the
current release.

Recommendation:
    None.

Syslog:
    None.


----------------------------------------------------------------
Name: ssl-bad-record-detect
SSL bad record detected:
    This counter is incremented for each unknown SSL record type received from the remote
peer. Any unknown record type received from the peer is treated as a fatal error and the
SSL connections that encounter this error must be terminated.

Recommendation:
```

```
    It is not normal to see this counter increment at any time. If this counter is
incremented, it usually means that the SSL protocol state is out of sync with the client
software. The most likely cause of this problem is a software defect in the client
software. Contact the Cisco TAC with the client software or web browser version and
provide a network trace of the SSL data exchange to troubleshoot this problem.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssl-handshake-failed
SSL handshake failed:
    This counter is incremented when the TCP connection is dropped because the SSL
handshake failed.

Recommendation:
    This is to indicate that the TCP connection is dropped because the SSL handshake
failed. If the problem cannot be resolved based on the syslog information generated by the
handshake failure condition, please include the related syslog information when contacting
the Cisco TAC.

Syslogs:
    725006.
    725014.


----------------------------------------------------------------
Name: ssl-malloc-error
SSL malloc error:
    This counter is incremented for each malloc failure that occurs in the SSL lib. This
is to indicate that SSL encountered a low memory condition where it can't allocate a
memory buffer or packet block.

Recommendation:
    Check the security appliance memory and packet block condition and contact Cisco the
TAC with this memory information.

Syslogs:
    None.


----------------------------------------------------------------
Name: ctm-crypto-request-error
CTM crypto request error:
    This counter is incremented each time CTM cannot accept our crypto request. This
usually means the crypto hardware request queue is full.

Recommendation:
    Issue the show crypto protocol statistics ssl command and contact the Cisco TAC with
this information.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssl-record-decrypt-error
SSL record decryption failed:
    This counter is incremented when a decryption error occurs during SSL data receive.
This usually means that there is a bug in the SSL code of the ASA or peer, or an attacker
may be modifying the data stream. The SSL connection has been closed.

Recommendation:
```

```
    Investigate the SSL data streams to and from your ASA. If there is no attacker, then
this indicates a software error that should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: np-socket-conn-not-accepted
A new socket connection was not accepted:
    This counter is incremented for each new socket connection that is not accepted by the
security appliance.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-failure
NP socket failure:
    This is a general counter for critical socket processing errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-relay-failure
NP socket relay failure:
    This is a general counter for socket relay processing errors.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-data-move-failure
NP socket data movement failure:
    This counter is incremented for socket data movement errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-new-conn-failure
```

```
NP socket new connection failure:
    This counter is incremented for new socket connection failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-transport-closed
NP socket transport closed:
    This counter is incremented when the transport attached to the socket is abruptly
closed.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-block-conv-failure
NP socket block conversion failure:
    This counter is incremented for socket block conversion failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: ssl-received-close-alert
SSL received close alert:
    This counter is incremented each time the security appliance receives a close alert
from the remote client. This indicates that the client has notified us they are going to
drop the connection. It is part of the normal disconnect process.

Recommendation:
    None.

Syslog:
    725007.


----------------------------------------------------------------
Name: children-limit
Max per-flow children limit exceeded:
    The number of children flows associated with one parent flow exceeds the internal
limit of 200.

Recommendation:
    This message indicates either a misbehaving application or an active attempt to
exhaust the firewall memory. Use "set connection per-client-max" command to further fine
tune the limit. For FTP, additionally enable the "strict" option in "inspect ftp".

Syslogs:
```

```
    210005


-----------------------------------------------------------------
Name: tracer-flow
packet-tracer traced flow drop:
    This counter is internally used by packet-tracer for flow freed once tracing is
complete.

Recommendation:
    None.

Syslog:
    None.


-----------------------------------------------------------------
Name: sp-looping-address
looping-address:
    This counter is incremented when the source and destination addresses in a flow are
the same. SIP flows where address privacy is enabled are excluded, as it is normal for
those flows to have the same source and destination address.

 Recommendation:
    There are two possible conditions when this counter will increment. One is when the
appliance receives a packet with the source address equal to the destination. This
represents a type of DoS attack. The second is when the NAT configuration of the appliance
NATs a source address to equal that of the destination. One should examine syslog message
106017 to determine what IP address is causing the counter to increment, then enable
packet captures to capture the offending packet, and perform additional analysis.

 Syslogs:
    106017


-----------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
    This counter will increment when the security appliance receives a packet on an
existing flow that no longer has a valid output adjacency. This can occur if the nexthop
is no longer reachable or if a routing change has occurred typically in a dynamic routing
environment.

 Recommendation:
    No action required.

 Syslogs:
    None


-----------------------------------------------------------------
Name: np-midpath-service-failure
NP midpath service failure:
    This is a general counter for critical midpath service errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


-----------------------------------------------------------------
Name: np-midpath-cp-event-failure
```

```
NP midpath CP event failure:
    This is counter for critical midpath events that could not be sent to the CP.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-context-removed
NP virtual context removed:
    This counter is incremented when the virtual context with which the flow is going to
be associated has been removed. This could happen in multi-core environment when one CPU
core is in the process of destroying the virtual context, and another CPU core tries to
create a flow in the context.

Recommendation:
    No action is required.

Syslog:
    None.


----------------------------------------------------------------
Name: fover-idle-timeout
Flow removed from standby unit due to idle timeout:
    A flow is considered idle if standby unit no longer receives periodical update from
active which is supposed to happen to at fixed internal when flow is alive. This counter
is incremented when such flow is removed from standby unit.

Recommendation:
    This counter is informational.

Syslogs:
    None.


----------------------------------------------------------------
Name: dynamic-filter
Flow matched dynamic-filter blacklist:
    A flow matched a dynamic-filter blacklist or greylist entry with a threat-level higher
than the threat-level threshold configured to drop traffic.

Recommendation:
    Use the internal IP address to trace the infected host. Take remediation steps to
remove the infection.

Syslogs:
    None.


----------------------------------------------------------------

Name: route-change
Flow terminated due to route change:
    When the system adds a lower cost (better metric) route, incoming packets that match
the new route will cause their existing connection to be torn down after the user
configured timeout (floating-conn) value. Subsequent packets will rebuild the connection
out the interface with the better metric.

Recommendation:
```

```
    To prevent the addition of lower cost routes from affecting active flows, the
'floating-conn' configuration timeout value can be set to 0:0:0.

Syslogs:
    None.


----------------------------------------------------------------
Name: svc-selector-failure
SVC VPN inner policy selector mismatch detected:
    This counter is incremented when an SVC packet is received with an inner IP header
that does not match the policy for the tunnel.

 Recommendation:
    None. This packet will be discarded automatically.

 Syslogs:
    None.


----------------------------------------------------------------
Name: dtls-hello-close
DTLS hello processed and closed:
     This counter is incremented when the UDP connection is dropped after the DTLS client
hello message processing is finished. This does not indicate an error.

Recommendation:
None.

 Syslogs:
    None.


----------------------------------------------------------------
Name: svc-conn-timer-cb-fail
SVC connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


----------------------------------------------------------------
Name: svc-udp-conn-timer-cb-fail
SVC UDP connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


----------------------------------------------------------------
Name: nat64/46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in conversion of IPv6 traffic to IPv4 or
vice-versa.
```

```
 Recommendation:
    None.

 Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-cflow-clu-closed
Cluster flow with CLU closed on owner:
    Director/backup unit received a cluster flow clu delete message from the owner unit
and terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the owner
unit.

Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-cflow-clu-timeout
Cluster flow with CLU removed from due to idle timeout:
    A cluster flow with CLU is considered idle if director/backup unit no longer receives
periodical update from owner which is supposed to happen at fixed interval when flow is
alive.

Recommendation:
    This counter is informational.

Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-redirect
Flow matched a cluster redirect classify rule:
    A stub forwarding flow will thereafter forward packets to the cluster unit that owns
the flow.

Recommendations:
    This counter is informational and the behavior expected. The packet was forwarded to
the owner over the Cluster Control Link.

Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-drop-on-slave
Flow matched a cluster drop-on-slave classify rule:
    This is for cases that the packets from L3 subnet are seen by all units and only
master unit need to process them.

Recommendations:
    This counter is informational and the behavior expected. The packet is processed by
master.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-director-change
The flow director changed due to a cluster join event:
    A new unit joined the cluster and is now the director for the flow. The old
director/backup has removed it's flow and the flow owner will update the new director.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-mcast-owner-change
The multicast flow owner changed due to a cluster join or leave event:
     This flow gets created on a new owner unit.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-convert-to-dirbak
Forwarding or redirect flow converted to director or backup flow:
    Forwarding or redirect flow is removed, so that director or backup flow can be
created.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-scansafe-server-not-reachable
Scansafe server is not configured or the cloud is down:
    Either the scansafe server IP is not specified in the scansafe general options or the
scansafe server is not reachable.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-director-closed
Flow removed due to director flow closed:
    Owner unit received a cluster flow clu delete message from the director unit and
terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the
director unit.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-pinhole-master-change
Master only pinhole flow removed at bulk sync due to master change:
    Master only pinhole flow is removed during bulk sync because cluster master has
changed.

Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-parent-owner-left
Flow removed at bulk sync becasue parent flow is gone:
    Flow is removed during bulk sync becasue the parent flow's owner has left the cluster.

Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-ctp-punt-channel-missing
Flow removed at bulk sync becasue CTP punt channel is missing:
    Flow is removed during bulk sync because CTP punt channel is missing in cluster
restored flow.

Recommendation:
    The cluster master may have just left the cluster. And there might be packet drops on
the Cluster Control Link.

Syslogs:
    302014


----------------------------------------------------------------
Name: vpn-overlap-conflict

VPN Network Overlap Conflict:
When a packet is decrypted, the inner packet is examined against the crypto map
configuration. If the packet matches a different crypto map entry than the one it was
received on, it will be dropped and this counter will increment. A common cause for this
is two crypto map entries containing similar/overlapping address spaces.

Recommendation:
    Check your VPN configuration for overlapping networks. Verify the
    order of your crypto maps and use of deny rules in ACLs.

Syslogs:
    None


----------------------------------------------------------------
Name: invalid-vxlan-segment-id
Invalid VXLAN segment-id:
    This counter is incremented when the security appliance sees an invalid VXLAN
segment-id attached to a flow.

Recommendation:
```

```
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-valid-nve-ifc
No valid NVE interface:
    This counter is incremented when the security appliance fails to identify the NVE
interface of a VNI interface for a flow.

Recommendation:
    Verify that the nve is configured for all interfaces.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-peer-nve
Invalid peer NVE:
    This counter is incremented when the security appliance fails to get IP and MAC
address of a peer NVE for a flow.

Recommendation:
    Verify that peer nve is configured or learned for the nve.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-encap-error
Fail to encap with VXLAN:
    This counter is incremented when the security appliance fails to encapsulate a packet
with VXLAN for a flow.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: sfr-request
SFR requested to terminate the flow:
    The SFR requested to terminate the flow. The actions bit 0 is set.
Recommendation:
    Review SFR policies for any such rule denying the flow.

Syslogs:
    None.


----------------------------------------------------------------
Name: reset-by-sfr
SFR requested to terminate and reset the flow:
    The SFR requested to terminate and reset the flow. The actions bit 1 is set.
Recommendation:
    Review SFR policies for any such rule denying the flow.

Syslogs:
```

```
    None.


----------------------------------------------------------------
Name: sfr-fail-close
Flow was terminated:
    The flow was terminated because the card is down and the configured policy was
'fail-close'.
Recommendation:
    Check card status and attempt to restart services or reboot it.

Syslogs:
    None.


----------------------------------------------------------------
Name: cmd-invalid-encap
The security appliance received an invalid CMD packet.
     An invalid CMD packet is one which does not conform to the standard CMD header
values. This counter checks if the packet conforms to the correct metadata, version,
length, option and sgt range.
Recommendation:
     None.

Syslogs:
     None.


----------------------------------------------------------------
Name: ifc-not-cmd-enabled
The security appliance receives a CMD packet on an interface not configured to receive
one.
     The packet is dropped.
Recommendation:
     None.

Syslogs:
     None.


----------------------------------------------------------------
Name: ifc-zn-chg
Interface experienced a zone change
     The parent interface has been joined or left a zone.
Recommendation:
     None.

Syslogs:
     302014, 302016, 302018, 302021, 302304


----------------------------------------------------------------
```

예

다음은 카운터가 마지막으로 지워진 시간을 나타내는 타임스탬프가 포함된 **show asp drop** 명령의 샘플 출력입니다.

```
ciscoasa# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                              3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                          4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                             760
  Expired flow (flow-expired)                                               1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                                 24
  NAT failed (nat-failed)                                               28739
  NAT reverse path failed (nat-rpf-failed)                              22266
  Inspection failure (inspect-fail)                                     19433

Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

관련 명령

명령	설명
capture	ASP 삭제 코드에 따라 패킷을 캡처합니다(패킷 캡처 옵션 포함).
clear asp drop	가속화된 보안 경로에 대한 삭제 통계를 지웁니다.
show conn	연결 정보를 표시합니다.

show asp event dp-cp

데이터 경로 또는 제어 경로 이벤트 대기열을 디버깅하려면 특권 EXEC 모드에서 **show asp event dp-cp** 명령을 사용합니다.

show asp event dp-cp [**cxsc msg**]

구문 설명

cxsc msg	(선택 사항) CXSC 이벤트 대기열으로 전송되는 CXSC 이벤트 메시지를 식별합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.
9.1(3)	라우팅 이벤트 대기열 항목이 추가되었습니다.

사용 지침

show asp event dp-cp 명령은 데이터 경로 및 제어 경로 내용을 표시하여 문제 해결을 도와줍니다. 데이터 경로 및 제어 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp event dp-cp** 명령의 샘플 출력입니다.

```
ciscoasa# show asp event dp-cp

DP-CP EVENT QUEUE                  QUEUE-LEN  HIGH-WATER
Punt Event Queue                           0        2048
Routing Event Queue                        0           1
Identity-Traffic Event Queue               0          17
General Event Queue                        0           0
Syslog Event Queue                         0        3192
Non-Blocking Event Queue                   0           4
Midpath High Event Queue                   0           0
Midpath Norm Event Queue                   0           0
SRTP Event Queue                           0           0
HA Event Queue                             0           3
Threat-Detection Event Queue               0           3
ARP Event Queue                            0           3
```

```
IDFW Event Queue                            0           0
CXSC Event Queue                            0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt              4005920          0   935295  3070625  4005920        4372
  inspect-sunrp   4005920          0   935295  3070625  4005920        4372
routing              77          0       77        0       77           0
arp-in              618          0      618        0      618           0
identity-traffic   1519          0     1519        0     1519           0
syslog             5501          0     5501        0     5501           0
threat-detection     12          0       12        0       12           0
ips-cplane         1047          0     1047        0     1047           0
ha-msg              520          0      520        0      520           0
cxsc-msg            127          0      127        0      127           0
```

show asp load-balance

로드 밸런서 대기열 크기의 히스토그램의 표시하려면 특권 EXEC 모드에서 **show asp load-balance** 명령을 사용합니다.

show asp load-balance [**detail**]

구문 설명

detail	(선택 사항) 해시 버킷에 대한 자세한 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.1(1)	이 명령이 도입되었습니다.

사용 지침

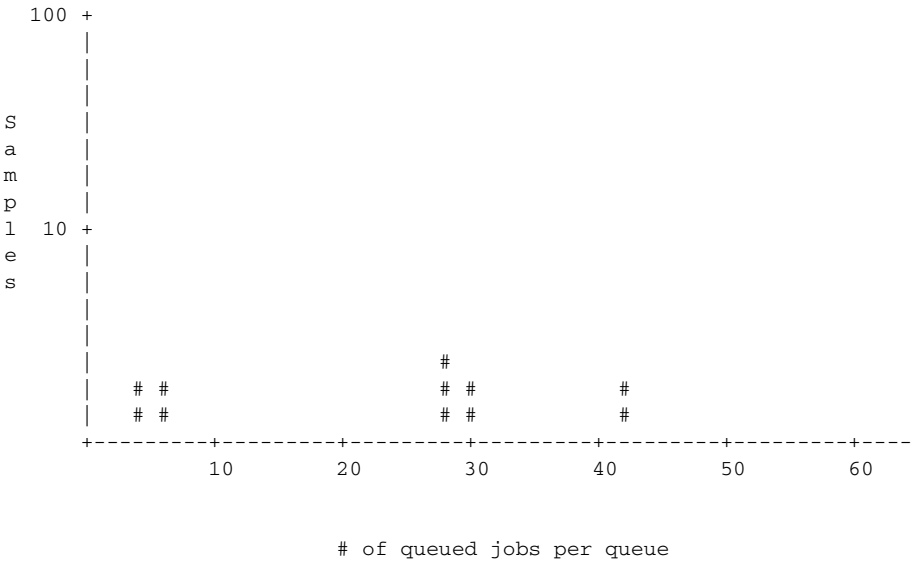
show asp load-balance 명령은 문제 해결을 도와줄 수 있습니다. 일반적으로 패킷은 인터페이스 수신 링에서 가져온 동일한 코어에 의해 처리됩니다. 그러나 다른 코어에서 방금 받은 패킷과 동일한 연결을 이미 처리 중인 경우에는 패킷이 해당 코어의 대기열에 추가됩니다. 이 대기열 처리로 인해 다른 코어가 유휴 상태인 동안 로드 밸런서 대기열이 증가할 수 있습니다. 자세한 내용은 **asp load-balance per-packet** 명령을 참고하십시오.

예

다음은 **show asp load-balance** 명령의 샘플 출력입니다. X축은 서로 다른 대기열에서 대기 중인 패킷 수를 나타냅니다. Y축은 대기 중인 패킷이 있는 로드 밸런서 해시 버킷 수(히스토그램 버킷을 나타내는 히스토그램 제목의 버킷과 혼동하지 않도록)를 나타냅니다. 대기열이 있는 해시 버킷의 정확한 개수를 확인하려면 **detail** 키워드를 사용합니다.

```
ciscoasa# show asp load-balance

Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                     ASP load balancer queue sizes
```



다음은 **show asp load-balance detail** 명령의 샘플 출력입니다.

```
ciscoasa# show asp load-balance detail

<Same histogram output as before with the addition of the following values for the
histogram>

Data points:
<snip>
  bucket[1-1] = 0 samples
  bucket[2-2] = 0 samples
  bucket[3-3] = 0 samples
  bucket[4-4] = 1 samples
  bucket[5-5] = 0 samples
  bucket[6-6] = 1 samples
<snip>
  bucket[28-28] = 2 samples
  bucket[29-29] = 0 samples
  bucket[30-30] = 1 samples
<snip>
  bucket[41-41] = 0 samples
  bucket[42-42] = 1 samples
```

관련 명령

명령	설명
asp load-balance per-packet	멀티 코어 ASA 모델의 코어 부하 균형 방식을 변경합니다.

show asp load-balance per-packet

ASP 부하 균형에 대한 특정 통계를 패킷별로 표시하려면 특권 EXEC 모드에서 **show asp load-balance per-packet** 명령을 사용합니다.

show asp load-balance per-packet [**history**]

구문 설명

history	(선택 사항) 컨피그레이션 상태(활성, 비활성 또는 자동), 현재 상태(활성 또는 비활성화), 높은 워터마크 및 낮은 워터마크, 전역 임계값, 자동 전환이 발생한 횟수, 자동 전환이 활성화된 최소 및 최대 대기 시간, 타임스탬프가 포함된 패킷별 ASP 부하 균형 기록, 켜고 끈 이유 등을 표시합니다.

기본값

옵션을 지정하지 않은 경우 이 명령은 기본 상태, 관련 값 및 패킷별 ASP 부하 균형 통계를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.3(1)	이 명령이 도입되었습니다.

사용 지침

show asp load-balance per-packet 명령은 패킷별 ASP 부하 균형에 대한 컨피그레이션 상태(활성, 비활성 또는 자동), 현재 상태(활성 또는 비활성화), 높은 워터마크 및 낮은 워터마크, 전역 임계값, 자동 전환이 발생한 횟수, 자동 전환이 활성화된 최소 및 최대 대기 시간 등을 표시합니다.

정보는 다음 형식으로 표시됩니다.

```
Config mode    : [ enabled | disabled | auto ]
Current status : [ enabled | disabled ]

RX ring Blocks low/high watermark      : [RX ring Blocks low watermark in percentage] /
[RX ring Blocks high watermark in percentage]
System RX ring count low threshold     : [System RX ring count low threshold] / [Total
number of RX rings in the system]
System RX ring count high threshold    : [System RX ring count high threshold] / [Total
number of RX rings in the system]
```

자동 모드

```
Current RX ring count threshold status : [Number of RX rings crossed watermark] / [Total
number of RX rings in the system]
Number of times auto switched          : [Number of times ASP load-balance per-packet has
been switched]
Min/max wait time with auto enabled    : [Minimal wait time with auto enabled] / [Maximal
wait time with auto enabled] (ms)
```

수동 모드

```
Current RX ring count threshold status : N/A
```

ASA 5585-X 및 ASASM에서만 이 명령을 사용할 수 있습니다.

예

다음은 **show asp load-balance per-packet** 명령의 샘플 출력입니다.

```
ciscoasa# show asp load-balance per-packet

Config status  : auto
Current status : disabled

RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)
```

다음은 **show asp load-balance per-packet history** 명령의 샘플 출력입니다.

```
ciscoasa# show asp load-balance per-packet history

Config status  : auto
Current status : disabled

RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)

==========================================================================================
From State          To State            Reason
==========================================================================================
15:07:13 UTC Dec 17 2013
Manually Disabled   Manually Disabled   Disabled at startup

15:09:14 UTC Dec 17 2013
Manually Disabled   Manually Enabled    Config

15:09:15 UTC Dec 17 2013
Manually Enabled    Auto Disabled       0/33 of the ring(s) crossed the watermark

15:10:16 UTC Dec 17 2013
Auto Disabled       Auto Enabled        1/33 of the ring(s) crossed the watermark
                                        Internal-Data0/0 RX[01] crossed above high watermark

15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        2/33 of the ring(s) crossed the watermark
                                        Internal-Data0/1 RX[04] crossed above high watermark
```

```
15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        3/33 of the ring(s) crossed the watermark
                                        Internal-Data0/1 RX[05] crossed above high watermark

15:10:16 UTC Dec 17 2013
Auto Enabled        Auto Enabled        2/33 of the ring(s) crossed the watermark
                                        Internal-Data0/0 RX[01] dropped below low watermark

15:10:17 UTC Dec 17 2013
Auto Enabled        Auto Enabled        3/33 of the ring(s) crossed the watermark
                                        Internal-Data0/2 RX[01] crossed above high watermark

(---More---)

15:14:01 UTC Dec 17 2013
Auto Enabled        Auto Disabled       8/33 of the ring(s) crossed the watermark
                                        Internal-Data0/3 RX[01] crossed above high watermark

15:14:01 UTC Dec 17 2013
Auto Disabled       Auto Enabled        7/33 of the ring(s) crossed the watermark
                                        Internal-Data0/3 RX[01] dropped below low watermark

(---More---)

15:20:11 UTC Dec 17 2013
Auto Enabled        Auto Disabled       0/33 of the ring(s) crossed the watermark
                                        Internal-Data0/2 RX[01] dropped below low watermark
(---More---)
```

관련 명령

명령	설명
asp load-balance per-packet auto	각 인터페이스 수신 링 또는 흐름 집합에서 패킷별 ASP 부하 균형을 자동으로 켜고 끕니다.
clear asp load-balance history	패킷별 ASP 부하 균형 기록을 지우고 자동 전환이 발생한 횟수를 재설정합니다.

show asp table arp

가속화된 보안 경로 ARP 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table arp** 명령을 사용합니다.

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

구문 설명

address *ip_address*	(선택 사항) ARP 테이블 항목을 보려는 IP 주소를 식별합니다.
interface *interface_name*	(선택 사항) ARP 테이블을 볼 특정 인터페이스를 식별합니다.
netmask *mask*	(선택 사항) IP 주소의 서브넷 마스크를 설정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show arp 명령은 제어 평면의 내용을 표시하고, **show asp table arp** 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로 내용을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp table arp** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

관련 명령

명령	설명
show arp	ARP 테이블을 표시합니다.
show arp statistics	ARP 통계를 표시합니다.

show asp table classify

가속화된 보안 경로 분류자 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table classify** 명령을 사용합니다.

s**how asp table classify** [**interface** *interface_name*] [**crypto** | **domain** *domain_name*] [**hits**] [**match** *regexp*] [**user-statistics**]

구문 설명

crypto	(선택 사항) 암호화, 암호 해독 및 ipsec 터널 흐름 도메인만 표시합니다.
domain *domain_name*	(선택 사항) 특정 분류자 도메인에 대한 항목을 표시합니다. 도메인 목록은 "사용 지침" 섹션을 참고하십시오.
hits	(선택 사항) 0이 아닌 적중 값이 있는 분류자 항목을 표시합니다.
interface *interface_name*	(선택 사항) 분류자 테이블을 볼 특정 인터페이스를 식별합니다.
match *regexp*	(선택 사항) 정규식과 일치하는 분류자 항목을 표시합니다. 정규식에 공백이 포함된 경우 따옴표를 사용합니다.
user-statistics	(선택 사항) 사용자 및 그룹 정보를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.2(4)	ASP 테이블 카운터가 마지막으로 지워진 시간을 나타내는 타임스탬프와 **hits** 옵션이 추가되었습니다.
8.0(2)	일치 컴파일이 중단된 횟수를 표시하는 새 카운터가 추가되었습니다. 이 카운터는 값이 0보다 큰 경우에만 표시됩니다.
8.2(2)	**match** *regexp* 옵션이 추가되었습니다.
8.4(4.1)	ASA CX 모듈에 대한 **csxc** 및 **cxsc-auth-proxy** 도메인이 추가되었습니다.
9.0(1)	**user-statistics** 키워드가 추가되었습니다. 보안 그룹 이름과 소스 및 대상 태그가 추가되도록 출력이 업데이트되었습니다.
9.2(1)	ASA FirePOWER 모듈에 대한 sfr 도메인이 추가되었습니다.
9.3(1)	출력에서 SGT(보안 그룹 태그) 값이 수정되었습니다. 태그 값 "tag=0"은 "알 수 없음"에 대한 예약된 SGT 값인 0x0과의 정확한 일치를 나타내고, SGT 값 “tag=any”는 규칙에서 고려할 필요가 없는 값을 나타냅니다.

사용 지침

show asp table classify 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 분류자 내용을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 분류자는 프로토콜과 같은 인커밍 패킷의 속성과 소스 및 목적지 주소를 검사하여 각 패킷을 해당 분류 규칙에 일치시킵니다. 각 규칙에는 패킷 삭제 또는 통과 허용과 같은 수행되는 작업의 유형을 확인하는 분류 도메인이 레이블로 지정됩니다. 이 정보는 디버깅에만 사용되며, 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

분류자 도메인은 다음과 같습니다.

```
aaa-acct
aaa-auth
aaa-user
accounting
app-redirect
arp
autorp
backup interface CLI (Apply backup interface rule)
capture
cluster-drop-mcast-from-peer
cluster-drop-on-non-owner
cluster-drop-on-slave
cluster-mark-mcast-from-peer
cluster-redirect
conn-nailed
conn-set
ctcp
cxsc
cxsc-auth-proxy
debug-icmp-trace
decrypt
dhcp
dynamic-filter
eigrp
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
flow-export
host
host-limit
hqf
ids
inspect-ctiqbe
inspect-dcerpc
inspect-dns-cp
inspect-dns-ids
inspect-dns-np
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-im
inspect-ip-options
inspect-ipsec-pass-thru
inspect-ipv6
```

```
inspect-mgcp
inspect-mmp
inspect-netbios
inspect-phone-proxy
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-scansafe
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-srtp
inspect-sunrpc
inspect-tftp
inspect-waas
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipv6
l2tp
l2tp-ppp
limits
lu
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-per-session
nat-reverse
no forward CLI (Apply no forward interface rule)
null
ospf
permit
permit-ip-option
permit-ip-option-explicit
pim
ppp
priority-q
punt
punt-root (soft NP)
qos
qos-per-class (soft NP)
qos-per-dest (soft NP)
qos-per-flow (soft NP)
qos-per-source (soft NP)
rip
sal-relay
sfr
shun
soft-np-tcp-module
soft-np-udp-module
splitdns
ssm
ssm-app-capacity
ssm-isvw
ssm-isvw-capable
svc-ib-tunnel-flow
svc-ob-tunnel-flow
tcp-intercept
tcp-ping
udp-unidirectional
```

```
user-statistics
vpn-user
wccp
```

예

다음은 **show asp table classify** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table classify

Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
```

다음은 마지막으로 적중 횟수를 지운 레코드가 포함된 **show asp table classify hits** 명령의 샘플 출력입니다.

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

다음은 계층 2 정보가 포함된 **show asp table classify hits** 명령의 샘플 출력입니다.

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
```

```
    input_ifc=LAN-SEGMENT, output_ifc=any

.
.
.

Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
    input_ifc=LAN-SEGMENT, output_ifc=any
```

다음은 보안 그룹이 액세스 목록에 지정되지 않은 경우 **show asp table classify** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table classify
in  id=0x7ffedb54cfe0, priority=500, domain=permit, deny=true
        hits=0, user_data=0x6, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=224.0.0.0, mask=240.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=management, output_ifc=any
```

관련 명령

명령	설명
show asp drop	삭제된 패킷에 대한 가속화된 보안 경로 카운터를 표시합니다.

show asp table cluster chash-table

클러스터링을 위해 가속화된 보안 경로 cHash 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table cluster chash-table** 명령을 사용합니다.

show asp table cluster chash-table

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show asp table cluster chash-table 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 내용을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp table cluster chash-table** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
33111111
11000112
22332000
```

```
00231121
11222220
33330223
31013211
11101111
13111111
11023133
30001100
00000111
12022222
00133333
33222000
00022222
33011333
11110002
33333322
13333030
```

관련 명령

명령	설명
show asp cluster counter	클러스터 데이터 경로 카운터 정보를 표시합니다.

show asp table cts sgt-map

Cisco TrustSec에 대한 데이터 경로에서 유지되는 IP 주소-보안 그룹 테이블 데이터베이스에서 IP 주소-보안 그룹 테이블 매핑을 표시하려면 특권 EXEC 모드에서 **show asp table cts sgt-map** 명령을 사용합니다.

show asp table cts sgt-map [**address** *ipv4* | **address** *ipv6* | **ipv4** | **ipv6** | **sgt** *sgt*]

구문 설명

address *ipv4*	(선택 사항) 지정된 IPv4 주소에 대한 IP 주소-보안 그룹 테이블 매핑을 표시합니다.
address *ipv6*	(선택 사항) 지정된 IPv6 주소에 대한 IP 주소-보안 그룹 테이블 매핑을 표시합니다.
ipv4	(선택 사항) IPv4 주소에 대한 IP 주소-보안 그룹 테이블 매핑을 표시합니다.
ipv6	(선택 사항) IPv6 주소에 대한 IP 주소-보안 그룹 테이블 매핑을 표시합니다.
sgt *sgt*	(선택 사항) 지정된 보안 그룹 테이블 주소에 대한 IP 주소-보안 그룹 테이블 매핑을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

주소를 지정하지 않으면 데이터 경로에 있는 IP 주소-보안 그룹 테이블 데이터베이스의 모든 항목이 표시됩니다. 주소는 정확한 주소 또는 서브넷 기반 주소일 수 있습니다. 또한 사용 가능한 경우 보안 그룹 이름이 표시됩니다.

예

다음은 **show asp table cts sgt-map** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table cts sgt-map

IP Address                              SGT
=====================================================
10.10.10.5                              1234:Marketing
55.67.89.12                             5:Engineering
56.34.0.0                               338:HR
192.4.4.4                               345:Finance
```

```
Total number of entries shown = 4
```

다음은 **show asp table cts sgt-map address** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table cts sgt-map address 10.10.10.5

IP Address                          SGT
================================================
10.10.10.5                          1234:Marketing

Total number of entries shown = 1
```

다음은 **show asp table cts sgt-map ipv6** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table cts sgt-map ipv6

IP Address                                  SGT
============================================================
FE80::A8BB:CCFF:FE00:110                    17:Marketing-Servers
FE80::A8BB:CCFF:FE00:120                    18:Eng-Servers

Total number of entries shown = 2
```

다음은 **show asp table cts sgt-map sgt** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table cts sgt-map sgt 17

IP Address                                  SGT
============================================
FE80::A8BB:CCFF:FE00:110                    17

Total number of entries shown = 1
```

관련 명령

명령	설명
show running-config cts	실행 중인 컨피그레이션에 대한 SXP 연결을 표시합니다.
show cts environment	환경 데이터 새로 고침 작업의 상태를 표시합니다.

show asp table dynamic-filter

가속화된 보안 경로 봇네트(botnet) 트래픽 필터 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table dynamic-filter** 명령을 사용합니다.

show asp table dynamic-filter [**hits**]

구문 설명

hits	(선택 사항) 0이 아닌 적중 값이 있는 분류자 항목을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

show asp table dynamic-filter 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 봇네트(botnet) 트래픽 필터 규칙을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp table dynamic-filter** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table dynamic-filter

Context: admin
 Address 10.246.235.42 mask 255.255.255.255 name: example.info
flags: 0x44 hits 0
 Address 10.40.9.250 mask 255.255.255.255 name: bad3.example.com
flags: 0x44 hits 0
 Address 10.64.147.20 mask 255.255.255.255 name: bad2.example.com flags: 0x44
hits 0
 Address 10.73.210.121 mask 255.255.255.255 name: bad1.example.com flags:
0x44 hits 0
 Address 10.34.131.135 mask 255.255.255.255 name: bad.example.com flags:
0x44 hits 0
 Address 10.64.147.16 mask 255.255.255.255 name:
1st-software-downloads.com flags: 0x44 hits 2
 Address 10.131.36.158 mask 255.255.255.255 name: www.example.com flags: 0x41 hits 0
 Address 10.129.205.209 mask 255.255.255.255 flags: 0x1 hits 0
 Address 10.166.20.10 mask 255.255.255.255 flags: 0x1 hits 0
...
```

관련 명령

명령	설명
address	차단 목록 또는 허용 목록에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇네트 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇네트 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇네트 트래픽 필터 통계를 지웁니다.
dns domain-lookup	ASA에서 DNS 요청을 DNS 서버로 보내 지원되는 명령에 대한 이름 조회를 수행할 수 있도록 합니다.
dns server-group	ASA의 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 유보 목록(greylist)의 트래픽을 차단 목록의 트래픽으로 처리합니다.
dynamic-filter blacklist	봇네트 트래픽 필터 차단 목록을 수정합니다.
dynamic-filter database fetch	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter drop blacklist	차단 목록의 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않은 모든 트래픽 또는 트래픽의 클래스에 봇네트 트래픽 필터를 사용합니다.
dynamic-filter updater-client enable	동적 데이터베이스 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스 사용을 활성화합니다.
dynamic-filter whitelist	봇네트 트래픽 필터 허용 목록을 수정합니다.
inspect dns dynamic-filter-snoop	봇네트 트래픽 필터 스누핑을 통한 DNS 검사를 활성화합니다.
name	차단 목록 또는 허용 목록에 이름을 추가합니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등을 포함하여 동적 데이터베이스에 대한 정보를 표시합니다.
show dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 요약을 표시하거나, **detail** 키워드를 사용하여 실제 IP 주소 및 이름을 표시합니다.
show dynamic-filter reports	상위 10개의 봇네트 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇네트 트래픽 필터로 모니터링된 연결 수 및 이러한 연결 중 허용 목록, 차단 목록 및 유보 목록과 일치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	서버 IP 주소, 다음에 ASA에서 서버에 연결할 시간, 마지막으로 설치된 데이터베이스 버전 등 업데이터 서버에 대한 정보를 표시합니다.
show running-config dynamic-filter	봇네트 트래픽 필터에서 실행 중인 컨피그레이션을 표시합니다.

show asp table filter

가속화된 보안 경로 필터 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table filter** 명령을 사용합니다.

show asp table filter [**access-list** *acl-name*] [**hits**] [**match** *regexp*]

구문 설명

acl-name	(선택 사항) 지정된 액세스 목록에 대해 설치된 필터를 지정합니다.
hits	(선택 사항) 0이 아닌 적중 값이 있는 필터 규칙을 지정합니다.
match *regexp*	(선택 사항) 정규식과 일치하는 분류자 항목을 표시합니다. 정규식에 공백이 포함된 경우 따옴표를 사용합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(2)	이 명령이 도입되었습니다.

사용 지침

필터가 VPN 터널에 적용된 경우 필터 규칙이 필터 테이블에 설치됩니다. 터널에 지정된 필터가 있으면 암호화하기 전과 암호를 해독한 후에 필터 테이블을 확인하여 내부 패킷을 허용할지 또는 거부할지 결정합니다.

예

다음은 user1이 연결하기 전 **show asp table filter** 명령의 샘플 출력입니다. 인바운드와 아웃바운드 두 방향 모두에서 IPv4 및 IPv6에 대해 암시적 거부 규칙만 설치됩니다.

```
ciscoasa# show asp table filter

Global Filter Table:
 in  id=0xd616ef20, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f420, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
         src ip=::/0, port=0
         dst ip=::/0, port=0
 out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
```

```
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

다음은 user1이 연결한 후 **show asp table filter** 명령의 샘플 출력입니다. VPN 필터 ACL은 인바운드 방향에 따라 정의됩니다. 소스는 피어를 나타내고 대상은 내부 리소스를 나타냅니다. 아웃바운드 규칙은 인바운드 규칙의 소스와 대상을 서로 바꾸는 방식으로 파생됩니다.

```
ciscoasa# show asp table filter

Global Filter Table:
 in  id=0xd682f4a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd682f460, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=21
 in  id=0xd68366a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6d89050, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5001
 in  id=0xd45d5b08, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5ac8, filter_id=0x2(vpnfilter), protocol=17
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5002
 in  id=0xd6244f30, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6244ef0, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=0
 in  id=0xd64edca8, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64edc68, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f018, priority=11, domain=vpn-user, deny=true
        hits=43, user_data=0xd613eb58, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f518, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd615f068, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
 out id=0xd7395650, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd7395610, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=21
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d49b8, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d4978, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=5001
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d5cf0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5cb0, filter_id=0x2(vpnfilter), protocol=17
        src ip=95.1.224.100, mask=255.255.255.255, port=5002
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd6245118, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd62450d8, filter_id=0x2(vpnfilter), protocol=1
        src ip=95.1.224.100, mask=255.255.255.255, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd64ede90, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64ede50, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd616f298, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d9f8, filter_id=0x0(-implicit deny-), protocol=0
```

```
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f7c8, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161730, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

관련 명령

명령	설명
show asp drop	삭제된 패킷에 대한 가속화된 보안 경로 카운터를 표시합니다.
show asp table classifier	가속화된 보안 경로의 분류자 내용을 표시합니다.

show asp table interfaces

가속화된 보안 경로 인터페이스 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table interfaces** 명령을 사용합니다.

show asp table interfaces

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show asp table interfaces 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 인터페이스 테이블 내용을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp table interfaces** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
```

```
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show asp table routing

가속화된 보안 경로 라우팅 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table routing** 명령을 사용합니다. 이 명령은 IPv4 및 IPv6 주소를 지원합니다.

show asp table routing [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*]

구문 설명

address *ip_address*	라우팅 항목을 볼 IP 주소를 설정합니다. IPv6 주소의 경우 슬래시(/) 뒤에 오는 접두사(0~128)로 서브넷 마스크를 포함할 수 있습니다. 예를 들어 다음과 같이 입력합니다. `fe80::2e0:b6ff:fe01:3b7a/128`
input	입력 경로 테이블의 항목을 표시합니다.
interface *interface_name*	(선택 사항) 라우팅 테이블을 볼 특정 인터페이스를 식별합니다.
netmask *mask*	IPv4 주소의 경우 서브넷 마스크를 지정합니다.
output	출력 경로 테이블의 항목을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.3(2)	영역별 라우팅 정보가 추가되었습니다.

사용 지침

show asp table routing 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 라우팅 테이블 내용을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

참고 ASA 5505에서는 show asp table routing 명령 출력에 잘못된 항목이 표시될 수도 있습니다.

예

다음은 **show asp table routing** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

참고 ASA 5505 플랫폼에서는 **show asp table routing** 명령 출력에 잘못된 항목이 표시될 수도 있습니다. 이러한 항목은 무시하십시오. 아무 영향이 없습니다.

관련 명령

명령	설명
show route	제어 평면의 라우팅 테이블을 표시합니다.

show asp table socket

가속화된 보안 경로 소켓 정보를 디버깅하려면 특권 EXEC 모드에서 **show asp table socket** 명령을 사용합니다.

show asp table socket [**socket handle**] [**stats**]

구문 설명

socket handle	소켓의 길이를 지정합니다.
stats	가속화된 보안 경로 소켓 테이블의 통계를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

show asp table socket 명령은 가속화된 보안 경로 소켓 문제 해결에 도움이 될 수 있는 가속화된 보안 경로 소켓 정보를 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp table socket** 명령의 샘플 출력입니다.

```
TCP Statistics:
  Rcvd:
     total14794
     checksum errors0
     no port0
  Sent:
     total0

UDP Statistics:
  Rcvd:
     total0
     checksum errors0
  Sent:
     total0
     copied0
```

```
NP SSL System Stats:
  Handshake Started:33
  Handshake Complete:33
  SSL Open:4
  SSL Close:117
  SSL Server:58
  SSL Server Verify:0
  SSL Client:0
```

TCP/UDP 통계는 텔넷, SSH 또는 HTTPS와 같이 ASA에서 실행 중이거나 수신 대기 중인 서비스를 대상으로 하는 전송된 패킷 수 또는 수신된 패킷 수를 나타내는 패킷 카운터입니다. 체크섬 오류는 계산된 패킷 체크섬이 패킷에 저장된 체크섬 값과 일치하지 않아(즉, 패킷이 손상됨) 삭제된 패킷 수입니다. NP SSL 통계는 수신된 각 메시지 유형 수를 나타냅니다. 대부분은 SSL 서버 또는 SSL 클라이언트에 대한 새 SSL 연결의 시작 및 완료를 나타냅니다.

관련 명령

명령	설명
show asp table vpn-context	가속화된 보안 경로 VPN 상황 테이블을 표시합니다.

show asp table vpn-context

가속화된 보안 경로 VPN 상황 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table vpn-context** 명령을 사용합니다.

show asp table vpn-context [**detail**]

구문 설명

detail	(선택 사항) VPN 상황 테이블에 대한 추가 세부 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.0(4)	각 상황에 대해 터널 삭제 후 상태 저장 흐름을 유지하는 +PRESERVE 플래그가 추가되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

show asp table vpn-context 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 VPN 상황 내용을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp table vpn-context** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

다음은 영구 IPsec 터널링된 흐름이 활성화된 경우(PRESERVE 플래그로 표시됨) **show asp table vpn-context** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

다음은 **show asp table vpn-context detail** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

다음은 영구 IPsec 터널링된 흐름이 활성화된 경우(PRESERVE 플래그로 표시됨) **show asp table vpn-context detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
```

```
VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
ciscoasa(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

관련 명령

명령	설명
show asp drop	삭제된 패킷에 대한 가속화된 보안 경로 카운터를 표시합니다.

show asp table zone

가속화된 보안 경로 영역 테이블을 디버깅하려면 특권 EXEC 모드에서 **show asp table zone** 명령을 사용합니다.

show asp table zone [*zone_name*]

구문 설명

zone_name	(선택 사항) 영역 이름을 식별합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

show asp table zone 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 내용을 표시합니다. 가속화된 보안 경로에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

예

다음은 **show asp table zone** 명령의 샘플 출력입니다.

```
ciscoasa# show asp table zone

Zone: outside-zone id: 2
 Context: test-ctx
  Zone Member(s) : 2
   outside1       GigabitEthernet0/0
   outside2       GigabitEthernet0/1
```

관련 명령

명령	설명
show asp table routing	디버깅을 위해 가속화된 보안 경로 테이블을 표시하며, 각 경로와 연계된 영역을 표시합니다.
show zone	영역 ID, 상황, 보안 수준 및 멤버를 표시합니다.

show auto-update

Auto Update Server 상태를 확인하려면 특권 EXEC 모드에서 **show auto-update** 명령을 사용합니다.

show auto-update

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 Auto Update Server 상태를 볼 수 있습니다.

예

다음은 **show auto-update** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show auto-update
Poll period: 720 minutes, retry count: 0, retry period: 5 minutes
Timeout: none
Device ID: host name [ciscoasa]
```

관련 명령

auto-update device-id	Auto Update Server에서 사용할 ASA 디바이스 ID를 설정합니다.
auto-update poll-period	ASA가 Auto Update Server에서 업데이트를 확인하는 주기를 설정합니다.
auto-update server	Auto Update Server를 식별합니다.
auto-update timeout	시간 제한 이내에 Auto Update Server에 연결하지 못한 경우 트래픽이 ASA를 통과하지 못하도록 합니다.
clear configure auto-update	Auto Update Server 컨피그레이션을 지웁니다.
show running-config auto-update	Auto Update Server 컨피그레이션을 표시합니다.

4 장

show bgp through show cpu 명령

show bgp

BGP(Border Gateway Protocol) 라우팅 테이블의 항목을 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp** 명령을 사용합니다.

show bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath** | **multipaths** | **subnets**] | **bestpath** | **multipaths**] | **all** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name*]]

구문 설명

ip-address	(선택 사항) AS 경로 액세스 목록 이름을 지정합니다.
mask	(선택 사항) 지정된 네트워크의 일부인 호스트를 필터링하거나 일치시킬 마스크입니다.
longer-prefixes	(선택 사항) 지정된 경로 및 모든 구체적인 경로를 표시합니다.
injected	(선택 사항) BGP 라우팅 테이블에 삽입된 특정 접두사를 표시합니다.
shorter-prefixes	(선택 사항) 지정된 경로 및 모든 구체적이지 않은 경로를 표시합니다.
length	(선택 사항) 접두사 길이입니다. 이 인수 값은 0~32의 숫자입니다.
bestpath	(선택 사항) 이 접두사에 대한 최상의 경로를 표시합니다.
multipaths	(선택 사항) 이 접두사에 대한 다중 경로를 표시합니다.
subnets	(선택 사항) 지정된 접두사에 대한 서브넷 경로를 표시합니다.
all	(선택 사항) BGP 라우팅 테이블의 모든 주소 패밀리 정보를 표시합니다.
prefix-list *name*	(선택 사항) 지정된 접두사 목록을 기반으로 출력을 필터링합니다.
pending-prefixes	(선택 사항) BGP 라우팅 테이블에서 삭제 보류 중인 접두사를 표시합니다.
route-map *name*	(선택 사항) 지정된 경로 맵을 기반으로 출력을 필터링합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

show bgp 명령은 BGP 라우팅 테이블의 내용을 표시하는 데 사용됩니다. 특정 접두사, 접두사 길이 및 접두사 목록, 경로 맵 또는 조건부 알림을 통해 삽입된 접두사에 대한 항목을 표시하도록 출력을 필터링할 수 있습니다.

Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4 이상, 4바이트 자동 시스템 번호의 Cisco 구현에서는 asplain(예: 65538)을 자동 시스템 번호의 기본 정규식 일치 및 출력 표시로 사용하지만, RFC 5396에 설명된 대로 asplain 형식과 asdot 형식 둘 다로 4바이트 자동 시스템 번호를 구성할 수 있습니다. 4바이트 자동 시스템 번호의 기본 정규식 일치 및 출력 표시를 asdot 형식으로 변경하려면 **clear bgp *** 명령이 뒤에 오는 **bgp asnotation dot** 명령을 사용하여 모든 현재 BGP 세션의 하드 재설정을 수행합니다.

예

다음 샘플 출력에서는 BGP 라우팅 테이블을 보여 줍니다.

```
Router# show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
```

표 4-1에는 각 필드에 대한 설명이 나와 있습니다.

표 4-1 show bgp 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. • s - 테이블 항목이 표시되지 않습니다. • d - 테이블 항목이 감소합니다. • h - 테이블 항목이 기록입니다. • * - 테이블 항목이 유효합니다. • > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. • i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다. • r - 테이블 항목에서 RIB 오류가 발생했습니다. • s - 테이블 항목이 오래되었습니다. • m - 테이블 항목에 해당 네트워크에 사용할 여러 경로가 있습니다. • b - 테이블 항목에 해당 네트워크에 사용할 백업 경로가 있습니다. • x - 테이블 항목에 해당 네트워크에 사용할 최상의 외부 경로가 있습니다.

필드	설명
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. • i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. • e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. • ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	네트워크 엔터티의 IP 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 라우터에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다.
(stale)	지정된 자동 시스템의 다음 경로가 정상 재시작 프로세스 중에 "stale"로 표시되었음을 나타냅니다.

show bgp(4바이트 자동 시스템 번호): 예

다음 샘플 출력은 Path 필드 아래에 표시된 4바이트 자동 시스템 번호 65536 및 65550이 있는 BGP 라우팅 테이블을 보여 줍니다. 이 예에는 Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4 이상이 필요합니다.

```
RouterB# show bgp

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

show bgp ip-address: 예

다음 샘플 출력은 BGP 라우팅 테이블의 192.168.1.0 항목에 대한 정보를 표시합니다.

```
Router# show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

다음 샘플 출력은 BGP 라우팅 테이블의 10.3.3.3 255.255.255.255 항목에 대한 정보를 표시합니다.

```
Router# show bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

표 4-2에는 각 필드에 대한 설명이 나와 있습니다.

표 4-2 show bgp(4바이트 자동 시스템 번호)필드

필드	설명
BGP routing table entry fo	라우팅 테이블 항목의 IP 주소 또는 네트워크 번호입니다.
version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
Paths	사용 가능한 경로 수 및 설치된 최상의 경로 수입니다. 이 줄에는 최상의 경로가 IP 라우팅 테이블에 설치된 경우 "Default-IP-Routing-Table"이 표시됩니다.
Multipath	이 필드는 다중 경로 부하 공유가 활성화된 경우에 표시됩니다. 이 필드는 다중 경로가 iBGP인지 또는 eBGP인지 나타냅니다.
Advertised to update-groups	알림이 처리되는 각 업데이트 그룹 수입니다.
Origin	항목의 출처입니다. 출처는 IGP, EGP 또는 incomplete일 수 있습니다. 이 줄에는 구성된 메트릭(메트릭이 구성되지 않은 경우 0), 로컬 환경 설정 값(기본값은 100) 및 경로의 상태와 유형(internal, external, multipath, best)이 표시됩니다.
Extended Community	이 필드는 경로에 확장 커뮤니티 특성이 수반되는 경우에 표시됩니다. 특성 코드가 이 줄에 표시됩니다. 확장 커뮤니티에 대한 정보는 후속 줄에 표시됩니다.

show bgp all: 예

다음은 **all** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다. 구성된 모든 주소 패밀리에 대한 정보가 표시됩니다.

```
Router# show bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

show bgp longer-prefixes: 예

다음은 **longer-prefixes** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다.

```
Router# show bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30         8896         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.1.0         10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.11.0        10.92.72.30        42482         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.14.0        10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.15.0        10.92.72.30         8696         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.16.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.17.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.18.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.19.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
```

show bgp shorter-prefixes: 예

다음은 **shorter-prefixes** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다. 8비트 접두사 길이가 지정됩니다.

```
Router# show bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0         10.0.0.2                               0 ?
*                     10.0.0.2                0              0 200 ?
```

show bgp prefix-list: 예

다음은 **prefix-list** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다.

```
Router# show bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?

*                   10.0.0.2                 0           0 200 ?
```

show bgp route-map: 예

다음은 **route-map** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다.

```
Router# show bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?
*                   10.0.0.2                 0           0 200 ?
```

show bgp all community

특정 BGP(Border Gateway Protocol) 커뮤니티에 속한 모든 주소 패밀리의 경로를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp all community** 명령을 사용합니다.

show bgp all community [*community-number...*[*community-number*]] **[local-as] [no-advertise] [no-export] [exact-match]**

구문 설명

community-number.	(선택 사항) 지정된 커뮤니티 번호와 관련된 경로를 표시합니다. 여러 커뮤니티 번호를 지정할 수 있습니다. 범위는 1~4294967295 또는 AA:NN(자동 시스템:커뮤니티 번호, 2바이트 번호)입니다.
local-as	(선택 사항) 로컬 자동 시스템(잘 알려진 커뮤니티) 외부로 전송되지 않는 경로만 표시합니다.
no-advertise	(선택 사항) 피어(잘 알려진 커뮤니티)로 보급되지 않는 경로만 표시합니다.
no-export	(선택 사항) 로컬 자동 시스템(잘 알려진 커뮤니티) 외부로 내보낼 수 없는 경로만 표시합니다.
exact-match	(선택 사항) 지정된 BGP 커뮤니티 목록과 정확히 일치하는 경로만 표시합니다. **참고** 명령에서 키워드를 사용할 수 있는지 여부는 명령 모드에 따라 다릅니다. **exact-match** 키워드는 사용자 EXEC 모드에서 사용할 수 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

사용자가 **local-as**, **no-advertise** 및 **no-export** 키워드를 순서에 상관없이 입력할 수 있습니다. **bgp all community** 명령을 사용할 때는 잘 알려진 커뮤니티 앞에 숫자 커뮤니티를 입력해야 합니다.

예를 들어 다음 문자열은 유효하지 않습니다.

```
ciscoasa# show bgp all community local-as 111:12345
```

대신 다음 문자열을 사용합니다.

```
ciscoasa# show bgp all community 111:12345 local-as
```

예

다음은 커뮤니티 1, 2345 및 6789012를 지정하여 실행한 **show bgp all community** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp all community 1 2345 6789012 no-advertise local-as no-export
exact-match

For address family: IPv4 Unicast

BGP table version is 5, local router ID is 30.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network  Next Hop            Metric LocPrf Weight Path
*> 10.0.3.0/24       10.0.0.4                               0 4 3 ?
*> 10.1.0.0/16       10.0.0.4                 0             0 4 ?
*> 10.12.34.0/24     10.0.0.6                 0             0 6 ?
```

표 4-26에는 각 필드에 대한 설명이 나와 있습니다.

표 4-3 show bgp all community 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	BGP 커뮤니티가 표시되도록 설정된 라우터의 라우터 ID입니다. 마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. d - 테이블 항목이 감소합니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 내부 BGP 세션을 통해 학습되었습니다.
Origin codes	항목의 출처를 나타냅니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 network 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.
Network	네트워크 엔터티의 네트워크 주소 및 네트워크 마스크입니다. 주소 유형은 주소 패밀리에 따라 다릅니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 주소 유형은 주소 패밀리에 따라 다릅니다.
Metric	내부 자동 시스템 메트릭 값입니다. 이 필드는 자주 사용되지 않습니다.
LocPrf	**set local-preference** 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.

표 4-3 show bgp all community 필드(계속)

필드	설명
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다.

show bgp all neighbors

모든 주소 패밀리의 네이버와 BGP(Border Gateway Protocol)의 연결에 대한 정보를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp all neighbors** 명령을 사용합니다.

show bgp all neighbors [*ip-address* **] [advertised-routes | paths [***reg-exp***] | policy [detail] | received prefix-filter | received-routes | routes]**

구문 설명

ip-address	(선택 사항) 네이버의 IP 주소입니다. 이 인수를 생략하면 모든 네이버에 대한 정보가 표시됩니다.
advertised-routes	(선택 사항) 네이버에 보급된 모든 경로를 표시합니다.
paths *reg-exp*	(선택 사항) 지정된 네이버에서 학습된 자동 시스템 경로를 표시합니다. 선택적 정규식을 사용하여 출력을 필터링할 수 있습니다.
policy	(선택 사항) 주소 패밀리별로 네이버에 적용되는 정책을 표시합니다.
detail	(선택 사항) 경로 맵, 접두사 목록, 커뮤니티 목록, ACL(Access Control List: 액세스 제어 목록), 자동 시스템 경로 필터 목록 등 자세한 정책 정보를 표시합니다.
received prefix-filter	(선택 사항) 지정된 네이버에서 전송된 접두사 목록(ORF(아웃바운드 경로 필터))를 표시합니다.
received-routes	(선택 사항) 지정된 네이버에서 수신된 모든 경로(허용 및 거부 모두)를 표시합니다.
routes	(선택 사항) 수신되고 허용된 모든 경로를 표시합니다. 이 키워드를 입력한 경우에 표시되는 출력은 **received-routes** 키워드로 표시되는 출력의 하위 집합입니다.

기본값

이 명령의 출력은 모든 네이버에 대한 정보를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

show bgp all neighbors 명령을 사용하여 IPv4와 같은 주소 패밀리에 특정한 네이버 세션에 대한 BGP 및 TCP 연결 정보를 표시할 수 있습니다.

예

다음 예에서는 **show bgp all neighbors** 명령의 샘플 출력을 보여 줍니다.

```
ciscoasa# show bgp all neighbors

For address family: IPv4 Unicast
BGP neighbor is 172.16.232.53, remote AS 100, external link
 Member of peer-group internal for session parameters
  BGP version 4, remote router ID 172.16.232.53
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        11
  Default minimum time between advertisement runs is 5 seconds

  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0


Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837

SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle

Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent:4445 (retransmit: 5), with data: 4445, total data bytes;244128
```

표 4-4에는 각 필드에 대한 설명이 나와 있습니다.

표 4-4 show bgp all neighbor 필드

필드	설명
For address family	다음 필드에서 참조하는 주소 패밀리입니다.
BGP neighbor	BGP 네이버의 IP 주소 및 자동 시스템 번호입니다.
remote AS	네이버의 자동 시스템 번호입니다.

표 4-4 show bgp all neighbor 필드(계속)

필드	설명
external link	eBGP(외부 Border Gateway Protocol) 피어입니다.
BGP version	원격 라우터와 통신하는 데 사용되는 BGP 버전입니다.
remote router ID	네이버의 IP 주소입니다.
BGP state	이 BGP 연결의 상태입니다.
up for	기본 TCP 연결이 존재한 시간(hh:mm:ss)입니다.
Last read	BGP가 이 네이버에서 마지막으로 메시지를 수신한 이후에 경과한 시간(hh:mm:ss)입니다.
hold time	BGP가 메시지를 수신하지 않고 이 네이버와의 세션을 유지할 시간(초)입니다.
keepalive interval	킵얼라이브 메시지가 이 네이버로 전송되는 시간 간격(초)입니다.
Message statistics	메시지 유형별로 구성된 통계입니다.
InQ depth is	입력 대기열의 메시지 수입니다.
OutQ depth is	출력 대기열의 메시지 수입니다.
Sent	전송된 총 메시지 수입니다.
Rcvd	수신된 총 메시지 수입니다.
Opens	전송되거나 수신된 열어 본 메시지 수입니다.
Notifications	전송되거나 수신된 알림(오류) 메시지 수입니다.
Updates	전송되거나 수신된 업데이트 메시지 수입니다.
Keepalives	전송되거나 수신된 킵얼라이브 메시지 수입니다.
Route Refresh	전송되거나 수신된 경로 새로 고침 요청 메시지 수입니다.
Total	전송되거나 수신된 총 메시지 수입니다.
Default minimum time between...	알림 전송 간의 시간 간격(초)입니다.
Connections established	TCP와 BGP 간의 연결이 성공적으로 설정된 횟수입니다.
dropped	유효 세션이 실패하거나 중단된 횟수입니다.
Last reset	이 피어링 세션이 마지막으로 재설정된 이후에 경과한 시간(hh:mm:ss)입니다. 재설정 사유가 이 줄에 표시됩니다.
External BGP neighbor may be...	BGP TTL(Time to Live) 보안 검사가 활성화되었음을 나타냅니다. 로컬 및 원격 피어를 구분할 수 있는 최대 홉 수가 이 줄에 표시됩니다.
Connection state	BGP 피어의 연결 상태입니다.
Local host, Local	로컬 BGP 스피커의 IP 주소와 포트 번호입니다.
Foreign host, Foreign port	네이버 주소와 BGP 대상 포트 번호입니다.
Enqueued packets for retransmit:	TCP에서 재전송 대기 중인 패킷 수입니다.
Event Timers	TCP 이벤트 타이머입니다. 시작 및 대기 모드 해제(만료된 타이머)에 대한 카운터가 제공됩니다.
Retrans	패킷이 재전송된 횟수입니다.

표 4-4 show bgp all neighbor 필드(계속)

필드	설명
TimeWait	재전송 타이머 만료 대기 시간입니다.
AckHold	확인 응답 보류 타이머입니다.
SendWnd	전송 기간입니다.
KeepAlive	킵얼라이브 패킷 수입니다.
GiveUp	확인 응답이 없어 패킷이 삭제된 횟수입니다.
PmtuAger	경로 MTU 검색 타이머입니다.
DeadWait	정지된 세그먼트에 대한 만료 타이머입니다.
iss:	초기 패킷 전송 시퀀스 번호입니다.
snduna:	확인 응답을 받지 않은 마지막 전송 시퀀스 번호입니다.
sndnxt:	전송할 다음 패킷 시퀀스 번호입니다.
sndwnd:	원격 호스트의 TCP 윈도우 크기입니다.
irs:	초기 패킷 수신 시퀀스 번호입니다.
rcvnxt:	로컬로 확인 응답을 받은 마지막 수신 시퀀스 번호입니다.
rcvwnd:	로컬 호스트의 TCP 윈도우 크기입니다.
delrcvwnd:	지연된 수신 창, 즉 로컬 호스트에서 연결에서 읽었지만 원격 호스트로 보급한 수신 창에서 아직 제거하지 않은 데이터입니다. 이 필드의 값은 rcvwnd 필드에 적용된 시점의 전체 크기 패킷보다 클 때까지 점진적으로 증가합니다.
SRTT:	계산된 평균 왕복 시간 제한입니다.
RTTO:	왕복 시간 제한입니다.
RTV:	왕복 시간의 편차입니다.
KRTT:	새 왕복 시간 제한(Karn 알고리즘 사용)입니다. 이 필드는 재전송된 패킷의 왕복 시간을 별도로 추적합니다.
minRTT:	기록된 최소 왕복 시간 제한(계산에 사용된 고정 값)입니다.
maxRTT:	기록된 최대 왕복 시간 제한입니다.
ACK hold	로컬 호스트가 추가 데이터를 전달(piggyback)하기 위해 확인 응답을 지연시킬 기간입니다.
IP Precedence value	BGP 패킷의 IP 우선 순위입니다.
Datagrams	네이버에서 수신된 업데이트 패킷 수입니다.
Rcvd:	수신된 패킷 수입니다.
with data	데이터와 함께 전송된 업데이트 패킷 수입니다.
total data bytes	수신된 총 데이터(바이트)입니다.
Sent	전송된 업데이트 패킷 수입니다.
with data	데이터와 함께 수신된 업데이트 패킷 수입니다.
total data bytes	전송된 총 데이터(바이트)입니다.

show bgp cidr-only

CIDR(Classless Inter-Domain Routing)과 함께 경로를 표시하려면 EXEC 모드에서 **show bgp cidr-only** 명령을 사용합니다.

show bgp cidr-only

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 **show bgp cidr-only** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

표 4-5에는 각 필드에 대한 설명이 나와 있습니다.

표 4-5 show bgp cidr-only 필드

필드	설명
BGP table version is 220	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.

표 4-5 show bgp cidr-only 필드(계속)

필드	설명
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp community

지정된 BGP 커뮤니티에 속한 경로를 표시하려면 EXEC 모드에서 **show bgp community** 명령을 사용합니다.

show bgp community *community-number* **[exact]**

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 특권 EXEC 모드에 실행된 **show bgp community** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp community 111:12345 local-as

 BGP table version is 10, local router ID is 224.0.0.10
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
 *> 172.16.2.2/32    10.43.222.2            0             0 222 ?
 *> 10.0.0.0         10.43.222.2            0             0 222 ?
 *> 10.43.0.0        10.43.222.2            0             0 222 ?
 *> 10.43.44.44/32   10.43.222.2            0             0 222 ?
 *  10.43.222.0/24   10.43.222.2            0             0 222 i
 *> 172.17.240.0/21  10.43.222.2            0             0 222 ?
 *> 192.168.212.0    10.43.222.2            0             0 222 i
 *> 172.31.1.0       10.43.222.2            0             0 222 ?
```

표 4-6에는 각 필드에 대한 설명이 나와 있습니다.

표 4-6 show bgp community 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.

표 4-6 show bgp community 필드(계속)

필드	설명
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp community-list

BGP(Border Gateway Protocol) 커뮤니티 목록에서 허용하는 경로를 표시하려면 사용자 또는 특권 EXEC 모드에서 **show bgp community-list** 명령을 사용합니다.

show bgp community-list {*community-list-number* | *community-list-name* [**exact-match**]}

구문 설명

community-list-number	1~500의 표준 또는 확장 커뮤니티 목록 번호입니다.
community-list-name	커뮤니티 목록 이름입니다. 커뮤니티 목록 이름은 표준 또는 확장일 수 있습니다.
exact-match	(선택 사항) 정확히 일치하는 항목이 있는 경로만 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용할 때는 인수를 지정해야 합니다. **exact-match** 키워드는 선택 사항입니다

예

다음은 특권 EXEC 모드에 실행된 **show bgp community-list** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp community-list 20

BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1             0    100      0 1800 1239 ?
*>i                 10.0.16.1             0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1             0    100      0 1800 690 568 ?
*>i                 10.0.16.1             0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1             0    100      0 1800 701 35 ?
*>i                 10.0.16.1             0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1             0    100      0 1800 690 560 ?
*>i                 10.0.16.1             0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1             0    100      0 1800 690 200 ?
*>i                 10.0.16.1             0    100      0 1800 690 200 ?
*                   10.92.72.24                         0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1             0    100      0 1800 174 ?
```

```
*>i                 10.0.16.1               0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1               0    100      0 1800 701 i
*>i                 10.0.16.1               0    100      0 1800 701 i
*                   10.92.72.24                           0 1878 704 701 i
```

표 4-7에는 각 필드에 대한 설명이 나와 있습니다.

표 4-7 show bgp community-list 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp filter-list

지정된 필터 목록과 일치하는 경로를 표시하려면 EXEC 모드에서 **show bgp filter-list** 명령을 사용합니다.

show bgp filter-list *access-list-name*

구문 설명

access-list-name	자동 시스템 경로 액세스 목록의 이름입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 특권 EXEC 모드에 실행된 **show bgp filter-list** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp filter-list filter-list-acl

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                         0 109 108 ?
*  172.16.17.0      172.16.72.30                         0 109 108 ?
*  172.16.18.0      172.16.72.30                         0 109 108 ?
*  172.16.19.0      172.16.72.30                         0 109 108 ?
*  172.16.24.0      172.16.72.30                         0 109 108 ?
*  172.16.29.0      172.16.72.30                         0 109 108 ?
*  172.16.30.0      172.16.72.30                         0 109 108 ?
*  172.16.33.0      172.16.72.30                         0 109 108 ?
*  172.16.35.0      172.16.72.30                         0 109 108 ?
*  172.16.36.0      172.16.72.30                         0 109 108 ?
*  172.16.37.0      172.16.72.30                         0 109 108 ?
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

표 4-8에는 각 필드에 대한 설명이 나와 있습니다.

표 4-8 show bgp filter-list 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp injected-paths

BGP(Border Gateway Protocol) 라우팅 테이블의 거부된 모든 경로를 표시하려면 사용자 또는 특권 EXEX 모드에서 **show bgp injected-paths** 명령을 사용합니다.

show bgp injected-paths

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 EXEC 모드에 실행된 **show bgp injected-paths** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

표 4-9에는 각 필드에 대한 설명이 나와 있습니다.

표 4-9 show bgp injected-path 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.

표 4-9 show bgp injected-path 필드(계속)

필드	설명
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv4

IPv4(IP 버전 4) BGP(Border Gateway Protocol) 라우팅 테이블의 항목을 표시하려면 특권 EXEC 모드에서 **show bgp ipv4** 명령을 사용합니다.

show bgp ipv4

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 **show bgp ipv4 unicast** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

다음은 **show bgp ipv4 multicast** 명령의 샘플 출력입니다.

```
Router# show bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

표 4-10에는 각 필드에 대한 설명이 나와 있습니다.

표 4-10 show bgp ipv4 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6

IPv6 BGP(Border Gateway Protocol) 라우팅 테이블의 항목을 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp ipv6** 명령을 사용합니다.

show bgp ipv6 unicast [*ipv6-prefix*/*prefix-length*] [**longer-prefixes**] [**labels**]

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
ipv6-prefix	(선택 사항) IPv6 BGP 라우팅 테이블의 특정 네트워크를 표시하기 위해 입력된 IPv6 네트워크 번호입니다. 이 인수는 RFC 2373에 나와 있는 형식이어야 합니다. 즉, 콜론 사이의 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.
/prefix-length	(선택 사항) IPv6 접두사의 길이입니다. 접두사(주소의 네트워크 부분)를 구성하는 상위 연속 비트 수를 나타내는 10진수 값입니다. 10진수 값 앞에 슬래시가 표시되어야 합니다.
longer-prefixes	(선택 사항) 지정된 경로 및 보다 구체적인 경로를 표시합니다.
labels	(선택 사항) 주소 패밀리별로 이 네이버에 적용되는 정책을 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

다음은 **show bgp ipv6** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast

BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete


Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0            0  300 i
*> 10.10.20.0/24   172.16.10.1             0            0  300 i
*  10.20.10.0/24   172.16.10.1             0            0  300 i
```

다음은 **show bgp ipv4 multicast** 명령의 샘플 출력입니다.

```
Router# show bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
*                   3FFE:C00:E:C::2                       0 3748 4697 1752 i
*                   3FFE:1100:0:CC00::1
                                                          0 1849 1273 1752 i
*  2001:618:3::/48  3FFE:C00:E:4::2          1            0 4554 1849 65002 i
*>                  3FFE:1100:0:CC00::1
                                                          0 1849 65002 i
*  2001:620::/35    2001:0DB8:0:F004::1
                                                          0 3320 1275 559 i
*                   3FFE:C00:E:9::2                       0 1251 1930 559 i
*                   3FFE:3600::A                          0 3462 10566 1930 559 i
*                   3FFE:700:20:1::11
                                                          0 293 1275 559 i
*                   3FFE:C00:E:4::2          1            0 4554 1849 1273 559 i
*                   3FFE:C00:E:B::2                       0 237 3748 1275 559 i
```

표 4-10에는 각 필드에 대한 설명이 나와 있습니다.

표 4-11 show bgp ipv6 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.

표 4-11 show bgp ipv6 필드(계속)

필드	설명
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

다음은 접두사 3FFE:500::/24에 대한 정보를 표시하는 **show bgp ipv6** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast 3FFE:500::/24

BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external

ciscoasa# show bgp ipv6 unicast

BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

show bgp ipv6 community

IPv6 BGP(Border Gateway Protocol) 라우팅 테이블의 항목을 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp ipv6community** 명령을 사용합니다.

show bgp ipv6 unicast community [*community-number*] **[exact-match]** [**local-as | no-advertise | no-export**]

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
community-number	(선택 사항) 유효한 값은 1~4294967295의 커뮤니티 번호 또는 AA:NN(자동 시스템:커뮤니티 번호, 2바이트 번호)입니다.
exact-match	(선택 사항) 정확히 일치하는 항목이 있는 경로만 표시합니다.
local-as	(선택 사항) 로컬 자동 시스템(잘 알려진 커뮤니티) 외부로 전송되지 않는 경로만 표시합니다.
no-advertise	(선택 사항) 피어(잘 알려진 커뮤니티)로 보급되지 않는 경로만 표시합니다.
no-export	(선택 사항) 로컬 자동 시스템(잘 알려진 커뮤니티) 외부로 내보낼 수 없는 경로만 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 community 명령은 IPv6에 특정하다는 점을 제외하고는 **show ip bgp community** 명령과 유사한 출력을 제공합니다.

커뮤니티는 **set community** route-map 컨피그레이션 명령으로 설정됩니다. 잘 알려진 커뮤니티 앞에 숫자 커뮤니티를 입력해야 합니다. 예를 들어 다음 문자열은 유효하지 않습니다.

```
ciscoasa# show ipv6 bgp unicast community local-as 111:12345
```

대신 다음 문자열을 사용합니다.

```
ciscoasa# show ipv6 bgp unicast community 111:12345 local-as
```

예

다음은 **show bgp ipv6 community** 명령의 샘플 출력입니다.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
```

```
     Network              Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64      ::                                   0 32768 i
*> 2001:0DB8:0:1:1::/80     ::                                   0 32768 ?
*> 2001:0DB8:0:2::/64       2001:0DB8:0:3::2                        0 2 i
*> 2001:0DB8:0:2:1::/80     2001:0DB8:0:3::2                        0 2 ?
* 2001:0DB8:0:3::1/64       2001:0DB8:0:3::2                        0 2 ?
*>                       ::                                  0 32768 ?
*> 2001:0DB8:0:4::/64       2001:0DB8:0:3::2                        0 2 ?
*> 2001:0DB8:0:5::1/64      ::                                   0 32768 ?
*> 2001:0DB8:0:6::/64       2000:0:0:3::2                        0 2 3 i
*> 2010::/64                ::                                   0 32768 ?
*> 2020::/64                ::                                   0 32768 ?
*> 2030::/64                ::                                   0 32768 ?
*> 2040::/64                ::                                   0 32768 ?
*> 2050::/64                ::                                   0 32768 ?
```

표 4-12 show bgp ipv6 community 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.

표 4-12 show bgp ipv6 community 필드(계속)

필드	설명
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 community-list

IPv6 BGP(Border Gateway Protocol) 커뮤니티 목록에서 허용하는 경로를 표시하려면 사용자 또는 특권 EXEC 모드에서 show bgp IPv6 community-list 명령을 사용합니다.

show bgp ipv6 unicast community-list {*number* | *name*} **[exact-match]**

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
number	1~199의 커뮤니티 목록 번호입니다.
name	커뮤니티 목록 이름입니다.
exact-match	(선택 사항) 정확히 일치하는 항목이 있는 경로만 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 unicast community-list 명령은 IPv6에 특정하다는 점을 제외하고는 **show ip bgp community-list** 명령과 유사한 출력을 제공합니다.

예

다음은 커뮤니티 목록 번호 3에 대한 **show bgp ipv6 community-list** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast community-list 3

BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64     2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80   2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64    ::                                     0 32768 i
*> 2001:0DB8:0:2:1::/80   ::                                     0 32768 ?
* 2001:0DB8:0:3::2/64     2001:0DB8:0:3::1                         0 1 ?
*>                       ::                                   0 32768 ?
*> 2001:0DB8:0:4::2/64    ::                                     0 32768 ?
*> 2001:0DB8:0:5::/64     2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64              2001:0DB8:0:3::1                         0 1 ?
```

```
*> 2040::/64                2001:0DB8:0:3::1                        0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                        0 1 ?
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 4-13 show bgp ipv6 community-list 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 filter-list

지정된 IPv6 필터 목록과 일치하는 경로를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp ipv6 filter-list** 명령을 사용합니다.

show bgp ipv6 unicast filter-list *access-list*-**number**

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
access-list-number	IPv6 자동 시스템 경로 액세스 목록 번호입니다. 1~199의 숫자일 수 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 filter-list 명령은 IPv6에 특정하다는 점을 제외하고는 **show ip bgp filter-list** 명령과 유사한 출력을 제공합니다.

예:

다음은 IPv6 자동 시스템 경로 액세스 목록 번호 1에 대한 **show bgp ipv6 filter-list** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast filter-list 1

BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network              Next Hop                            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                         0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:4::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 ?
*> 2001:0DB8:0:5::/64        ::                                         32768  ?
*                            2001:0DB8:0:4::2                         0 2 1 ?
*> 2001:0DB8:0:6::1/64       ::                                         32768  i
*> 2030::/64                  2001:0DB8:0:4::2                         0 1
*> 2040::/64                  2001:0DB8:0:4::2                         0 2 1 ?
*> 2050::/64                  2001:0DB8:0:4::2                         0 2 1 ?
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 4-14 show bgp ipv6 community-list 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 inconsistent-as

시작 자동 시스템이 일치하지 않는 IPv6 BGP(Border Gateway Protocol) 경로를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서show bgp ipv6 inconsistent-as 명령을 사용합니다.

show bgp ipv6 unicast inconsistent-as

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 unicast inconsistent-as 명령은 IPv6에 특정하다는 점을 제외하고는 **show ip bgp inconsistent-as** 명령과 유사한 출력을 제공합니다.

예

다음은 **show bgp ipv6 inconsistent-as** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast inconsistent-as

BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                       0 1251 4270 10318 ?
*                   3FFE:3600::A                          0 3462 6175 ?
*                   3FFE:700:20:1::11                     0 293 6175 ?
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 4-15 show bgp ipv6 community-list 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).

표 4-15 show bgp ipv6 community-list 필드(계속)

필드	설명
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 neighbors

네이버와 IPv6 BGP(Border Gateway Protocol)의 연결에 대한 정보를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 show bgp ipv6 neighbors 명령을 사용합니다.

show bgp ipv6 unicast neighbors [*ipv6-address*] [**received-routes | routes | advertised-routes | paths** *regular-expression*]

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
ipv6-address	(선택 사항) IPv6 BGP 발신 네이버의 주소입니다. 이 인수를 생략하면 모든 IPv6 네이버가 표시됩니다. 이 인수는 RFC 2373에 나와 있는 형식이어야 합니다. 즉, 콜론 사이의 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.
received-routes	(선택 사항) 지정된 네이버에서 수신된 모든 경로(허용 및 거부 모두)를 표시합니다.
routes	(선택 사항) 수신되고 허용된 모든 경로를 표시합니다. 이는 received-routes 키워드 출력의 하위 집합입니다.
advertised-routes	(선택 사항) 네트워킹 디바이스에서 네이버로 보급되는 모든 경로를 표시합니다.
paths *regular-expression*	(선택 사항) 수신된 경로와 일치시키는 데 사용되는 정규식입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 unicast neighbors는 IPv6에 특정하다는 점을 제외하고는 show ip bgp neighbors 명령과 유사한 출력을 제공합니다.

예

다음은 show bgp ipv6 neighbors 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
```

```
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 4-16 show bgp ipv6 community-list 필드

필드	설명
BGP neighbor	BGP 네이버의 IP 주소 및 자동 시스템 번호입니다. 네이버가 라우터와 동일한 자동 시스템에 있는 경우 둘 사이의 링크는 내부 링크입니다. 그렇지 않으면 외부로 간주됩니다.
remote AS	네이버의 자동 시스템 번호입니다.
internal link	이 피어가 iBGP(내부 Border Gateway Protocol) 피어임을 나타냅니다.
BGP version	원격 라우터와 통신하는 데 사용되는 BGP 버전입니다. 네이버의 라우터 ID(IP 주소)도 지정됩니다.
remote router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).

표 4-16 show bgp ipv6 community-list 필드(계속)

필드	설명
BGP state	이 BGP 연결의 상태를 나타냅니다.
up for	기본 TCP 연결이 존재한 기간입니다.
Last read	BGP에서 이 네이버의 메시지를 마지막으로 읽은 시간입니다.
hold time	피어의 메시지 간에 경과할 수 있는 최대 기간입니다.
keepalive interval	TCP 연결이 유지되도록 킵얼라이브 패킷을 전송할 시간 간격입니다.
Neighbor capabilities	이 네이버에서 보급 및 수신된 BGP 기능입니다.
Route refresh	네이버가 경로 새로 고침 기능을 사용하여 동적 소프트 재설정을 지원함을 나타냅니다.
Address family IPv6 Unicast	BGP 피어가 IPv6 연결 정보를 교환함을 나타냅니다.
Received	킵얼라이브 메시지를 포함하여 이 피어에서 수신된 총 BGP 메시지 수입니다.
notifications	피어에서 수신된 오류 메시지 수입니다.
Sent	킵얼라이브 메시지를 포함하여 이 피어로 전송된 총 BGP 메시지 수입니다.
notifications	라우터에서 이 피어로 전송한 오류 메시지 수입니다.
advertisement runs	최소 알림 간격 값입니다.
For address family	다음 필드에서 참조하는 주소 패밀리입니다.
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
neighbor version	소프트웨어에서 전송한 패킷과 이 네이버로 전송해야 하는 패킷을 추적하는 데 사용하는 번호입니다.
Route refresh request	이 네이버에서 전송 및 수신된 경로 새로 고침 요청 수입니다.
Community attribute(샘플 출력에 표시되지 않음)	이 네이버에 대해 neighbor send-community 명령이 구성되어 있는 경우 표시됩니다.
Inbound path policy(샘플 출력에 표시되지 않음)	인바운드 필터 목록 또는 경로 맵이 구성되어 있는지 여부를 나타냅니다.
Outbound path policy(샘플 출력에 표시되지 않음)	아웃바운드 필터 목록, 경로 맵 또는 표시 안 함 해제 맵이 구성되어 있는지 여부를 나타냅니다.
bgp-in(샘플 출력에 표시되지 않음)	IPv6 유니캐스트 주소 패밀리에 대한 인바운드 업데이트 접두사 필터 목록의 이름입니다.
aggregate(샘플 출력에 표시되지 않음)	IPv6 유니캐스트 주소 패밀리에 대한 아웃바운드 업데이트 접두사 필터 목록의 이름입니다.
uni-out(샘플 출력에 표시되지 않음)	IPv6 유니캐스트 주소 패밀리에 대한 아웃바운드 경로 맵의 이름입니다.
accepted prefixes	허용된 접두사 수입니다.

표 4-16 show bgp ipv6 community-list 필드(계속)

필드	설명
Prefix advertised	보급된 접두사 수입니다.
suppressed	표시되지 않는 접두사 수입니다.
withdrawn	취소된 접두사 수입니다.
history paths(샘플 출력에 표시되지 않음)	기록을 저장하기 위해 유지되는 경로 항목 수입니다.
Connections established	라우터가 TCP 연결을 설정하고 두 피어가 서로 BGP를 발신하도록 동의한 횟수입니다.
dropped	정상 조건이 실패하거나 중단된 횟수입니다.
Last reset	이 피어 세션이 마지막으로 재설정된 이후에 경과한 시간(시간:분:초)입니다.
Connection state	BGP 피어의 상태입니다.
unread input bytes	여전히 처리 중인 패킷의 바이트 수입니다.
Local host, Local port	로컬 라우터의 피어링 주소 및 포트입니다.
Foreign host, Foreign port	네이버의 피어링 주소입니다.
Event Timers	각 타이머의 시작 및 대기 모드 해제 수를 표시하는 테이블입니다.
snduna	로컬 호스트에서 전송했지만 확인 응답을 받지 않은 마지막 전송 시퀀스 번호입니다.
sndnxt	로컬 호스트가 다음에 전송할 시퀀스 번호입니다.
sndwnd	원격 호스트의 TCP 윈도우 크기입니다.
irs	초기 수신 시퀀스 번호입니다.
rcvnxt	로컬 호스트가 확인 응답을 받은 마지막 수신 시퀀스 번호입니다.
rcvwnd	로컬 호스트의 TCP 윈도우 크기입니다.
delrecvwnd	지연된 수신 창, 즉 로컬 호스트에서 연결에서 읽었지만 원격 호스트로 보급한 수신 창에서 아직 제거하지 않은 데이터입니다. 이 필드의 값은 rcvwnd 필드에 적용된 시점의 전체 크기 패킷보다 클 때까지 점진적으로 증가합니다.
SRTT	계산된 평균 왕복 시간 제한(밀리초)입니다.
RTTO	왕복 시간 제한(밀리초)입니다.
RTV	왕복 시간의 편차(밀리초)입니다.
KRTT	Karn 알고리즘을 사용하는 새 왕복 시간 제한(밀리초)입니다. 이 필드는 재전송된 패킷의 왕복 시간을 별도로 추적합니다.
minRTT	계산에 사용된 고정 값이 있는 기록된 최소 왕복 시간 제한(밀리초)입니다.
maxRTT	기록된 최대 왕복 시간 제한(밀리초)입니다.
ACK hold	로컬 호스트가 데이터를 "piggyback"하기 위해 확인 응답을 지연시킬 기간(밀리초)입니다.
Flags	BGP 패킷의 IP 우선 순위입니다.
Datagrams: Rcvd	네이버에서 수신된 업데이트 패킷 수입니다.
with data	데이터와 함께 수신된 업데이트 패킷 수입니다.

표 4-16 show bgp ipv6 community-list 필드(계속)

필드	설명
total data bytes	데이터의 총 바이트 수입니다.
Sent	전송된 업데이트 패킷 수입니다.
with data	데이터와 함께 전송된 업데이트 패킷 수입니다.
total data bytes	데이터의 총 바이트 수입니다.

다음은 advertised-routes 키워드와 함께 실행한 show bgp ipv6 neighbors 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                         0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                         0 3748 4697 i
```

다음은 routes 키워드와 함께 실행한 show bgp ipv6 neighbors 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                       0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                       0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                       0 293 1275 3748 i
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 4-17 show bgp ipv6 neighbors advertised-routes 및 routes 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.

표 4-17 show bgp ipv6 neighbors advertised-routes 및 routes 필드(계속)

필드	설명
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

다음은 paths 키워드와 함께 실행한 show bgp ipv6 neighbors 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

show bgp ipv6 neighbors paths 필드

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 값은 INTER_AS입니다.
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

다음 show bgp ipv6 neighbors 명령의 샘플 출력에서는 IPv6 주소 2000:0:0:4::2에 대한 수신된 경로를 보여 줍니다.

```
ciscoasa# show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
Network               Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64     2000:0:0:4::2                        0 2 1 i
*> 2000:0:0:2::/64     2000:0:0:4::2                        0 2 i
*> 2000:0:0:2:1::/80   2000:0:0:4::2                        0 2 ?
*> 2000:0:0:3::/64     2000:0:0:4::2                        0 2 ?
*  2000:0:0:4::1/64    2000:0:0:4::2                        0 2 ?
```

show bgp ipv6 paths

데이터베이스의 모든 IPv6 BGP(Border Gateway Protocol) 경로를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 show bgp ipv6 paths 명령을 사용합니다.

show bgp ipv6 unicast paths *regular-expression*

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
regular-expression	데이터베이스에서 수신된 경로와 일치시키는 데 사용되는 정규식입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 unicast paths 명령은 IPv6에 특정하다는 점을 제외하고는 show ip bgp paths 명령과 유사한 출력을 제공합니다.

예

다음은 show bgp ipv6 paths 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 값은 INTER_AS입니다.
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

show bgp ipv6 prefix-list

접두사 목록과 일치하는 경로를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 show bgp ipv6 prefix-list 명령을 사용합니다.

show bgp ipv6 unicast prefix-list *name*

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
name	지정된 접두사 목록입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

지정된 접두사 목록은 IPv4 접두사 목록과 형식이 유사한 IPv6 접두사 목록이어야 합니다.

예

```
다음은 show bgp ipv6 prefix-list 명령의 샘플 출력입니다.
Router# show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 quote-regexp

자동 시스템 경로 정규식과 일치하는 IPv6 BGP(Border Gateway Protocol) 경로를 따옴표로 묶인 문자열로 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 show bgp ipv6 quote-regexp 명령을 사용합니다.

show bgp ipv6 unicast quote-regexp *regular expression*

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
regular expression	BGP 자동 시스템 경로와 일치시키는 데 사용되는 정규식입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 unicast quote-regexp 명령은 IPv6에 특정하다는 점을 제외하고는 **show** ip bgp quote-regexp 명령과 유사한 출력을 제공합니다.

예

다음은 33으로 시작하거나 293을 포함하는 경로를 표시하는 show bgp ipv6 quote-regexp 명령의 샘플 출력입니다.

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*  3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 regexp

자동 시스템 경로 정규식과 일치하는 IPv6 BGP(Border Gateway Protocol) 경로를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 show bgp ipv6 regexp 명령을 사용합니다.

show bgp ipv6 unicast regexp *regular-expression*

관련 명령

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
regular-expression	BGP 자동 시스템 경로와 일치시키는 데 사용되는 정규식입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 unicast regexp 명령은 IPv6에 특정하다는 점을 제외하고는 show ip bgp regexp 명령과 유사한 출력을 제공합니다.

예

다음은 33으로 시작하거나 293을 포함하는 경로를 표시하는 show bgp ipv6 regexp 명령의 샘플 출력입니다.

```
Router# show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 route-map

라우팅 테이블에 설치하지 못한 IPv6 BGP(Border Gateway Protocol) 경로를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 show bgp ipv6 route-map 명령을 사용합니다.

show bgp ipv6 unicast route-map *name*

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
name	일치시킬 지정된 경로 맵입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

다음은 rmap이라는 경로 맵에 대한 show bgp ipv6 route-map 명령의 샘플 출력입니다.

```
Router# show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
             r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1             0    100     50 ?
*>i543::/64         2001:0DB8:101::1             0    100     50 ?
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. h - 테이블 항목이 기록입니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp ipv6 summary

모든 IPv6 BGP(Border Gateway Protocol) 연결의 상태를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 show bgp ipv6 summary 명령을 사용합니다.

show bgp ipv6 unicast summary

구문 설명

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

show bgp ipv6 unicast summary 명령은 IPv6에 특정하다는 점을 제외하고는 show ip bgp summary 명령과 유사한 출력을 제공합니다.

예

다음은 show bgp ipv6 summary 명령의 샘플 출력입니다.

```
ciscoasa# show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor          V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2  4    200    6869     6882        0    0     0  06:25:24  Active
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

필드	설명
BGP device identifier	네트워킹 디바이스의 IP 주소입니다.
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
main routing table version	기본 라우팅 테이블에 삽입된 BGP 데이터베이스의 마지막 버전입니다.
Neighbor	네이버의 IPv6 주소입니다.
V	해당 네이버로 발신된 BGP 버전 번호입니다.

필드	설명
AS	자동 시스템입니다.
MsgRcvd	해당 네이버에서 수신된 BGP 메시지입니다.
MsgSent	해당 네이버로 전송된 BGP 메시지입니다.
TblVer	해당 네이버로 전송된 BGP 데이터베이스의 마지막 버전입니다.
InQ	처리 대기 중인 해당 네이버의 메시지 수입니다.
OutQ	해당 네이버로 전송 대기 중인 메시지 수입니다.
Up/Down	BGP 세션이 Established 상태 또는 현재 상태(Established가 아닌 경우)로 유지된 기간입니다.
State/PfxRcd	디바이스가 네이버에서 수신한 BGP 세션의 현재 상태/접두사 수입니다. 최대 수(neighbor maximum-prefix 명령으로 설정)에 도달하면 문자열 "PfxRcd"가 항목에 표시되고, 네이버가 종료되며, 연결이 Idle 상태로 전환됩니다. Idle 상태의 An(Admin) 항목은 neighbor shutdown 명령을 통해 연결이 종료되었음을 나타냅니다.

show bgp neighbors

네이버와 BGP(Border Gateway Protocol)의 연결에 대한 정보를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp neighbors** 명령을 사용합니다.

show bgp neighbors [slow | *ip-address* [advertised-routes | | paths [*reg-exp*] |policy [detail] | received prefix-filter | received-routes | routes]]

구문 설명

slow	(선택 사항) 동적으로 구성된 느린 피어에 대한 정보를 표시합니다.
ip-address	(선택 사항) IPv4 네이버에 대한 정보를 표시합니다. 이 인수를 생략하면 모든 네이버에 대한 정보가 표시됩니다.
advertised-routes	(선택 사항) 네이버에 보급된 모든 경로를 표시합니다.
paths *reg-exp*	(선택 사항) 지정된 네이버에서 학습된 자동 시스템 경로를 표시합니다. 선택적 정규식을 사용하여 출력을 필터링할 수 있습니다.
policy	(선택 사항) 주소 패밀리별로 이 네이버에 적용되는 정책을 표시합니다.
detail	(선택 사항) 경로 맵, 접두사 목록, 커뮤니티 목록, ACL(Access Control List: 액세스 제어 목록), 자동 시스템 경로 필터 목록 등 자세한 정책 정보를 표시합니다.
received prefix-filter	(선택 사항) 지정된 네이버에서 전송된 접두사 목록(ORF(아웃바운드 경로 필터))를 표시합니다.
received-routes	(선택 사항) 지정된 네이버에서 수신된 모든 경로(허용 및 거부 모두)를 표시합니다.
routes	(선택 사항) 수신되고 허용된 모든 경로를 표시합니다. 이 키워드를 입력한 경우에 표시되는 출력은 **received-routes** 키워드로 표시되는 출력의 하위 집합입니다.

명령 기본값

이 명령의 출력은 모든 네이버에 대한 정보를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

show bgp neighbors 명령을 사용하여 네이버 세션에 대한 BGP 및 TCP 연결을 표시할 수 있습니다. BGP의 경우 자세한 네이버 특성, 기능, 경로 및 접두사 정보가 포함됩니다. TCP의 경우 BGP 네이버 세션 설정 및 유지 관리와 관련된 통계가 포함됩니다.

접두사 활동은 보급 및 취소된 접두사 수를 기반으로 표시됩니다. 정책 거부는 보급되었지만 출력에 표시된 기능 또는 특성에 따라 무시된 경로 수를 표시합니다.

4바이트 자동 시스템 번호의 Cisco 구현에서는 asplain(예: 65538)을 자동 시스템 번호의 기본 정규식 일치 및 출력 표시 형식으로 사용하지만 RFC 5396에 설명된 대로 asplain 형식과 asdot 형식으로 4바이트 자동 시스템 번호를 구성할 수 있습니다. 4바이트 자동 시스템 번호의 기본 정규식 일치 및 출력 표시를 asdot 형식으로 변경하려면 **clear bgp *** 명령이 뒤에 오는 **bgp asnotation dot** 명령을 사용하여 모든 현재 BGP 세션의 하드 재설정을 수행합니다.

예

예제 출력은 **show bgp neighbors** 명령에 사용할 수 있는 여러 키워드에 따라 다릅니다. 여러 키워드를 사용한 예제는 다음 섹션에 나와 있습니다.

show bgp neighbors: 예

다음 예에서는 10.108.50.2에 있는 BGP 네이버에 대한 출력을 보여 줍니다. 이 네이버는 iBGP(내부 BGP) 피어입니다. 이 네이버는 경로 새로 고침 및 정상 재시작 기능을 지원합니다.

```
ciscoasa# show bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                Sent       Rcvd
  Prefix activity:              ----       ----
    Prefixes Current:              0          0
    Prefixes Total:                0          0
    Implicit Withdraw:             0          0
    Explicit Withdraw:             0          0
    Used as bestpath:            n/a          0
    Used as multipath:           n/a          0
```

```
                                    Outbound    Inbound
  Local Policy Denied Prefixes:     --------    -------
    Total:                                 0          0
  Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다. 앞에 별표 문자(*)가 있는 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.

표 4-10에는 각 필드에 대한 설명이 나와 있습니다.

표 4-18 show bgp ipv4 필드

필드	설명
BGP neighbor	BGP 네이버의 IP 주소 및 자동 시스템 번호입니다.
remote AS	네이버의 자동 시스템 번호입니다.
local AS 300 no-prepend(화면에 표시되지 않음)	로컬 자동 시스템 번호가 수신된 외부 경로 앞에 추가되어 있지 않은지 확인합니다. 이 출력은 자동 시스템을 마이그레이션할 때 로컬 자동 시스템 숨기기를 지원합니다.
internal link	"internal link"는 iBGP 네이버에 대해 표시됩니다. "external link"는 eBGP(외부 BGP) 네이버에 대해 표시됩니다.
BGP version	원격 라우터와 통신하는 데 사용되는 BGP 버전입니다.
remote router ID	네이버의 IP 주소입니다.
BGP state	세션 협상의 FSM(Finite State Machine) 단계입니다.

표 4-18 show bgp ipv4 필드(계속)

필드	설명
up for	기본 TCP 연결이 존재한 기간(hhmmss)입니다.
Last read	BGP가 이 네이버에서 마지막으로 메시지를 수신한 이후에 경과한 시간(hhmmss)입니다.
last write	BGP가 이 네이버에 마지막으로 메시지를 전송한 이후에 경과한 시간(hhmmss)입니다.
hold time	BGP가 메시지를 수신하지 않고 이 네이버와의 세션을 유지할 시간(초)입니다.
keepalive interval	킵얼라이브 메시지가 이 네이버로 전송되는 시간 간격(초)입니다.
Neighbor capabilities	이 네이버에서 보급 및 수신된 BGP 기능입니다. 두 라우터 간에 기능이 성공적으로 교환된 경우 "advertised and received"가 표시됩니다.
Route Refresh	경로 새로 고침 기능의 상태입니다.
Graceful Restart Capability	정상 재시작 기능의 상태입니다.
Address family IPv4 Unicast	이 네이버의 IP 버전 4 유니캐스트 관련 속성입니다.
Message statistics	메시지 유형별로 구성된 통계입니다.
InQ depth is	입력 대기열의 메시지 수입니다.
OutQ depth is	출력 대기열의 메시지 수입니다.
Sent	전송된 총 메시지 수입니다.
Received	수신된 총 메시지 수입니다.
Opens	전송되거나 수신된 열어 본 메시지 수입니다.
notifications	전송되거나 수신된 알림(오류) 메시지 수입니다.
Updates	전송되거나 수신된 업데이트 메시지 수입니다.
Keepalives	전송되거나 수신된 킵얼라이브 메시지 수입니다.
Route Refresh	전송되거나 수신된 경로 새로 고침 요청 메시지 수입니다.
Total	전송되거나 수신된 총 메시지 수입니다.
Default minimum time between...	알림 전송 간의 시간 간격(초)입니다.
For address family:	다음 필드에서 참조하는 주소 패밀리입니다.
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
neighbor version	소프트웨어에서 전송한 패킷과 전송해야 하는 패킷을 추적하는 데 사용하는 번호입니다.
update-group	이 주소 패밀리에 대한 업데이트 그룹 멤버 번호입니다.
Prefix activity	이 주소 패밀리에 대한 접두사 통계입니다.
Prefixes current	이 주소 패밀리에 대해 허용된 접두사 수입니다.
Prefixes total	수신된 총 접두사 수입니다.
Implicit Withdraw	접두사가 취소되고 다시 보급된 횟수입니다.
Explicit Withdraw	접두사가 더 이상 실행할 수 없어 취소된 횟수입니다.

표 4-18 show bgp ipv4 필드(계속)

필드	설명
Used as bestpath	최상의 경로로 설치된 수신된 접두사 수입니다.
Used as multipath	다중 경로로 설치된 수신된 접두사 수입니다.
* Saved (soft-reconfig)	소프트 재구성을 지원하는 네이버와 함께 수행된 소프트 재설정 횟수입니다. 이 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
* History paths	이 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
* Invalid paths	잘못된 경로 수입니다. 이 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
Local Policy Denied Prefixes	로컬 정책 컨피그레이션으로 인해 거부된 접두사입니다. 인바운드 및 아웃바운드 정책 거부 시 카운터가 업데이트됩니다. 이 머리글 아래의 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
* route-map	인바운드 및 아웃바운드 route-map 정책 거부를 표시합니다.
* filter-list	인바운드 및 아웃바운드 filter-list 정책 거부를 표시합니다.
* prefix-list	인바운드 및 아웃바운드 prefix-list 정책 거부를 표시합니다.
* AS_PATH too long	아웃바운드 AS-path length 정책 거부를 표시합니다.
* AS_PATH loop	아웃바운드 AS-path loop 정책 거부를 표시합니다.
* AS_PATH confed info	아웃바운드 confederation 정책 거부를 표시합니다.
* AS_PATH contains AS 0	AS(자동 시스템) 0에 대한 아웃바운드 거부를 표시합니다.
* NEXT_HOP Martian	아웃바운드 martian 거부를 표시합니다.
* NEXT_HOP non-local	아웃바운드 non-local next-hop 거부를 표시합니다.
* NEXT_HOP is us	아웃바운드 next-hop-self 거부를 표시합니다.
* CLUSTER_LIST loop	아웃바운드 cluster-list loop 거부를 표시합니다.
* ORIGINATOR loop	로컬 시작 루프에 대한 아웃바운드 거부를 표시합니다.
* unsuppress-map	unsuppress-map으로 인한 인바운드 거부를 표시합니다.
* advertise-map	advertise-map으로 인한 인바운드 거부를 표시합니다.
* Well-known Community	잘 알려진 커뮤니티에 대한 인바운드 거부를 표시합니다.
* SOO loop	site-of-origin으로 인한 인바운드 거부를 표시합니다.
* Bestpath from this peer	로컬 라우터에서 가져온 최상의 경로로 인한 인바운드 거부를 표시합니다.
* Suppressed due to dampening	감소 상태에 있는 네이버 또는 링크로 인한 인바운드 거부를 표시합니다.
* Bestpath from iBGP peer	iBGP 네이버에서 가져온 최상의 경로로 인한 인바운드 거부를 표시합니다.
* Incorrect RIB for CE	CE 라우터의 RIB 오류로 인한 인바운드 거부를 표시합니다.

표 4-18 show bgp ipv4 필드(계속)

필드	설명
* BGP distribute-list	배포 목록으로 인한 인바운드 거부를 표시합니다.
Number of NLRIs...	업데이트의 네트워크 계층 연결 특성 수입니다.
Connections established	TCP와 BGP 간의 연결이 성공적으로 설정된 횟수입니다.
dropped	유효 세션이 실패하거나 중단된 횟수입니다.
Last reset	이 피어링 세션이 마지막으로 재설정된 이후에 경과한 시간입니다. 재설정 사유가 이 줄에 표시됩니다.
External BGP neighbor may be... (not shown in the display)	BGP TTL 보안 검사가 활성화되었음을 나타냅니다. 로컬 및 원격 피어를 구분할 수 있는 최대 홉 수가 이 줄에 표시됩니다.
Connection state	BGP 피어의 연결 상태입니다.
Connection is ECN Disabled	명시적인 혼잡 알림 상태(enabled 또는 disabled)입니다.
Local host: 10.108.50.1, Local port: 179	로컬 BGP 스피커의 IP 주소입니다. BGP 포트 번호는 179입니다.
Foreign host: 10.108.50.2, Foreign port: 42698	네이버 주소와 BGP 대상 포트 번호입니다.
Enqueued packets for retransmit:	TCP에서 재전송 대기 중인 패킷 수입니다.
Event Timers	TCP 이벤트 타이머입니다. 시작 및 대기 모드 해제(만료된 타이머)에 대한 카운터가 제공됩니다.
Retrans	패킷이 재전송된 횟수입니다.
TimeWait	재전송 타이머 만료 대기 시간입니다.
AckHold	확인 응답 보류 타이머입니다.
SendWnd	전송 기간입니다.
KeepAlive	킵얼라이브 패킷 수입니다.
GiveUp	확인 응답이 없어 패킷이 삭제된 횟수입니다.
PmtuAger	경로 MTU 검색 타이머입니다.
DeadWait	정지된 세그먼트에 대한 만료 타이머입니다.
iss:	초기 패킷 전송 시퀀스 번호입니다.
snduna	확인 응답을 받지 않은 마지막 전송 시퀀스 번호입니다.
sndnxt:	전송할 다음 패킷 시퀀스 번호입니다.
sndwnd:	원격 네이버의 TCP 윈도우 크기입니다.
irs:	초기 패킷 수신 시퀀스 번호입니다.
rcvnxt:	로컬로 확인 응답을 받은 마지막 수신 시퀀스 번호입니다.
rcvwnd:	로컬 호스트의 TCP 윈도우 크기입니다.

표 4-18 show bgp ipv4 필드(계속)

필드	설명
delrcvwnd:	지연된 수신 창, 즉 로컬 호스트에서 연결에서 읽었지만 원격 호스트로 보급한 수신 창에서 아직 제거하지 않은 데이터입니다. 이 필드의 값은 rcvwnd 필드에 적용된 시점의 전체 크기 패킷보다 클 때까지 점진적으로 증가합니다.
SRTT:	계산된 평균 왕복 시간 제한입니다.
RTTO:	왕복 시간 제한입니다.
RTV:	왕복 시간의 편차입니다.
KRTT:	새 왕복 시간 제한(Karn 알고리즘 사용)입니다. 이 필드는 재전송된 패킷의 왕복 시간을 별도로 추적합니다.
minRTT:	기록된 최소 왕복 시간 제한(계산에 사용된 고정 값)입니다.
maxRTT:	기록된 최대 왕복 시간 제한입니다.
ACK hold:	로컬 호스트가 추가 데이터를 전달(piggyback)하기 위해 확인 응답을 지연시킬 기간입니다.
IP Precedence value:	BGP 패킷의 IP 우선 순위입니다.
Datagrams	네이버에서 수신된 업데이트 패킷 수입니다.
Rcvd:	수신된 패킷 수입니다.
with data	데이터와 함께 전송된 업데이트 패킷 수입니다.
total data bytes	수신된 총 데이터(바이트)입니다.
Sent	전송된 업데이트 패킷 수입니다.
Second Congestion	혼잡으로 인해 전송된 두 번째 재전송 수입니다.
Datagrams: Rcvd	네이버에서 수신된 업데이트 패킷 수입니다.
out of order:	잘못된 시퀀스로 수신된 패킷 수입니다.
with data	데이터와 함께 수신된 업데이트 패킷 수입니다.
Last reset	이 피어링 세션이 마지막으로 재설정된 이후에 경과한 시간입니다.
unread input bytes	여전히 처리 중인 패킷의 바이트 수입니다.
retransmit	재전송된 패킷 수입니다.
fastretransmit	재전송 타이머가 만료되기 전에 잘못된 순서의 세그먼트에 대해 재전송된 중복 확인 응답 수입니다.
partialack	부분 확인 응답을 위한 재전송(후속 확인 응답 전의 전송 또는 후속 확인 응답이 없는 전송) 수입니다.

show bgp neighbors advertised-routes: 예

다음 예에서는 172.16.232.178 네이버에만 보급되는 경로를 표시합니다.

```
ciscoasa# show bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

표 4-19에는 각 필드에 대한 설명이 나와 있습니다.

표 4-19 show bgp neighbors advertised routes 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. s - 테이블 항목이 표시되지 않습니다. * - 테이블 항목이 유효합니다. > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. i - IGP(내부 게이트웨이 프로토콜)에서 시작된 후 **network** 라우터 컨피그레이션 명령을 통해 보급된 항목입니다. e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	항목이 설명하는 네트워크의 인터넷 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 액세스 서버에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	**set local-preference** route-map 컨피그레이션 명령으로 설정된 로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다. 경로의 원본 코드가 경로 끝에 표시됩니다. i - 항목이 IGP에서 시작된 후 **network** 라우터 컨피그레이션 명령으로 보급되었습니다. e - 경로가 EGP에서 시작되었습니다. ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 경로입니다.

show bgp neighbors paths: 예

다음은 **paths** 키워드와 함께 실행한 **show bgp neighbors** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp neighbors 172.29.232.178 paths ^10

Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

표 4-20에는 각 필드에 대한 설명이 나와 있습니다.

표 4-20 show bgp neighbors paths 필드

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 값은 INTER_AS입니다.
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

show bgp neighbors received prefix-filter: 예

다음 예에서는 10.0.0.0 네트워크가 192.168.20.72 네이버에서 수신한 모든 경로를 필터링하는 접두사 목록을 보여 줍니다.

```
ciscoasa# show bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

표 4-21에는 각 필드에 대한 설명이 나와 있습니다.

표 4-21 show bgp neighbors received prefix filter 필드

필드	설명
Address family	접두사 필터를 수신한 주소 패밀리 모드입니다.
ip prefix-list	지정된 네이버에서 전송된 접두사 목록입니다.

show bgp neighbors policy: 예

다음 샘플 출력에서는 192.168.1.2에 있는 네이버에 적용되는 정책을 보여 줍니다. 네이버 디바이스에 구성된 정책이 출력에 표시됩니다.

```
ciscoasa# show bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

show bgp neighbors: 예

다음은 172.16.1.2에 있는 BGP 네이버에 대해 BGP TCP 경로 MTU(최대 전송 단위) 검색이 활성화되어 있는지 확인하는 **show bgp neighbors** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

다음은 192.168.3.2에 있는 외부 BGP 피어에 대한 BGP 정상 재시작 기능의 상태를 확인하는 **show bgp neighbors** 명령의 일부 출력입니다. 이 BGP 피어에 대해 정상 재시작이 비활성화된 것으로 표시됩니다.

```
ciscoasa# show bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

show bgp paths

데이터베이스의 모든 BGP 경로를 표시하려면 EXEC 모드에서 **show bgp paths** 명령을 사용합니다.

show bgp paths

Cisco 10000 Series Router

show bgp paths *regexp*

구문 설명

regexp	BGP 자동 시스템 경로와 일치시킬 정규식입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 특권 EXEC 모드에 실행된 **show bgp paths** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp paths

Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

표 4-22에는 각 필드에 대한 설명이 나와 있습니다.

표 4-22 show bgp paths 필드

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Hash	경로가 저장되는 해시 버킷입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 값은 INTER_AS입니다.
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

show bgp policy-list

구성된 정책 목록 및 정책 목록 항목에 대한 정보를 표시하려면 사용자 EXEC 모드에서 **show bgp policy-list** 명령을 사용합니다.

show bgp policy-list [*policy-list-name*]

구문 설명

policy-list-name	(선택 사항) 이 인수를 사용하여 지정된 정책 목록에 대한 정보를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 **show bgp policy-list** 명령의 샘플 출력입니다. 이 명령의 출력에는 정책 목록 이름 및 구성된 일치 절이 표시됩니다. 다음 샘플 출력은 표시되는 출력과 유사합니다.

```
ciscoasa# show bgp policy-list

policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

show bgp prefix-list

접두사 목록 또는 접두사 목록 항목에 대한 정보를 표시하려면 사용자 또는 특권 EXEC 모드에서 **show bgp prefix-list** 명령을 사용합니다.

show bgp prefix-list [detail | summary][*prefix-list-name* [**seq** *sequence-number* | *network/length* [**longer| first-match**]]]

구문 설명

detail | summary	(선택 사항) 모든 접두사 목록에 대한 상세 정보 및 요약 정보를 표시합니다.
first-match	(선택 사항) 지정된 *network/length*와 일치하는 지정된 접두사 목록의 첫 번째 항목을 표시합니다.
longer	(선택 사항) 지정된 *network/length*와 일치하거나 더 구체적인 지정된 접두사 목록의 모든 항목을 표시합니다.
network/length	(선택 사항) 이 네트워크 주소 및 넷마스크(비트)를 사용하는 지정된 접두사 목록의 모든 항목을 표시합니다.
prefix-list-name	(선택 사항) 특정 접두사 목록의 항목을 표시합니다.
seq *sequence-number*	(선택 사항) 지정된 접두사 목록에서 지정된 시퀀스 번호가 있는 접두사 목록 항목만 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음 예에서는 test라는 접두사 목록에 대한 세부사항이 포함된 **show bgp prefix-list** 명령의 출력을 보여 줍니다.

```
ciscoasa# show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

show bgp regexp

자동 시스템 경로 정규식과 일치하는 경로를 표시하려면 EXEC 모드에서 **show bgp regexp** 명령을 사용합니다.

show bgp regexp *regexp*

구문 설명

regexp	BGP 자동 시스템 경로와 일치시킬 정규식입니다. 자동 시스템 번호 형식에 대한 자세한 내용은 **router bgp** 명령을 참고하십시오.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

4바이트 자동 시스템 번호의 Cisco 구현에서는 asplain(예: 65538)을 자동 시스템 번호의 기본 정규식 일치 및 출력 표시 형식으로 사용하지만 RFC 5396에 설명된 대로 asplain 형식과 asdot 형식으로 4바이트 자동 시스템 번호를 구성할 수 있습니다. 4바이트 자동 시스템 번호의 기본 정규식 일치 및 출력 표시를 asdot 형식으로 변경하려면 **clear bgp *** 명령이 뒤에 오는 **bgp asnotation dot** 명령을 사용하여 모든 현재 BGP 세션의 하드 재설정을 수행합니다.

원활한 변환을 위해 4바이트 자동 시스템 번호를 사용하여 식별된 자동 시스템 내의 모든 BGP 스피커를 4바이트 자동 시스템 번호를 지원하도록 업그레이드하는 것이 좋습니다.

예

다음은 특권 EXEC 모드에 실행된 **show bgp regexp** 명령의 샘플 출력입니다.

```
Router# show bgp regexp 108$

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
```

```
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

bgp asnotation dot 명령이 구성된 후에는 4바이트 자동 시스템 경로에 대한 정규식 일치 형식이 asdot 표기법 형식으로 변경됩니다. asplain 또는 asdot 형식을 사용하여 정규식에서 4바이트 자동 시스템 번호를 구성할 수 있지만 현재 기본 형식을 사용하여 구성한 4바이트 자동 시스템 번호만 일치합니다. 첫 번째 예에서 **show bgp regexp** 명령은 asplain 형식의 4바이트 자동 시스템 번호로 구성되었습니다. 기본 형식이 현재 asdot 형식이므로 일치에 실패하고 아무 것도 출력되지 않습니다. asdot 형식을 사용한 두 번째 예에서는 일치에 통과하고 4바이트 자동 시스템 경로에 대한 정보가 asdot 표기법으로 표시됩니다.

참고 asdot 표기법에서는 Cisco 정규식에서 특수 문자인 마침표를 사용합니다. 특별한 의미를 제거하기 위해 마침표 앞에 역슬래시를 사용합니다.

```
Router# show bgp regexp ^65536$

Router# show bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

다음은 4바이트 자동 시스템 번호를 표시하기 위해 입력된 **bgp asnotation dot** 명령 뒤의 **show bgp regexp** 명령에 대한 샘플 출력입니다.

참고 asdot 표기법에서는 Cisco 정규식에서 특수 문자인 마침표를 사용합니다. 특별한 의미를 제거하기 위해 마침표 앞에 역슬래시를 사용합니다.

```
Router# show bgp regexp ^1\.14$

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.14   i
```

show bgp replication

BGP(Border Gateway Protocol) 업데이트 그룹에 대한 업데이트 복제 통계를 표시하려면 EXEC 모드에서 **show bgp replication** 명령을 사용합니다.

show bgp replication [*index-group* | *ip-address***]**

구문 설명

index-group	(선택 사항) 해당 인덱스 번호를 가진 업데이트 그룹에 대한 업데이트 복제 통계를 표시합니다. 업데이트 그룹 인덱스 번호의 범위는 1~4294967295입니다.
ip-address	(선택 사항) 이 네이버에 대한 업데이트 복제 통계를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령의 출력에는 BGP 업데이트 그룹 복제 통계가 표시됩니다.

아웃바운드 정책이 변경된 경우 라우터는 업데이트 그룹 멤버십을 자동으로 다시 계산하고 3분 타이머가 만료된 후 아웃바운드 소프트 재설정을 트리거하여 변경 사항을 적용합니다. 이 동작은 네트워크 운영자에게 실수한 경우 컨피그레이션을 변경할 수 있는 시간을 제공하기 위한 것입니다. **clearbgp** *ip-address* **soft out** 명령을 입력하여 타이머가 만료되기 전에 아웃바운드 소프트 재설정을 수동으로 활성화할 수 있습니다.

예

다음 **show bgp replication** 명령의 샘플 출력에서는 모든 네이버에 대한 업데이트 그룹 복제 정보를 보여 줍니다.

```
ciscoasa# show bgp replication

BGP Total Messages Formatted/Enqueued : 0/0

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
The following sample output from the show bgp replication command shows update-group
Router# show bgp replication 10.4.9.5

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         2 internal        2        10.4.9.5        0        0      0      0
```

표 4-23에는 각 필드에 대한 설명이 나와 있습니다.

표 4-23 show bgp replication 필드

필드	설명
Index	업데이트 그룹의 인덱스 번호입니다.
Type	피어의 유형(internal 또는 external)입니다.
Members	동적 업데이트 피어 그룹의 멤버 수입니다.
Leader	동적 업데이트 피어 그룹의 첫 번째 멤버입니다.

show bgp rib-failure

RIB(Routing Information Base) 테이블에 설치하지 못한 BGP(Border Gateway Protocol) 경로를 표시하려면 특권 EXEC 모드에서 **show bgp rib-failure** 명령을 사용합니다.

show bgp rib-failure

구문 설명

이 명령에는 키워드 또는 인수가 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 **show bgp rib-failure** 명령의 샘플 출력입니다.

```
ciscoasa# show bgp rib-failure

Network          Next Hop                  RIB-failure   RIB-NH Matches
10.1.15.0/24     10.1.35.5          Higher admin distance             n/a
10.1.16.0/24     10.1.15.1          Higher admin distance             n/a
```

표 4-24에는 각 필드에 대한 설명이 나와 있습니다.

표 4-24 show bgp rib-failure 필드

필드	설명
Network	네트워크 엔터티의 IP 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 라우터에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.

표 4-24 show bgp rib-failure 필드(계속)

필드	설명
RIB-failure	RIB 오류 원인입니다. 더 높은 관리 영역은 고정 경로와 같은 더 나은(더 낮은) 관리 영역이 있는 경로가 IP 라우팅 테이블에 이미 있음을 의미합니다.
RIB-NH Matches	더 높은 관리 영역이 RIB-failure 열에 표시되고 사용 중인 주소 패밀리에 대해 **bgp suppress-inactive**가 구성된 경우에만 적용되는 경로 상태입니다. 다음 세 가지 선택 항목이 있습니다. • Yes - RIB의 경로에 BGP 경로와 동일한 다음 홉이 있거나 다음 홉이 BGP 다음 홉과 동일한 인접성으로 재귀적으로 작동함을 의미합니다. • No - RIB의 다음 홉이 BGP 경로의 다음 홉과 다르게 재귀적으로 작동함을 의미합니다. • n/a - 사용 중인 주소 패밀리에 대해 **bgp suppress-inactive**가 구성되어 있지 않습니다.

show bgp summary

모든 BGP(Border Gateway Protocol) 연결의 상태를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show bgp summary** 명령을 사용합니다.

show bgp summary

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

show bgp summary 명령은 모든 BGP 네이버 연결에 대한 BGP 경로, 접두사 및 특성 정보를 표시하는 데 사용됩니다.

접두사는 IP 주소와 네트워크 마스크입니다. 이는 전체 네트워크, 네트워크의 하위 집합 또는 단일 호스트 경로를 나타낼 수 있습니다. 경로는 지정된 대상에 대한 경로입니다. 기본적으로 BGP는 각 대상에 대해 단일 경로만 설치합니다. 다중 경로가 구성된 경우 BGP는 각 다중 모드 경로에 대한 경로 항목을 설치하며, 다중 모드 경로 중 하나의 경로만 최상의 경로로 표시됩니다.

BGP 특성 및 캐시 항목은 개별적으로 표시되거나 함께 표시됩니다. 함께 표시될 경우 최상의 경로 선택 프로세스가 영향을 받습니다. 이 출력의 필드는 관련 BGP 기능이 구성되어 있거나 특성이 수신된 경우에 표시됩니다. 메모리 사용량은 바이트 단위로 표시됩니다.

4바이트 자동 시스템 번호의 Cisco 구현에서는 asplain(예: 65538)을 자동 시스템 번호의 기본 정규식 일치 및 출력 표시 형식으로 사용하지만 RFC 5396에 설명된 대로 asplain 형식과 asdot 형식으로 4바이트 자동 시스템 번호를 구성할 수 있습니다. 4바이트 자동 시스템 번호의 기본 정규식 일치 및 출력 표시를 asdot 형식으로 변경하려면 **clear bgp *** 명령이 뒤에 오는 **bgp asnotation dot** 명령을 사용하여 모든 현재 BGP 세션의 하드 재설정을 수행합니다.

예

다음은 특권 EXEC 모드에 실행된 **show bgp summary** 명령의 샘플 출력입니다.

```
Router# show bgp summary

BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

표 4-25에는 각 필드에 대한 설명이 나와 있습니다.

표 4-25 show bgp summary 필드

필드	설명
BGP router identifier	**bgp router-id** 명령으로 지정된 라우터 식별자, 루프백 주소 또는 최상위 IP 주소입니다(우선 순위 및 가용성 순).
BGP table version	BGP 데이터베이스의 내부 버전 번호입니다.
main routing table version	기본 라우팅 테이블에 삽입된 BGP 데이터베이스의 마지막 버전입니다.
...network entries	BGP 데이터베이스에 있는 고유한 접두사 항목 수입니다.
...using ... bytes of memory	같은 줄에 표시된 경로, 접두사 또는 특성 항목에 사용되는 메모리(바이트)입니다.
...path entries using	BGP 데이터베이스에 있는 경로 항목 수입니다. 지정된 대상에 대해 단일 경로 항목만 설치됩니다. 다중 경로가 구성된 경우 다중 모드 경로의 각 경로에 대해 경로 항목이 설치됩니다.
...multipath network entries using	지정된 대상에 대해 설치된 다중 경로 항목 수입니다.
* ...BGP path/bestpath attribute entries using	경로가 최상의 경로로 선택된 고유한 BGP 특성 조합 수입니다.
* ...BGP rrinfo entries using	고유한 ORIGINATOR 및 CLUSTER_LIST 특성 조합 수입니다.
...BGP AS-PATH entries using	고유한 AS_PATH 항목 수입니다.
...BGP community entries using	고유한 BGP 커뮤니티 특성 조합 수입니다.
*...BGP extended community entries using	고유한 확장 커뮤니티 특성 조합 수입니다.
BGP route-map cache entries using	BGP route-map 일치 및 set 절 조합 수입니다. 0 값은 경로 캐시가 비어 있음을 나타냅니다.

표 4-25 show bgp summary 필드(계속)

필드	설명
...BGP filter-list cache entries using	AS-path 액세스 목록 허용 또는 거부 문과 일치하는 filter-list 항목 수입니다. 0 값은 filter-list 캐시가 비어 있음을 나타냅니다.
BGP advertise-bit cache entries using	(Cisco IOS Release 12.4(11)T 이상에만 해당) 보급된 비트 필드 항목 수 및 연계된 메모리 사용량입니다. 비트 필드 항목은 접두사가 동료에게 보급될 때 생성되는 정보 조각(1비트)을 나타냅니다. 보급된 비트 캐시는 필요할 때 동적으로 생성됩니다.
...received paths for inbound soft reconfiguration	인바운드 소프트 재컨피그레이션에 대해 수신 및 저장된 경로 수입니다.
BGP using...	BGP 프로세스에서 사용된 총 메모리 양(바이트)입니다.
Dampening enabled...	BGP 감소가 활성화되었음을 나타냅니다. 누적된 페널티가 있는 경로 수 및 감소된 경로 수가 이 줄에 표시됩니다.
BGP activity...	경로 또는 접두사에 대해 메모리가 할당되거나 해제된 횟수를 표시합니다.
Neighbor	네이버의 IP 주소입니다.
V	네이버로 발신된 BGP 버전 번호입니다.
AS	자동 시스템 번호입니다.
MsgRcvd	네이버에서 수신된 메시지 수입니다.
MsgSent	네이버로 전송된 메시지 수입니다.
TblVer	네이버로 전송된 BGP 데이터베이스의 마지막 버전입니다.
InQ	처리 대기 중인 네이버의 메시지 수입니다.
OutQ	네이버로 전송 대기 중인 메시지 수입니다.
Up/Down	BGP 세션이 Established 상태 또는 현재 상태(Established 상태가 아닌 경우)로 유지된 기간입니다.
State/PfxRcd	BGP 세션의 현재 상태 및 네이버 또는 피어 그룹에서 수신된 접두사 수입니다. 최대 수(**neighbor maximum-prefix** 명령으로 설정)에 도달하면 문자열 "PfxRcd"가 항목에 표시되고, 네이버가 종료되며, 연결이 Idle로 설정됩니다. Idle 상태의 An(Admin) 항목은 **neighbor shutdown** 명령을 통해 연결이 종료되었음을 나타냅니다.

다음 **show bgp summary** 명령의 출력에서는 BGP 네이버 192.168.3.2가 동적으로 생성되었으며, 수신 대기 범위 그룹 group192의 멤버임을 보여 줍니다. 또한 이 출력에서는 group192라는 수신 대기 범위 그룹에 대해 IP 접두사 범위 192.168.0.0/16이 정의되었음을 보여 줍니다. Cisco IOS Release 12.2(33)SXH 이상에서는 BGP 동적 네이버 기능에 피어 그룹(수신 대기 범위 그룹)과 연계된 서브넷 범위를 사용한 BGP 네이버 피어의 동적 생성을 지원하는 기능이 도입되었습니다.

```
ciscoasa# show bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
```

```
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

다음 **show bgp summary** 명령의 출력에서는 서로 다른 4바이트 자동 시스템 번호 65536 및 65550에 있는 두 개의 BGP 네이버 192.168.1.2 및 192.168.3.2를 보여 줍니다. 로컬 자동 시스템 65538도 4바이트 자동 시스템 번호이며, 이러한 번호는 기본 asplain 형식으로 표시됩니다.

```
Router# show bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15      0
```

다음 **show bgp summary** 명령의 출력에서는 동일한 BGP 네이버 두 개를 보여 주지만 4바이트 자동 시스템 번호가 asdot 표기법 형식으로 표시되어 있습니다. 표시 형식을 변경하려면 라우터 컨피그레이션 모드에서 **bgp asnotation dot** 명령을 구성해야 합니다.

```
Router# show bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24      0
```

다음 예에서는 **show bgp summary slow** 명령의 샘플 출력을 표시합니다.

```
ciscoasa> show bgp summary slow
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

show bgp system-config

사용자 상황에서 시스템 상황의 bgp에 대한 실행 중인 컨피그레이션을 표시하려면 사용자 또는 특권 EXEC 모드에서 **show bgp system-config** 명령을 사용합니다.

show bgp system-config

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC, 사용자 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 인수나 키워드 없이 사용자 상황에서만 사용할 수 있습니다. 이 명령은 시스템 상황에 의해 사용자 상황에 적용된 실행 중인 컨피그레이션을 확인하는 데 유용할 수 있습니다.

예

다음 샘플 출력은 사용자 EXEC 모드에서 **show bgp system-config** 명령을 입력한 경우에 표시되는 출력과 유사합니다.

```
ciscoasa/c1(config)# show bgp system-config
router bgp 1
 bgp log-neighbor-changes
 no bgp always-compare-med
 no bgp asnotation dot
 no bgp bestpath med
 no bgp bestpath compare-routerid
 bgp default local-preference 100
 no bgp deterministic-med
 bgp enforce-first-as
 bgp maxas-limit 0
 bgp transport path-mtu-discovery
 timers bgp 60 180 0
 address-family ipv4 unicast
  bgp scan-time 0
  bgp nexthop trigger enable
  bgp nexthop trigger delay 5
 exit-address-family
```

show blocks

패킷 버퍼 사용률을 표시하려면 특권 EXEC 모드에서 **show blocks** 명령을 사용합니다.

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** | [**exhaustion snapshot** | **history** [**list**] [*1-MAX_NUM_SNAPSHOT* | *index*] [**detail**]]

구문 설명

address *hex*	(선택 사항) 이 주소에 해당하는 블록을 16진수로 표시합니다.
all	(선택 사항) 모든 블록을 표시합니다.
assigned	(선택 사항) 할당되고 애플리케이션에서 사용 중인 블록을 표시합니다.
detail	(선택 사항) 각 고유 대기열 유형에 대한 첫 번째 블록의 일부(128바이트)를 표시합니다.
dump	(선택 사항) 헤더 및 패킷 정보를 포함하여 전체 블록 내용을 표시합니다. 덤프와 패킷의 차이점은 덤프에는 헤더와 패킷 사이의 추가 정보가 포함된다는 점입니다.
diagnostics	(선택 사항) 블록 진단을 표시합니다.
exhaustion snapshot	(선택 사항) 생성한 스냅샷 중 마지막 x개(여기서 x는 현재 10)와 마지막 스냅샷의 타임스탬프를 인쇄합니다. 스냅샷을 생성한 후 다른 스냅샷을 생성하려면 5분 이상이 경과해야 합니다.
free	(선택 사항) 사용할 수 있는 블록을 표시합니다.
header	(선택 사항) 블록의 헤더를 표시합니다.
history *1-MAX_NUM_SNAPSHOT* **history** *index* **history list**	**history** 옵션은 최근 스냅샷 및 기록에 있는 모든 스냅샷을 표시합니다. **history list** 옵션은 기록에 있는 스냅샷의 요약을 표시합니다. **history** *index* 옵션은 기록에 있는 스냅샷의 인덱스를 표시합니다. **history** *1-MAX_NUM_SNAPSHOT* 옵션은 기록에 있는 하나의 스냅샷만 표시합니다.
old	(선택 사항) 할당된 지 1분이 넘은 블록을 표시합니다.
packet	(선택 사항) 블록의 헤더와 패킷의 내용을 표시합니다.
pool *size*	(선택 사항) 특정 크기의 블록을 표시합니다.
queue history	(선택 사항) ASA에서 블록을 소진한 경우 블록이 할당된 위치를 표시합니다. 경우에 따라 블록이 풀에서 할당되지만 대기열에 할당되지는 않습니다. 이 경우 위치는 블록을 할당한 코드 주소입니다.
summary	(선택 사항) 이 클래스의 블록을 할당한 애플리케이션의 프로그램 주소, 이 클래스의 블록을 해제한 애플리케이션의 프로그램 주소 및 이 클래스의 유효한 블록이 속한 대기열별로 정렬된 블록 사용량에 대한 자세한 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	**pool summary** 옵션이 추가되었습니다.
8.0(2)	dupb 블록에서는 4바이트 블록 대신 이제 길이가 0인 블록을 사용합니다. 0바이트 블록에 대한 줄이 추가되었습니다.
9.1(5)	**exhaustion snapshot**, **history list**, **history** *index*, 및 **history** *1-MAX_NUM_SNAPSHOT* 옵션이 추가되었습니다.

사용 지침

show blocks 명령은 ASA가 오버로드되었는지 여부를 확인하는 데 유용합니다. 이 명령은 미리 할당된 시스템 버퍼 사용률을 나열합니다. 가득 찬 메모리 상태는 트래픽이 ASA를 통해 이동하고 있는 경우에는 문제가 되지 않습니다. **show conn** 명령을 사용하여 트래픽이 이동하고 있는지 확인할 수 있습니다. 트래픽이 이동하지 않는데 메모리가 가득 찬 경우에는 문제가 있을 수 있습니다.

SNMP를 사용하여 이 정보를 볼 수도 있습니다.

보안 상황에서 표시되는 정보에는 사용 중인 블록 및 블록 사용량의 상위 워터마크에 대한 시스템 수준 정보 및 상황별 정보가 포함됩니다.

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 단일 모드에서 실행된 **show blocks** 명령의 샘플 출력입니다.

```
ciscoasa# show blocks
  SIZE    MAX    LOW    CNT
     0    100     99    100
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
  1550   4716   3177   3184
 16384     10     10     10
  2048   1000   1000   1000
```

표 4-26에는 각 필드에 대한 설명이 나와 있습니다.

표 4-26 show blocks 필드

필드	설명
SIZE	블록 풀의 크기(바이트)입니다. 각 크기는 특정 유형을 나타냅니다.
0	dupb 블록에서 사용됩니다.
4	DNS, ISAKMP, URL 필터링, uauth, TFTP 및 TCP 모듈과 같은 애플리케이션에서 기존 블록을 복제합니다. 또한 이 크기의 블록은 일반적으로 코드를 통해 드라이버 등으로 패킷을 전송하는 데 사용될 수 있습니다.

표 4-26 show blocks 필드(계속)

필드	설명
80	TCP 가로채기에서 확인 응답 패킷을 생성하는 데 사용되거나 대체작동 hello 메시지에 사용됩니다.
256	상태 저장 대체작동 업데이트, 시스템 로깅 및 기타 TCP 기능에 사용됩니다. 이러한 블록은 주로 상태 저장 대체작동 메시지에 유용합니다. 활성 ASA에서 패킷을 생성한 후 대기 ASA로 전송하여 변환 및 연결 테이블을 생성합니다. 트래픽 양이 많아 연결 비율이 높거나 연결이 끊어질 수 있는 상황에서는 사용 가능한 블록 수가 0으로 감소할 수 있습니다. 이는 하나 이상의 연결이 대기 ASA로 업데이트되지 않았음을 의미합니다. 상태 저장 대체작동 프로토콜은 누락된 변환 또는 연결을 다음 번에 포착합니다. 256바이트 블록에 대한 CNT 열이 연장된 기간 동안 0에서 유지되거나 0에 근접한 경우에는 ASA에서 처리하는 초당 연결 수로 인해 ASA가 변환 및 연결 테이블을 유지하기 어렵습니다. 또한 ASA에서 전송된 syslog 메시지는 256바이트 블록을 사용하지만 256바이트 블록 풀을 소진시키는 양에서는 일반적으로 해제되지 않습니다. CNT 열에 256바이트 블록 수가 0에 가까운 것으로 표시된 경우 Debugging(수준 7)에서 syslog 서버에 기록하고 있지 않은지 확인하십시오. 이는 ASA 컨피그레이션의 기록 트랩 줄에 표시됩니다. 디버깅을 위해 추가 정보가 필요한 경우가 아니면 Notification(수준 5) 이하에서 기록을 설정하는 것이 좋습니다.
1550	ASA를 통해 처리할 이더넷 패킷을 저장하는 데 사용됩니다. 패킷이 ASA 인터페이스로 들어오면 입력 인터페이스 대기열에 배치되고 운영 체제로 전달되며 블록에 배치됩니다. ASA는 보안 정책에 따라 패킷을 허용할지 또는 거부할지 결정한 다음 아웃바운드 인터페이스의 출력 대기열을 통과하도록 패킷을 처리합니다. ASA에서 트래픽 부하를 유지하는 데 문제가 있는 경우 사용 가능한 블록 수가 0에 가까운 곳을 가리킵니다(명령 출력의 CNT 열에 표시됨). CNT 열이 0인 경우에는 ASA에서 추가 블록을 할당합니다. 이 명령을 실행한 경우 최대값은 1550바이트 블록에 대해 8192보다 클 수 있습니다. 더 이상 사용 가능한 블록이 없으면 ASA에서 패킷을 삭제합니다.
16384	64비트 66MHz 기가비트 이더넷 카드(i82543)에만 사용됩니다. 이더넷 패킷에 대한 자세한 내용은 1550에 대한 설명을 참고하십시오.
2048	컨트롤 업데이트에 사용되는 가이드 프레임 또는 컨트롤입니다.
MAX	지정된 바이트 블록 풀에 사용할 수 있는 최대 블록 수입니다. 최대 블록 수는 부팅 시 메모리에서 할당됩니다. 일반적으로 최대 블록 수는 변경되지 않습니다. 단, ASA에서 필요할 때 동적으로 추가 블록을 생성할 수 있는 256바이트 및 1550바이트 블록은 예외입니다. 이 명령을 실행한 경우 최대값은 1550바이트 블록에 대해 8192보다 클 수 있습니다.
LOW	Low-water mark. 이 숫자는 ASA의 전원이 켜지거나 블록을 마지막으로 지운(**clear blocks** 명령 사용) 이후에 사용 가능한 이 크기의 최소 블록 수를 나타냅니다. LOW 열의 0은 메모리가 가득 찬 이전 이벤트를 나타냅니다.
CNT	해당 특정 크기의 블록 풀에서 사용할 수 있는 현재 블록 수입니다. CNT 열의 0은 메모리가 현재 가득 찼음을 의미합니다.

다음은 **show blocks all** 명령의 샘플 출력입니다.

```
ciscoasa# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

표 4-27에는 각 필드에 대한 설명이 나와 있습니다.

표 4-27 show blocks all 필드

필드	설명
Block	블록 주소입니다.
allocd_by	블록을 마지막으로 사용한 애플리케이션의 프로그램 주소입니다(사용되지 않은 경우 0).
freed_by	블록을 마지막으로 해제한 애플리케이션의 프로그램 주소입니다.
data size	블록 내에 있는 애플리케이션 버퍼/패킷 데이터의 크기입니다.
alloccnt	블록이 존재한 이후 이 블록이 사용된 횟수입니다.
dup_cnt	이 블록에 대한 현재 참조 수입니다. 사용된 경우 0은 1회 참조, 1은 2회 참조를 의미합니다.
oper	블록에서 마지막으로 수행된 네 가지 작업(alloc, get, put 또는 free) 중 하나입니다.
location	블록을 사용하는 애플리케이션 또는 블록을 마지막으로 할당한 애플리케이션의 프로그램 주소입니다(allocd_by 필드와 동일).

다음은 상황에서 실행된 **show blocks** 명령의 샘플 출력입니다.

```
ciscoasa/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

다음은 **show blocks queue history** 명령의 샘플 출력입니다.

```
ciscoasa# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
```

```
      1     1 put                                    contextb
      1     1 put                                    contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                                    contexta
     15     1 put                                    contexta
      1     1 put                                    contexta
      1     1 put                                    contextb
      1     1 put                                    contextc
...
```

다음은 **show blocks queue history detail** 명령의 샘플 출력입니다.

```
ciscoasa# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                                    contexta
     15     1 put                                    contexta
      1     1 put                                    contexta
      1     1 put                                    contextb
      1     1 put                                    contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                                    contexta
      1     1 put                                    contexta
      1     1 put                                    contexta
      1     1 put                                    contextb
      1     1 put                                    contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

다음은 **show blocks pool summary** 명령의 샘플 출력입니다.

```
ciscoasa# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

다음은 **show blocks exhaustion history list** 명령의 샘플 출력입니다.

```
ciscoasa# show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

표 4-28에는 각 필드에 대한 설명이 나와 있습니다.

표 4-28 show blocks pool summary 필드

필드	설명
total_count	지정된 클래스에 대한 블록 수입니다.
miss_count	기술적인 이유 때문에 지정된 범주에 보고되지 않은 블록 수입니다.
Freed_pc	이 클래스의 블록을 해제한 애플리케이션의 프로그램 주소입니다.
Alloc_pc	이 클래스의 블록을 할당한 애플리케이션의 프로그램 주소입니다.
Queue	이 클래스의 유효한 블록이 속한 대기열입니다.
valid_cnt	현재 할당된 블록 수입니다.
invalid_cnt	현재 할당되지 않은 블록 수입니다.
Invalid Bad qtype	이 대기열이 해제되고 콘텐츠가 무효화되거나 이 대기열이 초기화되지 않았습니다.
Valid tcp_usr_conn_inp	대기열이 유효합니다.

관련 명령

명령	설명
blocks	블록 진단에 할당된 메모리를 늘립니다.
clear blocks	시스템 버퍼 통계를 지웁니다.
show conn	활성 연결을 표시합니다.

show boot device (IOS)

기본 부트 파티션을 보려면 **show boot device** 명령을 사용합니다.

show boot device [*mod_num*]

구문 설명

mod_num	(선택 사항) 모듈 번호를 지정합니다. **show module** 명령을 사용하여 설치된 모듈과 해당 번호를 볼 수 있습니다.

기본값

기본 부트 파티션은 cf:4입니다.

명령 모드

특권 EXEC

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 Cisco IOS 소프트웨어의 설치된 각 ASA에 대한 부트 파티션을 표시하는 **show boot device** 명령의 샘플 출력입니다.

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

관련 명령

명령	설명
boot device (IOS)	기본 부트 파티션을 설정합니다.
show module (IOS)	설치된 모든 모듈을 표시합니다.

show bootvar

부트 파일 및 컨피그레이션 속성을 표시하려면 특권 EXEC 모드에서 **show bootvar** 명령을 사용합니다.

show bootvar

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

BOOT 변수는 여러 디바이스에서 부팅 가능한 이미지 목록을 지정합니다. CONFIG_FILE 변수는 시스템을 초기화하는 동안 사용되는 컨피그레이션 파일을 지정합니다. 이러한 변수는 각각 **boot system** 명령 및 **boot config** 명령을 사용하여 설정합니다.

예

BOOT 변수는 disk0:/f1_image를 포함합니다. 이는 시스템이 다시 로드될 때 부팅되는 이미지입니다. BOOT의 현재 값은 disk0:/f1_image; disk0:/f1_backupimage입니다. 이 값은 **boot system** 명령을 통해 BOOT 변수가 수정되었지만 실행 중인 컨피그레이션이 **write memory** 명령을 통해 저장되지 않았음을 의미합니다. 실행 중인 컨피그레이션이 저장되면 BOOT 변수 및 현재 BOOT 변수가 둘 다 disk0:/f1_image; disk0:/f1_backupimage가 됩니다. 부트 로더는 실행 중인 컨피그레이션이 저장된 것으로 가정하여 disk0:/f1image부터 시작해 BOOT 변수의 내용을 로드하려고 하지만 실행 중인 컨피그레이션이 없거나 잘못된 경우에는 disk0:1/f1_backupimage를 부팅합니다.

CONFIG_FILE 변수는 시스템 시작 컨피그레이션을 가리킵니다. 다음 예에는 설정되어 있지 않으므로 시작 컨피그레이션 파일이 **boot config** 명령으로 지정된 기본값입니다. 현재 CONFIG_FILE 변수는 **boot config** 명령을 사용하여 수정하고 **write memory** 명령을 사용하여 저장할 수 있습니다.

다음은 **show bootvar** 명령의 샘플 출력입니다.

```
ciscoasa# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
ciscoasa#
```

관련 명령

명령	설명
boot	시작할 때 사용되는 컨피그레이션 파일 또는 이미지 파일을 지정합니다.

show bridge-group

할당된 인터페이스, MAC 주소 및 IP 주소와 같은 브리지 그룹 정보를 표시하려면 특권 EXEC 모드에서 **show bridge-group** 명령을 사용합니다.

show bridge-group *bridge-group-number*

구문 설명

bridge-group-number	브리지 그룹 번호를 1에서 100 사이의 정수로 지정합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

예

다음은 IPv4 주소를 사용한 **show bridge-group** 명령의 샘플 출력입니다.

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

다음은 IPv4 및 IPv6 주소를 사용한 **show bridge-group** 명령의 샘플 출력입니다.

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
    2000:101::1, subnet is 2000:101::/64
    2000:102::1, subnet is 2000:102::/64
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

관련 명령

명령	설명
bridge-group	투명 방화벽 인터페이스를 브리지 그룹으로 그룹화합니다.
clear configure interface bvi	브리지 그룹 인터페이스 컨피그레이션을 지웁니다.
interface	인터페이스를 구성합니다.
interface bvi	브리지 가상 인터페이스를 생성합니다.
ip address	브리지 그룹에 대한 관리 IP 주소를 설정합니다.
show running-config interface bvi	브리지 그룹 인터페이스 컨피그레이션을 표시합니다.

show call-home

구성된 Call Home 정보를 표시하려면 특권 EXEC 모드에서 **show call-home** 명령을 사용합니다.

[**cluster exec**] **show call-home** [**alert-group** | **detail** | **events** | **mail-server status** | **profile** {*profile _name* | **all**} | **statistics**]

구문 설명

alert-group	(선택 사항) 사용 가능한 알림 그룹을 표시합니다.
cluster exec	(선택 사항) 클러스터링 환경에서 하나의 디바이스에서 **show call-home** 명령을 실행하고 나머지 모든 디바이스에서 동시에 이 명령을 실행할 수 있도록 합니다.
detail	(선택 사항) Call Home 컨피그레이션을 자세히 표시합니다.
events	(선택 사항) 현재 감지된 이벤트를 표시합니다.
mail-server status	(선택 사항) Call Home 메일 서버 상태 정보를 표시합니다.
profile *profile _name* **all**	(선택 사항) 모든 기존 프로파일에 대한 컨피그레이션 정보를 표시합니다.
statistics	(선택 사항) Call Home 통계를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.2(2)	이 명령이 도입되었습니다.
9.1(3)	**show cluster history** 명령 및 **show cluster info** 명령의 출력을 포함하도록 새 유형의 Smart Call Home 메시지가 추가되었습니다.

예

다음은 구성된 Call Home 설정을 표시하는 **show call-home** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home
Current Smart Call-Home settings:
Smart Call-Home feature : enable
Smart Call-Home message's from address: from@example.com
Smart Call-Home message's reply-to address: reply-to@example.com
contact person's email address: example@example.com
contact person's phone: 111-222-3333
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: ExampleCorp
contract ID: X123456789
site ID: SantaClara
```

```
Mail-server[1]: Address: smtp.example.com Priority: 1
Mail-server[2]: Address: 192.168.0.1 Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword                  State
------------------------ -------
Syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile Name: prof1
Profile Name: prof2
```

다음은 자세한 Call Home 컨피그레이션 정보를 표시하는 **show call-home detail** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home detail
Description: Show smart call-home configuration in detail.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Current Smart Call-Home settings:
Smart Call-Home feature: enable
Smart Call-Home message's from address: from@example.example.com
Smart Call-Home message's reply-to address: reply-to@example.example.com
contact person's email address: abc@example.com
contact person's phone: 111-222-3333
street address: 1234 Any Street, Any city, Any state, 12345
customer ID: 111111
contract ID: 123123
site ID: SantaClara
Mail-server[1]: Address: example.example.com Priority: 1
Mail-server[2]: Address: example.example.com Priority: 10
Rate-limit: 60 message(s) per minute
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
Profiles:
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
```

```
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://kafan-lnx-01.cisco.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

다음은 사용 가능한 Call Home 이벤트를 표시하는 **show call-home events** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-------------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

다음은 사용 가능한 Call Home 메일 서버 상태를 표시하는 **show call-home mail-server status** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: example.example.com Priority: 1 [Available]
Mail-server[2]: Address: example.example.com Priority: 10 [Not Available]
```

다음은 사용 가능한 알림 그룹을 표시하는 **show call-home alert-group** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home alert-group
Description: Show smart call-home alert-group states.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Available alert groups:
Keyword State
------------------------ -------
syslog Enable
diagnostic Enable
environmental Enable
inventory Enable
configuration Enable
firewall Enable
troubleshooting Enable
report Enable
```

다음은 모든 사전 정의 프로파일 및 사용자 정의 프로파일을 표시하는 **show call-home profile profile-name | all** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home profile {profile-name | all}
Description: Show smart call-home profile configuration.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Profiles:
Profile Name: CiscoTAC-1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): anstage@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity
------------------------ ------------
inventory n/a
Profile Name: prof1
Profile status: ACTIVE Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
Profile Name: prof2
Profile status: ACTIVE Preferred Message Format: short-text
Message Size Limit: 1048576 Bytes
Email address(es): example@example.com
HTTP address(es): https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity
------------------------ ------------
configuration n/a
inventory n/a
```

다음은 Call Home 통계를 표시하는 **show call-home statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home statistics
Description: Show smart call-home statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Message Types Total Email HTTP
--------------------- ---------------- ---------------- ----------------
Total Success 0 0 0
Total In-Queue 0 0 0
Total Dropped 5 4 1
Tx Failed 5 4 1
inventory 3 2 1
configuration 2 2 0
Event Types Total
-------------------- ----------------
Total Detected 2
inventory 1
configuration 1
Total In-Queue 0
Total Dropped 0
Last call-home message sent time: 2009-06-17 14:22:09 GMT-07:00
```

다음은 Call Home 상태를 표시하는 **show call-home statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Mail-server[1]: Address: kafan-lnx-01.cisco.com Priority: 1 [Available]
Mail-server[2]: Address: kafan-lnx-02.cisco.com Priority: 10 [Not Available]

37. ciscoasa# show call-home events
Description: Show current detected events.
Supported Modes: single mode and system context in multi mode, routed/transparent.
Output:
Active event list:
Event client alert-group severity active (sec)
-----------------------------------------------------------------
Configuration Client configuration none 5
Inventory inventory none 15
```

다음은 클러스터에 대한 Call Home 통계를 표시하는 **cluster exec show call-home statistics** 명령의 샘플 출력입니다.

```
ciscoasa(config)# cluster exec show call-home statistics
A(LOCAL):**********************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                 3                3                0
                test                 3                3                0

 Total In-Delivering                 0                0                0

      Total In-Queue                 0                0                0

Total Dropped                       8                8                0
           Tx Failed                8                8                0
        configuration               2                2                0
                test                6                6                0


Event Types             Total
--------------------   ----------------
      Total Detected               10
       configuration                1
                test                9

 Total In-Processing                0

      Total In-Queue                0

Total Dropped                       0

Last call-home message sent time: 2013-04-15 05:37:16 GMT+00:00

B:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                 1                1                0
                test                 1                1                0

 Total In-Delivering                 0                0                0

      Total In-Queue                 0                0                0

Total Dropped                       2                2                0
```

```
           Tx Failed                  2                2                0
        configuration                 2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  2
       configuration                  1
                test                  1

 Total In-Processing                  0

      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: 2013-04-15 05:36:16 GMT+00:00

C:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  0                0                0

 Total In-Delivering                  0                0                0

      Total In-Queue                  0                0                0

Total Dropped                         2                2                0
           Tx Failed                  2                2                0
       configuration                  2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  1
       configuration                  1

 Total In-Processing                  0

      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: n/a

D:**********************************************************************
Message Types           Total            Email             HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  1                1                0
                test                  1                1                0

 Total In-Delivering                  0                0                0

      Total In-Queue                  0                0                0

Total Dropped                         2                2                0
           Tx Failed                  2                2                0
       configuration                  2                2                0

Event Types             Total
--------------------   ----------------
      Total Detected                  2
       configuration                  1
                test                  1

 Total In-Processing                  0
```

```
      Total In-Queue                  0

Total Dropped                         0

Last call-home message sent time: 2013-04-15 05:35:34 GMT+00:00

ciscoasa(config)#
```

관련 명령

명령	설명
call-home	Call Home 컨피그레이션 모드를 시작합니다.
call-home send alert-group	특정 알림 그룹 메시지를 보냅니다.
service call-home	Call Home을 활성화하거나 비활성화합니다.

show call-home registered-module status

등록된 모듈 상태를 표시하려면 특권 EXEC 모드에서 **show call-home registered-module status** 명령을 사용합니다.

show call-home registered-module status [**all**]

참고 [**all**] 옵션은 시스템 상황 모드에서만 유효합니다.

구문 설명

all	상황이 아니라 디바이스를 기반으로 모듈 상태를 표시합니다. 다중 상황 모드에서는 "**all**" 옵션이 포함된 경우 하나 이상의 상황에서 모듈이 활성화되면 해당 모듈이 활성화된 것으로 표시됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.2(2)	이 명령이 도입되었습니다.

예

다음 예에서는 **show call-home registered-module status all** 출력을 표시합니다.

```
Output:
Module Name Status
--------------------------------------- --------------------
Smart Call-Home enabled
Failover Standby/Active
```

관련 명령

명령	설명
call-home	Call Home 컨피그레이션 모드를 시작합니다.
call-home send alert-group	특정 알림 그룹 메시지를 보냅니다.
service call-home	Call Home을 활성화하거나 비활성화합니다.

show capture

옵션을 지정하지 않은 경우 캡처 컨피그레이션을 표시하려면 특권 EXEC 모드에서 **show capture** 명령을 사용합니다.

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

구문 설명

access-list *access_list_name*	(선택 사항) 특정 액세스 목록 식별을 위해 IP 또는 그 상위 필드를 기반으로 하는 패킷에 대한 정보를 표시합니다.
capture_name	(선택 사항) 패킷 캡처의 이름을 지정합니다.
cluster exec	(선택 사항) 클러스터링 환경에서 하나의 디바이스에서 **show capture** 명령을 실행하고 나머지 모든 디바이스에서 동시에 이 명령을 실행할 수 있도록 합니다.
count *number*	(선택 사항) 데이터가 지정된 패킷 수를 표시합니다.
decode	이 옵션은 캡처 유형 isakmp가 인터페이스에 적용된 경우에 유용합니다. 이 인터페이스를 통과하는 모든 ISAKMP 데이터는 암호 해독 후에 캡처되며 필드를 디코딩한 후 추가 정보와 함께 표시됩니다.
detail	(선택 사항) 각 패킷에 대한 추가 프로토콜 정보를 표시합니다.
dump	(선택 사항) 데이터 링크를 통해 전송되는 패킷의 16진수 덤프를 표시합니다.
packet-number *number*	지정된 패킷에서 표시를 시작합니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.4(2)	IDS에 대한 출력에 자세한 정보가 추가되었습니다.
9.0(1)	**cluster exec** 옵션이 추가되었습니다.
9.2(1)	**vpn-user** 도메인 이름이 출력에서 **filter-aaa**로 변경되었습니다.
9.3(1)	SGT와 이더넷 태그 지정에 대한 출력이 추가되었습니다.

사용 지침

*capture_name*을 지정한 경우 해당 캡처에 대한 캡처 버퍼 내용이 표시됩니다.

dump 키워드는 16진수 덤프에 MAC 정보를 표시하지 않습니다.

패킷의 디코딩된 출력은 패킷의 프로토콜에 따라 달라집니다. 표 4-29에서 대괄호 안의 출력은 **detail** 키워드를 지정한 경우에 표시됩니다.

표 4-29 패킷 캡처 출력 형식

패킷 유형	캡처 출력 형식
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/기타	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
기타	*HH:MM:SS.ms ether-hdr*: *hex-dump*

ASA에서 잘못된 형식의 TCP 헤더가 있는 패킷을 받고 ASP 삭제 사유 *invalid-tcp-hdr-length*로 인해 이를 삭제한 경우에는 해당 패킷을 받은 인터페이스에서의 **show capture** 명령 출력에 패킷이 표시되지 않습니다.

예

다음 예에서는 캡처 컨피그레이션을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

다음 예에서는 ARP 캡처에서 캡처한 패킷을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

다음 예에서는 클러스터링 환경의 단일 디바이스에서 캡처된 패킷을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

다음 예에서는 클러스터링 환경의 모든 디바이스에서 캡처된 패킷을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# cluster exec show capture
mycapture (LOCAL):--------------------------------------------------------

capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

```
yourcapture:-------------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

다음 예에서는 아래 명령을 입력한 후 클러스터링 환경의 클러스터 제어 링크에서 캡처된 패킷을 보여 줍니다.

```
ciscoasa (config)# capture a interface cluster
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet 0/0

ciscoasa(config)# show capture
capture a type raw-data interface cluster [Capturing - 970 bytes]
capture cp type raw-data interface cluster [Capturing - 26236 bytes]
  match udp any eq 49495 any
capture dp type raw-data access-list cc1 interface cluster [Capturing - 4545230 bytes]
capture lacp type lacp interface gigabitEthernet0/0 [Capturing - 140 bytes]
```

다음 예는 인터페이스에서 SGT와 이더넷 태그 지정이 활성화된 경우에 캡처된 패킷을 보여 줍니다.

```
ciscoasa(config)# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

SGT와 이더넷 태그 지정이 활성화된 경우에도 인터페이스에서 태그가 지정된 패킷 또는 태그가 지정되지 않은 패킷을 받을 수 있습니다. 표시된 예는 출력에 INLINE-TAG 36이 있는 태그가 지정된 패킷에 대한 예입니다. 동일한 인터페이스에서 태그가 지정되지 않은 패킷을 받은 경우에도 출력은 변경되지 않습니다(즉, 출력에 포함된 “INLINE-TAG 36” 항목이 없음).

관련 명령

명령	설명
capture	패킷 검사 및 네트워크 결함 분리를 위해 패킷 캡처 기능을 활성화합니다.
clear capture	캡처 버퍼를 지웁니다.
copy capture	캡처 파일을 서버에 복사합니다.

show chardrop

직렬 콘솔에서 삭제된 문자 수를 표시하려면 특권 EXEC 모드에서 **show chardrop** 명령을 사용합니다.

show chardrop

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음은 **show chardrop** 명령의 샘플 출력입니다.

```
ciscoasa# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

관련 명령

명령	설명
show running-config	현재 작동 중인 컨피그레이션을 표시합니다.

show checkheaps

checkheap 통계를 표시하려면 특권 EXEC 모드에서 **show checkheaps** 명령을 사용합니다. checkheap은 힙 메모리 버퍼의 온전성(동적 메모리는 시스템 힙 메모리 영역에서 할당됨) 및 코드 영역의 무결성을 확인하는 정기 프로세스입니다.

show checkheaps

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show checkheaps** 명령의 샘플 출력입니다.

```
ciscoasa# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

관련 명령

명령	설명
checkheaps	checkheap 확인 간격을 설정합니다.

show checksum

컨피그레이션 체크섬을 표시하려면 특권 EXEC 모드에서 **show checksum** 명령을 사용합니다.

show checksum

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

show checksum 명령을 사용하면 컨피그레이션 내용의 디지털 요약 역할을 하는 네 그룹의 16진수 숫자를 표시할 수 있습니다. 이 체크섬은 플래시 메모리에 컨피그레이션을 저장한 경우에만 계산됩니다.

show config 또는 **show checksum** 명령 출력에서 체크섬 앞에 점(“.”)이 표시된 경우 이 출력은 정상적인 컨피그레이션 로드 또는 쓰기 모드를 나타납니다(ASA 플래시 파티션에서 로드하거나 쓰는 경우). "."은 ASA가 작업으로 미리 점유되어 있지만 "중지"되지 않았음을 표시합니다. 이 메시지는 "시스템을 처리하는 중입니다. 기다려 주십시오."라는 메시지와 유사합니다.

예

다음 예에서는 컨피그레이션 또는 체크섬을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

청크 통계를 표시하려면 특권 EXEC 모드에서 **show chunkstat** 명령을 사용합니다.

show chunkstat

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 청크 통계를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

관련 명령

명령	설명
show counters	프로토콜 스택 카운터를 표시합니다.
show cpu	CPU 사용률 정보를 표시합니다.

show class

클래스에 할당된 상황을 표시하려면 특권 EXEC 모드에서 **show class** 명령을 사용합니다.

show class *name*

구문 설명

name	최대 20자의 문자열로 이름을 지정합니다. 기본 클래스를 표시하려면 이름에 대해 **default**를 입력합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음은 **show class default** 명령의 샘플 출력입니다.

```
ciscoasa# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

관련 명령

명령	설명
class	리소스 클래스를 구성합니다.
clear configure class	클래스 컨피그레이션을 지웁니다.
context	보안 상황을 구성합니다.
limit-resource	클래스에 대한 리소스 제한을 설정합니다.
member	리소스 클래스에 상황을 할당합니다.

show clock

ASA에서 시간을 보려면 사용자 EXEC 모드에서 **show clock** 명령을 사용합니다.

show clock [**detail**]

구문 설명

detail	(선택 사항) 시계 소스(NTP 또는 사용자 구성) 및 현재 일광 절약 시간 설정(있는 경우)을 나타냅니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show clock** 명령의 샘플 출력입니다.

```
ciscoasa# show clock
12:35:45.205 EDT Tue Jul 27 2004
```

다음은 **show clock detail** 명령의 샘플 출력입니다.

```
ciscoasa# show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

관련 명령

명령	설명
clock set	ASA에서 수동으로 시계를 설정합니다.
clock summer-time	일광 절약 시간을 표시하도록 날짜 범위를 설정합니다.
clock timezone	표준 시간대를 설정합니다.
ntp server	NTP 서버를 식별합니다.
show ntp status	NTP 연계 상태를 표시합니다.

show cluster

전체 클러스터에 대한 집계된 데이터 또는 다른 정보를 보려면 특권 EXEC 모드에서 **show cluster** 명령을 사용합니다.

show cluster {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **traffic** | **xlate count**}

구문 설명

access-list [*acl_name*]	액세스 정책에 대한 방문 횟수 카운터를 표시합니다. 특정 ACL에 대한 카운터를 보려면 *acl_name*을 입력합니다.
conn [**count**]	모든 디바이스에 대한 사용 중인 연결의 집계된 수를 표시합니다. **count** 키워드를 입력하면 연결 수만 표시됩니다.
cpu [**usage**]	CPU 사용 정보를 표시합니다.
history	클러스터 스위칭 기록을 표시합니다.
interface-mode	클러스터 인터페이스 모드(spanned 또는 individual)를 표시합니다.
memory	시스템 메모리 사용률 및 기타 정보를 표시합니다.
resource usage	시스템 리소스 및 사용 현황을 표시합니다.
traffic	트래픽 통계를 표시합니다.
xlate count	현재 변환 정보를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show cluster info 및 **show cluster user-identity** 명령도 참고하십시오.

예

다음은 **show cluster access-list** 명령의 샘플 출력입니다.

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0, 0,
0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

모든 디바이스에 대한 사용 중인 연결의 집계된 수를 표시하려면 다음을 입력합니다.

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*****************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):*************************************************************
  100 in use, 100 most used

  cl1:*************************************************************
  100 in use, 100 most used
```

관련 명령

명령	설명
show cluster info	클러스터 정보를 표시합니다.
show cluster user-identity	클러스터 사용자 ID 정보 및 통계를 표시합니다.

show cluster info

클러스터 정보를 보려면 특권 EXEC 모드에서 **show cluster info** 명령을 사용합니다.

show cluster info [**clients** | **conn-distribution** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport {asp** | **cp}**]

구문 설명

clients	(선택 사항) 레지스터 클라이언트의 버전을 표시합니다.
conn-distribution	(선택 사항) 클러스터의 연결 배포를 표시합니다.
goid [*options*]	(선택 사항) 전역 개체 ID 데이터베이스를 표시합니다. 옵션에는 다음이 포함됩니다. • **classmap** • **conn-set** • **hwidb** • **idfw-domain** • **idfw-group** • **interface** • **policymap** • **virtual-context**
health	(선택 사항) 상태 모니터링 정보를 표시합니다.
incompatible-config	(선택 사항) 현재 실행 중인 컨피그레이션에서 클러스터링과 호환되지 않는 명령을 표시합니다. 이 명령은 클러스터링을 활성화하기 전에 유용합니다.
loadbalance	(선택 사항) 부하 균형 정보를 표시합니다.
old-members	(선택 사항) 클러스터의 이전 멤버를 표시합니다.
packet-distribution	(선택 사항) 클러스터의 패킷 배포를 표시합니다.
trace [*options*]	(선택 사항) 클러스터링 제어 모듈 이벤트 추적을 표시합니다. 옵션에는 다음이 포함됩니다. • **latest** [*number*] - 마지막 *number* 이벤트를 표시합니다(여기서 number는 1~2147483647). 기본적으로 모두 표시합니다. • **level** *level* - 이벤트를 수준별로 필터링합니다(여기서 *level*은 **all**, **critical**, **debug**, **informational** 또는 **warning**). • **module** *module* - 이벤트를 모듈별로 필터링합니다(여기서 *module*은 **ccp**, **datapath**, **fsm**, **general**, **hc**, **license**, **rpc** 또는 **transport**). • **time** {[*month day*] [*hh*:*mm*:*ss*]} - 지정된 시간 또는 날짜 이전의 이벤트를 표시합니다.
transport {asp | **cp}**	(선택 사항) 다음에 대한 전송 관련 통계를 표시합니다. • **asp** - 데이터 평면 전송 통계 • **cp** - 제어 평면 전송 통계

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.
9.3(1)	**show cluster info health** 명령에 모듈에 대한 향상된 지원이 추가되었습니다.

사용 지침

아무 옵션도 지정하지 않은 경우 **show cluster info** 명령은 클러스터 이름 및 상태, 클러스터 멤버, 멤버 상태 등 일반적인 클러스터 정보를 표시합니다.

통계를 지우려면 **clear cluster info** 명령을 사용합니다.

show cluster 및 **show cluster user-identity** 명령도 참고하십시오.

예

다음은 **show cluster info** 명령의 샘플 출력입니다.

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Version   : 100.8(0.52)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Version   : 100.8(0.52)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Version   : 100.8(0.52)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
```

```
  Unit "B" in state SLAVE
      ID        : 3
      Version   : 100.8(0.52)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

다음은 **show cluster info incompatible-config** 명령의 샘플 출력입니다.

```
ciscoasa(cfg-cluster)# show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a user's
confirmation upon enabling clustering, can be removed automatically from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close

INFO: No manually-correctable incompatible configuration is found.
```

다음은 **show cluster info trace** 명령의 샘플 출력입니다.

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

다음은 ASA 5500-X에서 실행된 **show cluster info health** 명령의 샘플 출력입니다.

```
ciscoasa# show cluster info health
Member ID to name mapping:
  0 - A   1 - B(myself)

                          0        1
GigabitEthernet0/0        up       up
Management0/0             up       up

ips (policy off)          up       None
sfr (policy off)          None     up
Unit overall              healthy   healthy
Cluster overall           healthy
```

위 출력은 ASA IPS(ips) 및 ASA FirePOWER(sfr) 모듈을 모두 나열하며, 각 모듈에 대해 ASA는 “policy on” 또는 “policy off”를 표시하여 서비스 정책에서 모듈을 구성했는지 나타냅니다. 예를 들면 다음과 같습니다.

```
class-map sfr-class
    match sfr-traffic
policy-map sfr-policy
    class sfr-class
        sfr inline fail-close
service-policy sfr interface inside
```

위 컨피그레이션에서 ASA FirePOWER 모듈("sfr")은 "policy on"으로 표시됩니다. 하나의 클러스터 멤버에는 “up”인 모듈이 있고, 다른 멤버에는 “down” 또는 “None”인 모듈이 있는 경우 down 모듈이 있는 멤버는 클러스터에서 추방됩니다. 그러나 서비스 정책이 구성되지 않은 경우에는 클러스터 멤버가 클러스터에서 추방되지 않습니다. 모듈 상태는 모듈이 실행 중인 경우에만 관련이 있습니다.

다음은 ASA 5585-X에서 실행된 **show cluster info health** 명령의 샘플 출력입니다.

```
ciscoasa# show cluster info health
spyker-13# sh clu info heal
Member ID to name mapping:
  0 - A(myself) 1 - B

                       0 1
GigabitEthernet0/0       upup

SSM Card (policy off)    upup
Unit overall             healthyhealth
Cluster overall         healthyhealth
```

서비스 정책에서 모듈을 구성하면 출력에 “policy on”이 표시됩니다. 서비스 정책을 구성하지 않으면 섀시에 모듈이 있는 경우에도 출력에 “policy off”가 표시됩니다.

관련 명령

명령	설명
show cluster	전체 클러스터에 대한 집계된 데이터를 표시합니다.
show cluster user-identity	클러스터 사용자 ID 정보 및 통계를 표시합니다.

show cluster user-identity

전체 클러스터의 사용자 ID 정보 및 통계를 보려면 특권 EXEC 모드에서 **show cluster user-identity** 명령을 사용합니다.

show cluster user-identity {**statistics** [**user** *name* | **user-group** *group_name*] |
user [**active** [**domain** *name*] | **user** *name* | **user-group** *group_name*] [**list** [*detail*] | **all** [**list** [*detail*] | **inactive** {**domain** *name* | **user-group** *group_name*] [**list** [*detail*]]}

구문 설명

active	활성 IP-사용자 매핑이 있는 사용자를 표시합니다.
all	사용자 데이터베이스의 모든 사용자를 표시합니다.
domain *name*	도메인에 대한 사용자 정보를 표시합니다.
inactive	비활성 IP-사용자 매핑이 있는 사용자를 표시합니다.
list [*detail*]	사용자 목록을 표시합니다.
statistics	클러스터 사용자 ID 통계를 표시합니다.
user	사용자 데이터베이스 표시합니다.
user *name*	특정 사용자에 대한 정보를 표시합니다.
user-group *group_name*	특정 그룹의 각 사용자에 대한 정보를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show cluster info 및 **show cluster** 명령도 참고하십시오.

관련 명령

명령	설명
show cluster	전체 클러스터에 대한 집계된 데이터를 표시합니다.
show cluster info	클러스터 정보를 표시합니다.

show compression svc

ASA의 SVC 연결에 대한 압축 통계를 보려면 특권 EXEC 모드에서 **show compression svc** 명령을 사용합니다.

show compression svc

기본값

이 명령에 대한 기본 동작은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예		—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

예

다음 예에서는 **show compression svc** 명령의 출력을 보여 줍니다.

```
ciscoasa# show compression svc
Compression SVC Sessions                    1
Compressed Frames                      249756
Compressed Data In (bytes)            0048042
Compressed Data Out (bytes)           4859704
Expanded Frames                             1
Compression Errors                          0
Compression Resets                          0
Compression Output Buf Too Small            0
Compression Ratio                        2.06
Decompressed Frames                    876687
Decompressed Data In                279300233
```

관련 명령

명령	설명
compression	모든 SVC 및 WebVPN 연결을 대한 압축을 활성화합니다.
svc compression	특정 그룹 또는 사용자에 대해 SVC 연결을 통한 http 데이터의 압축을 활성화합니다.

show configuration

ASA의 플래시 메모리에 저장된 컨피그레이션을 표시하려면 특권 EXEC 모드에서 **show configuration** 명령을 사용합니다.

show configuration

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 수정되었습니다.

사용 지침

show configuration 명령은 ASA의 플래시 메모리에 저장된 컨피그레이션을 표시합니다. **show running-config** 명령과 달리 **show configuration** 명령은 실행하는 데 많은 CPU 리소스가 사용되지 않습니다.

ASA의 메모리에 저장된 활성 컨피그레이션(저장된 컨피그레이션 변경 포함)을 표시하려면 **show running-config** 명령을 사용합니다.

예

다음은 **show configuration** 명령의 샘플 출력입니다.

```
ciscoasa# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
```

```
 ip address 10.0.0.5 255.255.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 10.0.0.0 255.255.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
aaa authentication ssh console LOCAL
http server enable
```

```
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

관련 명령

명령	설명
configure	터미널에서 ASA를 구성합니다.

show configuration session

현재 컨피그레이션 세션 및 세션 내 변경 사항을 표시하려면 특권 EXEC 모드에서 **show configuration session** 명령을 사용합니다.

show configuration session [*session_name*]

구문 설명

session_name	기존 컨피그레이션 세션의 이름입니다. 이 파라미터를 생략하면 모든 기존 세션이 표시됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

이 명령을 **configure session** 명령과 함께 사용하면 ACL과 해당 개체를 편집할 수 있는 분리된 세션이 생성됩니다. 이 명령은 세션의 이름과 세션에서 적용된 모든 컨피그레이션 변경 사항을 표시합니다.

세션이 커밋된 것으로 표시된 경우 세션을 열고 변경 사항을 되돌릴 수 있습니다(세션이 예상대로 작동하지 않은 경우).

예

다음 예에서는 사용 가능한 모든 세션을 보여 줍니다.

```
ciscoasa# show configuration session
config-session abc (un-committed)
 access-list abc permit ip any any
 access-list abc permit tcp any any

config-session abc2 (un-committed)
 object network test
 host 1.1.1.1
 object network test2
 host 2.2.2.2

ciscoasa#
```

관련 명령

명령	설명
clear configuration session	컨피그레이션 세션과 해당 내용을 삭제합니다.
clear session	컨피그레이션 세션의 내용을 지우고 해당 액세스 플래그를 재설정합니다.
configure session	세션을 만들거나 엽니다.

show conn

지정한 연결 유형에 대한 연결 상태를 표시하려면 특권 EXEC 모드에서 **show conn** 명령을 사용합니다. 이 명령은 IPv4 및 IPv6 주소를 지원합니다.

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}] [**scansafe**] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]] [**user-identity** | **user** [*domain_nickname*\]*user_name* | **user-group** [*domain_nickname*\\]*user_group_name*] | **security-group**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

구문 설명

address	(선택 사항) 지정된 소스 또는 대상 IP 주소와의 연결을 표시합니다.
all	(선택 사항) 통과 트래픽 연결 외에 디바이스로의 연결 또는 디바이스에서의 연결을 표시합니다.
count	(선택 사항) 활성 연결 수를 표시합니다.
dest_ip	(선택 사항) 대상 IP 주소(IPv4 또는 IPv6)를 지정합니다. 범위를 지정하려면 대시(-)를 사용하여 IP 주소를 구분합니다. 예를 들면 다음과 같습니다. `10.1.1.1-10.1.1.5`
dest_port	(선택 사항) 대상 포트 번호를 지정합니다. 범위를 지정하려면 대시(-)를 사용하여 포트 번호를 구분합니다. 예를 들면 다음과 같습니다. `1000-2000`
detail	(선택 사항) 변환 유형 및 인터페이스 정보를 포함하여 연결을 자세히 표시합니다.
long	(선택 사항) 긴 형식의 연결을 표시합니다.
netmask *mask*	(선택 사항) 지정된 IP 주소에서 사용할 서브넷 마스크를 지정합니다.
port	(선택 사항) 지정된 소스 또는 대상 포트와의 연결을 표시합니다.
protocol {**tcp** | **udp**}	(선택 사항) 연결 프로토콜(**tcp** 또는 **udp**일 수 있음)을 지정합니다.
scansafe	(선택 사항) Cloud Web Security 서버로 전달되는 연결을 표시합니다.
security-group	(선택 사항) 표시된 모든 연결이 지정된 보안 그룹에 속하도록 지정합니다.
src_ip	(선택 사항) 소스 IP 주소(IPv4 또는 IPv6)를 지정합니다. 범위를 지정하려면 대시(-)를 사용하여 IP 주소를 구분합니다. 예를 들면 다음과 같습니다. `10.1.1.1-10.1.1.5`
src_port	(선택 사항) 소스 포트 번호를 지정합니다. 범위를 지정하려면 대시(-)를 사용하여 포트 번호를 구분합니다. 예를 들면 다음과 같습니다. `1000-2000`
state *state_type*	(선택 사항) 연결 상태 유형을 지정합니다. 연결 상태 유형에 사용할 수 있는 키워드 목록은 표 4-30을 참고하십시오.
user [*domain_nickname*\] *user_name*	(선택 사항) 표시된 모든 연결이 지정된 사용자에게 속하도록 지정합니다. *domain_nickname* 인수를 포함하지 않은 경우 ASA는 기본 도메인의 사용자에 대한 정보를 표시합니다.

user-group [*domain_nickname*\\] *user_group_name*	(선택 사항) 표시된 모든 연결이 지정된 사용자 그룹에 속하도록 지정합니다. *domain_nickname* 인수를 포함하지 않은 경우 ASA는 기본 도메인의 사용자 그룹에 대한 정보를 표시합니다.
user-identity	(선택 사항) ASA에서 ID 방화벽 기능에 대한 모든 연결을 표시하도록 지정합니다. 연결을 표시할 때 ASA는 일치하는 사용자를 식별한 경우 사용자 이름 및 IP 주소를 표시합니다. 마찬가지로 ASA는 일치하는 호스트를 식별한 경우 호스트 이름 및 IP 주소를 표시합니다.
zone [*zone_name*]	(선택 사항) 영역에 대한 연결을 표시합니다. **long** 및 **detail** 키워드는 연결이 설정된 기본 인터페이스와 트래픽을 전달하는 데 사용되는 현재 인터페이스를 보여 줍니다.

기본값

모든 통과 연결은 기본적으로 표시됩니다. 디바이스에 대한 관리 연결도 표시하려면 **all** 키워드를 사용해야 합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(8)/7.2(4)/8.0(4)	"로컬" 및 "외부" 대신 소스 및 대상 개념을 사용하도록 구문이 간소화되었습니다. 새 구문에서 소스 주소는 입력된 첫 번째 주소이고, 대상은 두 번째 주소입니다. 이전 구문에서는 **foreign** 및 **fport**와 같은 키워드를 사용하여 목적지 주소 및 포트를 확인했습니다.
7.2(5)/8.0(5)/8.1(2)/8.2(4)/8.3(2)	**tcp_embryonic** 상태 유형이 추가되었습니다. 이 유형은 i 플래그(불완전한 연결)와 함께 모든 TCP 연결을 표시합니다. UDP 연결에는 i 플래그가 표시되지 않습니다.
8.2(1)	TCP 상태 우회에 대해 b 플래그가 추가되었습니다.
8.4(2)	ID 방화벽을 지원하기 위해 **user-identity**, **user** 및 **user-group** 키워드가 추가되었습니다.
9.0(1)	클러스터링에 대한 지원이 추가되었습니다. **scansafe** 및 **security-group** 키워드가 추가되었습니다.
9.3(2)	**zone** 키워드가 추가되었습니다.

사용 지침

show conn 명령은 활성 TCP 및 UDP 연결 수를 표시하고, 여러 유형의 연결에 대한 정보를 제공합니다. **show conn all** 명령을 사용하여 전체 연결 테이블을 볼 수 있습니다.

참고 ASA에서 보조 연결을 허용하기 위해 핀홀을 만든 경우 이는 **show conn** 명령을 통해 불완전한 연결로 표시됩니다. 이 불완전한 연결을 지우려면 **clear conn** 명령을 사용합니다.

show conn state 명령을 사용하여 지정할 수 있는 연결 유형이 표 4-30에 정의되어 있습니다. 여러 연결 유형을 지정할 때는 공백 없이 쉼표를 사용하여 키워드를 구분합니다.

표 4-30 연결 상태 유형

키워드	표시되는 연결 유형
up	작동 중인 상태의 연결
conn_inbound	인바운드 연결
ctiqbe	CTIQBE 연결
data_in	인바운드 데이터 연결
data_out	아웃바운드 데이터 연결
finin	FIN 인바운드 연결
finout	FIN 아웃바운드 연결
h225	H.225 연결
h323	H.323 연결
http_get	HTTP 가져오기 연결
mgcp	MGCP 연결
nojava	Java 애플릿에 대한 액세스를 거부하는 연결
rpc	RPC 연결
service_module	SSM에서 스캔 중인 연결
sip	SIP 연결
skinny	SCCP 연결
smtp_data	SMTP 메일 데이터 연결
sqlnet_fixup_data	SQL*Net 데이터 검사 엔진 연결
tcp_embryonic	TCP 원시 연결
vpn_orphan	분리된 VPN 터널링 흐름

detail 옵션을 사용하면 표 4-31에 정의된 연결 플래그를 사용하여 변환 유형 및 인터페이스 정보가 표시됩니다.

표 4-31 연결 플래그

플래그	설명
a	SYN에 대한 외부 ACK 대기 중
A	SYN에 대한 내부 ACK 대기 중
b	TCP 상태 우회
B	외부의 초기 SYN
C	CTIQBE(Computer Telephony Interface Quick Buffer Encoding) 미디어 연결
d	덤프
D	DNS

표 4-31 연결 플래그(계속)

플래그	설명
E	외부 다시 연결. 이는 내부 호스트에서 시작해야 하는 보조 데이터 연결입니다. 예를 들어 FTP를 사용하는 경우 내부 클라이언트가 PASV 명령을 실행하고 외부 서버가 수락하면 ASA에서 이 플래그가 설정된 외부 다시 연결을 미리 할당합니다. 내부 클라이언트가 서버에 다시 연결하려고 하면 ASA에서 이 연결 시도를 거부합니다. 외부 서버만 미리 할당된 보조 연결을 사용할 수 있습니다.
f	내부 FIN
F	외부 FIN
g	MGCP(Media Gateway Control Protocol) 연결
G	연결이 그룹의 일부[1]
h	H.225
H	H.323
i	불완전한 TCP 또는 UDP 연결
I	인바운드 데이터
k	SCCP(Skinny Client Control Protocol) 미디어 연결
K	GTP t3-response
m	SIP 미디어 연결
M	SMTP 데이터
O	아웃바운드 데이터
p	복제됨(사용되지 않음)
P	내부 뒤로 연결. 이는 내부 호스트에서 시작해야 하는 보조 데이터 연결입니다. 예를 들어 FTP를 사용하는 경우 내부 클라이언트가 PORT 명령을 실행하고 외부 서버가 수락하면 ASA에서 이 플래그가 설정된 내부 다시 연결을 미리 할당합니다. 외부 서버가 클라이언트에 다시 연결하려고 하면 ASA에서 이 연결 시도를 거부합니다. 내부 클라이언트만 미리 할당된 보조 연결만 사용할 수 있습니다.
q	SQL*Net 데이터
r	내부 확인 응답된 FIN
R	TCP 연결에 대해 외부 확인 응답된 FIN
R	UDP RPC[2]
s	외부 SYN 대기 중
S	내부 SYN 대기 중
t	SIP 임시 연결[3]
T	SIP 연결[4]
U	up
V	VPN 분리
W	WAAS
X	서비스 모듈(예: CSC SSM)에 의해 검사됨
y	클러스터링의 경우 백업 소유자 흐름 식별
Y	클러스터링의 경우 디렉터 흐름 식별

표 4-31 연결 플래그(계속)

플래그	설명
z	클러스터링의 경우 전달자 흐름 식별
Z	Cloud Web Security

1. G 플래그는 연결이 그룹의 일부임을 나타냅니다. 이는 제어 연결 및 연계된 모든 보조 연결을 지정하는 GRE 및 FTP Strict 픽스업으로 설정됩니다. 제어 연결이 종료되면 연계된 모든 보조 연결도 종료됩니다.
2. **show conn** 명령 출력의 각 행은 하나의 연결(TCP 또는 UDP)을 나타내기 때문에 R 플래그는 행당 하나만 있습니다.
3. UDP 연결의 경우 값 t는 1분 후 시간 초과됨을 나타냅니다.
4. UDP 연결의 경우 값 T는 **timeout sip** 명령을 사용하여 지정된 값에 따라 연결이 시간 초과됨을 나타냅니다.

참고 DNS 서버를 사용하는 연결의 경우 연결의 소스 포트는 **show conn** 명령 출력에 있는 *DNS 서버의 IP 주소*로 대체될 수 있습니다.

여러 DNS 세션이 동일한 두 호스트 간에 존재하고 세션의 5개 튜플(소스/대상 IP 주소, 소스/대상 포트 및 프로토콜)이 동일한 경우 여러 DNS 세션에 대해 단일 연결이 생성됩니다. DNS 식별은 *app_id*로 추적되며, 각 app_id에 대한 유휴 타이머는 독립적으로 실행됩니다.

app_id는 독립적으로 만료되므로 올바른 DNS 응답은 제한 기간 내에만 ASA를 통과할 수 있으며 리소스 빌드업이 없습니다. 그러나 **show conn** 명령을 입력하면 새 DNS 세션에 의해 DNS 연결의 유휴 타이머가 재설정됩니다. 이는 공유 DNS 연결의 속성 때문이며 설계에 따른 것입니다.

참고 **timeout conn** 명령에 정의된 비활성 기간(기본적으로 1시간) 동안 TCP 트래픽이 없으면 연결이 닫히고 해당 연결 플래그 항목이 더 이상 표시되지 않습니다.

LAN-to-LAN/네트워크-확장 모드 터널이 삭제되고 다시 생성되지 않은 경우 여러 개의 분리된 터널 흐름이 있을 수 있습니다. 이러한 흐름은 터널 중단으로 인해 끊어지지만 이러한 통과하려고 시도하는 모든 데이터는 삭제됩니다. **show conn** 명령 출력에서는 이러한 분리된 흐름을 **V** 플래그로 표시합니다.

다음 TCP 연결 방향 플래그가 동일한 보안 인터페이스(**same-security permit** 명령 참고) 간의 연결에 적용된 경우 플래그의 방향은 동일한 보안 인터페이스로 인해 관련이 없으며, "내부" 또는 "외부"가 없습니다. ASA는 동일한 보안 연결에 이러한 플래그를 사용해야 하므로 ASA는 다른 연결 특성에 따라 둘 중 하나의 플래그(예: f 또는 F)를 선택할 수 있지만 이와 같이 선택된 방향은 무시해야 합니다.

- B - 외부에서 시작된 초기 SYN
- a - SYN에 대한 외부 ACK 대기 중
- A - SYN에 대한 내부 ACK 대기 중
- f - 내부 FIN
- F - 외부 F
- s - 외부 SYN 대기 중
- S - 내부 SYN 대기 중

특정 연결에 대한 정보를 표시하려면 **security-group** 키워드를 포함하고 연결의 소스와 대상 둘 다에 대해 보안 그룹 테이블 값 또는 보안 그룹 이름을 지정해야 합니다. ASA는 특정 보안 그룹 테이블 값 또는 보안 그룹 이름과 일치하는 연결을 표시합니다.

소스 및 대상 보안 그룹 테이블 값 또는 보안 그룹 이름을 지정하지 않고 **security-group** 키워드를 지정한 경우에는 ASA에서 모든 SXP 연결에 대한 데이터를 표시합니다.

ASA는 *security_group_name*(*SGT_value*) 형식 또는 *SGT_value*(보안 그룹 이름을 알 수 없는 경우)로 연결 데이터를 표시합니다.

참고 스텁 연결에는 보안 그룹 데이터를 사용할 수 없습니다. 스텁 연결은 느린 경로를 통해 이동하지 않기 때문입니다. 스텁 연결은 연결 소유자에게 패킷을 전달하는 데 필요한 정보만 유지합니다.

단일 보안 그룹 이름을 지정하여 클러스터의 모든 연결을 표시할 수 있습니다. 예를 들어 다음 예에서는 클러스터의 모든 디바이스에서 security-group mktg와 일치하는 연결을 표시합니다.

```
ciscoasa# show cluster conn security-group name mktg
```

예 여러 연결 유형을 지정할 때는 공백 없이 쉼표를 사용하여 키워드를 구분합니다. 다음 예에서는 Up 상태의 RPC, H.323 및 SIP 연결에 대한 정보를 표시합니다.

```
ciscoasa# show conn state up,rpc,h323,sip
```

다음은 **show conn count** 명령의 샘플 출력입니다.

```
ciscoasa# show conn count
54 in use, 123 most used
```

다음은 **show conn** 명령의 샘플 출력입니다. 이 예에서는 내부 호스트 10.1.1.15와 10.10.49.10에 있는 외부 텔넷 서버 간의 TCP 세션 연결을 표시합니다. B 플래그가 없으므로 이 연결은 내부에서 시작됩니다. “U”, “I” 및 “O” 플래그는 연결이 활성 상태이고 인바운드 및 아웃바운드 데이터를 수신했음을 나타냅니다.

```
ciscoasa# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

다음은 SSM에서 연결을 스캔하는 중임을 나타내는 “X” 플래그가 포함된 **show conn** 명령의 샘플 출력입니다.

```
ciscoasa# show conn address 10.0.0.122 state service_module
```

```
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

다음은 **show conn detail** 명령의 샘플 출력입니다. 이 예에서는 외부 호스트 10.10.49.10과 내부 호스트 10.1.1.15 간의 UDP 연결을 보여 줍니다. D 플래그는 이 연결이 DNS 연결임을 나타냅니다. 번호 1028은 DNS ID입니다.

```
ciscoasa# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

다음은 분리 흐름이 존재하는 경우(**V** 플래그로 표시) **show conn** 명령의 샘플 출력입니다.

```
ciscoasa# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

보고서를 분리 흐름이 있는 연결로 제한하려면 다음 예와 같이 **vpn_orphan** 옵션을 **show conn state** 명령에 추가합니다.

```
ciscoasa# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

클러스터링의 경우 연결 흐름 문제를 해결하려면 먼저 마스터 디바이스에서 **cluster exec show conn** 명령을 입력하여 모든 디바이스의 연결을 확인합니다. 디렉터(Y), 백업(y) 및 전달자(z) 플래그가 있는 흐름을 확인합니다. 다음 예에서는 세 ASA 모두에 대한 172.18.124.187:22와 192.168.103.131:44727 간의 SSH 연결을 보여 줍니다. ASA 1에는 연결의 전달자임을 나타내는 z 플래그가 있고, ASA3에는 연결의 디렉터임을 나타내는 Y 플래그가 있으며, ASA2에는 특별한 플래그가 없어 소유자임을 나타냅니다. 아웃바운드 방향에서 이 연결의 패킷은 ASA2의 내부 인터페이스로 들어가 외부 인터페이스를 나갑니다. 인바운드 방향에서 이 연결의 패킷은 ASA1 및 ASA3의 외부 인터페이스로 들어가 클러스터 제어 링크를 통해 ASA2로 전달된 다음 ASA2의 내부 인터페이스를 나갑니다.

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**********************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0, flags
Y
```

ASA2에 대한 **show conn detail**의 출력에서는 가장 최근 전달자가 ASA1이었음을 보여 줍니다.

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
       D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS, Z - Scansafe redirection,
       X - inspected by service module
       Y - director stub flow
       y - backup stub flow
       z - forwarder stub flow
TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044, cluster sent/rcvd bytes
0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder ASA1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

다음 예에서는 ID 방화벽 기능을 위한 연결을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show conn user-identity ?
exec mode commands/options:
  all       Enter this keyword to show conns including to-the-box and from-the-box
  detail    Enter this keyword to show conn in detail
  long      Enter this keyword to show conn in long format
  port      Enter this keyword to specify port
  protocol  Enter this keyword to specify conn protocol
  state     Enter this keyword to specify conn state
  |         Output modifiers

ciscoasa# show conn user-identity
1219 in use, 1904 most used
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags -
UDP inside (www.yahoo.com)10.0.0.2:1586 outside (user2)192.0.0.1:30000, idle 0:00:00,
bytes 10, flags –
UDP inside 10.0.0.34:1586 outside 192.0.0.25:30000, idle 0:00:00, bytes 10, flags –
…
ciscoasa# show conn user user1
2 in use
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00,
bytes 10, flags –
```

show conn long zone 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2):
10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

관련 명령

명령	설명
clear conn	연결을 지웁니다.
inspect ctiqbe	CTIQBE 애플리케이션 검사를 활성화합니다.
inspect h323	H.323 애플리케이션 검사를 활성화합니다.
inspect mgcp	MGCP 애플리케이션 검사를 활성화합니다.
inspect sip	HTTP 트래픽에서 Java 애플릿을 제거합니다.
inspect skinny	SCCP 애플리케이션 검사를 활성화합니다.

show console-output

현재 캡처된 콘솔 출력을 표시하려면 특권 EXEC 모드에서 **show console-output** 명령을 사용합니다.

show console-output

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 콘솔 출력이 없는 경우 다음 메시지를 표시하는 **show console-output** 명령의 샘플 출력입니다.

```
ciscoasa# show console-output
Sorry, there are no messages to display
```

관련 명령

명령	설명
clear configure console	기본 콘솔 연결 설정을 복원합니다.
clear configure timeout	컨피그레이션에서 기본 유휴 시간을 복원합니다.
console timeout	ASA에 대한 콘솔 연결의 유휴 시간 제한을 설정합니다.
show running-config console timeout	ASA에 대한 콘솔 연결의 유휴 시간 제한을 표시합니다.

show context

할당된 인터페이스 및 컨피그레이션 파일 URL, 구성된 상황 수 또는 시스템 실행 공간의 모든 상황 목록이 포함된 상황 정보를 표시하려면 특권 EXEC 모드에서 **show context** 명령을 사용합니다.

show context [*name* | **detail** | **count**]

구문 설명

count	(선택 사항) 구성된 상황 수를 표시합니다.
detail	(선택 사항) 실행 상태 및 내부용 정보 등 상황에 대한 추가 세부사항을 표시합니다.
name	(선택 사항) 상황 이름을 설정합니다. 이름을 지정하지 않으면 ASA에서 모든 상황을 표시합니다. 상황 내에서는 현재 상황 이름만 입력할 수 있습니다.

기본값

시스템 실행 공간에서는 이름을 지정하지 않은 경우 ASA에서 모든 상황을 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.0(2)	할당된 IPS 가상 세션에 대한 정보가 추가되었습니다.

사용 지침

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 **show context** 명령의 샘플 출력입니다. 다음 샘플 표시에서는 3개의 상황을 보여 줍니다.

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

표 4-32에는 각 필드에 대한 설명이 나와 있습니다.

표 4-32 show context 필드

필드	설명
Context Name	모든 상황 이름을 나열합니다. 별표(*)가 있는 상황 이름은 관리 상황입니다.
Interfaces	상황에 할당된 인터페이스입니다.
URL	ASA가 상황 컨피그레이션을 로드하는 URL입니다.

다음은 시스템 실행 공간에서 실행된 **show context detail** 명령의 샘플 출력입니다.

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

표 4-33에는 각 필드에 대한 설명이 나와 있습니다.

표 4-33 상황 상태

필드	설명
Context	상황 이름입니다. Null 상황 정보는 내부 전용입니다. 시스템 상황은 시스템 실행 공간을 나타냅니다.
State Message:	상황 상태입니다. 가능한 메시지는 다음과 같습니다.
Has been created, but initial ACL rules not complete	ASA가 컨피그레이션을 구문 분석했지만 기본 보안 정책을 설정하는 데 필요한 기본 ACL을 아직 다운로드하지 않았습니다. 기본 보안 정책은 초기에 모든 상황에 적용되며, 하위 보안 수준에서 상위 보안 수준으로의 트래픽을 허용 안 함, 애플리케이션 검사 활성화 및 기타 파라미터를 포함합니다. 이 보안 정책은 컨피그레이션이 구문 분석되었지만 컨피그레이션 ACL이 컴파일되지 않은 경우 트래픽이 ASA를 통과하지 못하도록 합니다. 컨피그레이션 ACL이 매우 빠르게 컴파일된 경우에는 이 상태가 나타나지 않습니다.
Has been created, but not initialized	**context** *name* 명령을 입력했지만 아직 **config-url** 명령을 입력하지 않았습니다.
Has been created, but the config hasn't been parsed	기본 ACL을 다운로드했지만 ASA가 아직 컨피그레이션을 구문 분석하지 않았습니다. 이 상태는 네트워크 연결 문제로 인해 컨피그레이션 다운로드에 실패했거나 **config-url** 명령을 아직 입력하지 않은 경우에 발생할 수 있습니다. 컨피그레이션을 다시 로드하려면 상황 내에서 **copy startup-config running-config**를 입력합니다. 시스템에서 **config-url** 명령을 다시 입력합니다. 또는 빈 실행 중인 컨피그레이션을 구성하기 시작할 수 있습니다.
Is a system resource	이 상태는 시스템 실행 공간 및 null 상황에만 적용됩니다. null 상황은 시스템에서 사용되며 정보는 내부 전용입니다.
Is a zombie	**no context** 또는 **clear context** 명령을 사용하여 상황을 삭제했지만 ASA에서 새 상황에 상황 ID를 다시 사용하거나 재시작할 때까지 상황 정보가 메모리에서 유지됩니다.
Is active	이 상황은 현재 실행 중이며 상황 컨피그레이션 보안 정책에 따라 트래픽을 전달할 수 있습니다.
Is ADMIN and active	이 상황은 관리 상황이며 현재 실행되고 있습니다.
Was a former ADMIN, but is now a zombie	**clear configure context** 명령을 사용하여 상황을 삭제했지만 ASA에서 새 상황에 상황 ID를 다시 사용하거나 재시작할 때까지 상황 정보가 메모리에서 유지됩니다.
Real Interfaces	상황에 할당된 인터페이스입니다. **allocate-interface** 명령에서 인터페이스 ID를 매핑한 경우 인터페이스의 실제 이름이 여기에 표시됩니다.
Mapped Interfaces	**allocate-interface** 명령에서 인터페이스 ID를 매핑한 경우 매핑된 이름이 여기에 표시됩니다. 인터페이스를 매핑하지 않은 경우 실제 이름이 다시 나열됩니다.
Real IPS Sensors	AIP SSM를 설치한 경우 상황에 할당된 IPS 가상 센서입니다. **allocate-ips** 명령에서 센서 이름을 매핑한 경우 센서의 실제 이름이 여기에 표시됩니다.
Mapped IPS Sensors	**allocate-ips** 명령에서 센서 이름을 매핑한 경우 매핑된 이름이 여기에 표시됩니다. 센서 이름을 매핑하지 않은 경우 실제 이름이 다시 나열됩니다.

표 4-33 상황 상태(계속)

필드	설명
Flag	내부 전용입니다.
ID	이 상황에 대한 내부 ID입니다.

다음은 **show context count** 명령의 샘플 출력입니다.

```
ciscoasa# show context count
Total active contexts: 2
```

관련 명령

명령	설명
admin-context	관리 상황을 설정합니다.
allocate-interface	상황에 인터페이스를 할당합니다.
changeto	상황 또는 시스템 실행 공간 간의 변경 사항입니다.
config-url	상황 컨피그레이션의 위치를 지정합니다.
context	시스템 컨피그레이션에서 보안 상황을 만들고 상황 컨피그레이션 모드를 시작합니다.

show controller

모든 인터페이스의 컨트롤러 관련 정보를 보려면 특권 EXEC 모드에서 **show controller** 명령을 사용합니다.

show controller [**slot**] [*physical_interface*] [**pci** [**bridge** [*bridge-id* [*port-num*]]]] [**detail**]

구문 설명

bridge	(선택 사항) ASA 5585-X에 대한 PCI 브리지 관련 정보를 표시합니다.
bridge-id	(선택 사항) ASA 5585-X에 대한 고유한 각 PCI 브리지 식별자를 표시합니다.
detail	(선택 사항) 컨트롤러에 대한 추가 세부사항을 표시합니다.
pci	(선택 사항) ASA 5585-X에 대한 PCI 컨피그레이션 공간의 처음 256바이트와 함께 PCI 디바이스의 요약을 표시합니다.
physical_interface	(선택 사항) 인터페이스 ID를 식별합니다.
port-num	(선택 사항) ASA 5585-X 적응형 ASA에 대한 각 PCI 브리지 내의 고유한 포트 번호를 표시합니다.
slot	(선택 사항) ASA 5580에 대한 PCI-e 버스 및 슬롯 정보만 표시합니다.

기본값

인터페이스를 식별하지 않은 경우 이 명령은 모든 인터페이스에 대한 정보를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.
8.0(2)	이제 이 명령이 ASA 5505뿐만 아니라 모든 플랫폼에 적용됩니다. **detail** 키워드가 추가되었습니다.
8.1(1)	**slot** 키워드가 ASA 5580에 대해 추가되었습니다.
8.2(5)	IPS SSP가 설치된 ASA 5585-X에 대해 **pci**, **bridge**, *bridge-id* 및 *port-num* 옵션이 추가되었습니다. 또한 일시 중지 프레임을 보내 1기가비트 이더넷 인터페이스의 흐름 제어를 활성화하는 기능에 대한 지원이 모든 ASA 모델에 대해 추가되었습니다.
8.6(1)	ASA 5512-X~ASA 5555-X Internal-Control0/0 인터페이스에서 ASA와 소프트웨어 모듈 간의 제어 트래픽에 사용되고 Internal-Data0/1 인터페이스에서 ASA 및 소프트웨어 모듈에 대한 데이터 트래픽에 사용되는 **detail** 키워드에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 Cisco TAC에서 내부 및 고객이 발견한 결함을 조사할 때 컨트롤러에 대한 유용한 디버그 정보를 수집하는 데 도움이 됩니다. 실제 출력은 모델 및 이더넷 컨트롤러에 따라 다릅니다. 또한 이 명령은 IPS SSP가 설치된 ASA 5585-X에서 관련된 모든 PCI 브리지에 대한 정보를 표시합니다. ASA 서비스 모듈의 경우 **show controller** 명령 출력은 PCIe 슬롯 정보를 표시하지 않습니다.

예

다음은 **show controller** 명령의 샘플 출력입니다.

```
ciscoasa# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

     Global Registers:
         Control:       0x0482

--------------------------------------------------------------------------
Number of VLANs: 1
--------------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
--------------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
--------------------------------------------------------------------------

....

Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0002
```

```
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

...

Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                           0xe0004000 = 0x00000000
    ctrl_status                   0xe0004004 = 0x5501064a
    irq_src                       0xe0004008 = 0x00000000
    irq_msk                       0xe000400c = 0x00000000
    irq_hw_err_src                0xe0004010 = 0x00000000
    irq_hw_err_msk                0xe0004014 = 0x00001000
    bmu_cs_rxq                    0xe0004060 = 0x002aaa80
    bmu_cs_stxq                   0xe0004068 = 0x01155540
    bmu_cs_atxq                   0xe000406c = 0x012aaa80

   Bank 2: MAC address registers:

....
```

다음은 **show controller detail** 명령의 샘플 출력입니다.

```
ciscoasa# show controller gigabitethernet0/0 detail

GigabitEthernet0/0:
   Intel i82546GB revision 03

     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
         Extended Control:           0xf8260018 = 0x000000c0
         RX Config:                  0xf8260180 = 0x0c000000
         TX Config:                  0xf8260178 = 0x000001a0
         RX Control:                 0xf8260100 = 0x04408002
         TX Control:                 0xf8260400 = 0x000400fa
         TX Inter Packet Gap:        0xf8260410 = 0x00602008
         RX Filter Cntlr:            0xf8260150 = 0x00000000
         RX Chksum:                  0xf8265000 = 0x00000300

     RX Descriptor Registers:
         RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
         RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
         RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
         RX Descriptor 0 Length:     0xf8262808 = 0x00001000
         RX Descriptor 0 Head:       0xf8262810 = 0x00000000
         RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
         RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
         RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
```

```
        RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
        RX Descriptor 1 Length:     0xf8260140 = 0x00000000
        RX Descriptor 1 Head:       0xf8260148 = 0x00000000
        RX Descriptor 1 Tail:       0xf8260150 = 0x00000000

    TX Descriptor Registers:
        TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
        TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
        TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
        TX Descriptor 0 Length:     0xf8263808 = 0x00001000
        TX Descriptor 0 Head:       0xf8263810 = 0x00000000
        TX Descriptor 0 Tail:       0xf8263818 = 0x00000000

    RX Address Array:
        Ethernet Address 0:         0012.d948.ef58
        Ethernet Address 1:         Not Valid!
        Ethernet Address 2:         Not Valid!
        Ethernet Address 3:         Not Valid!
        Ethernet Address 4:         Not Valid!
        Ethernet Address 5:         Not Valid!
        Ethernet Address 6:         Not Valid!
        Ethernet Address 7:         Not Valid!
        Ethernet Address 8:         Not Valid!
        Ethernet Address 9:         Not Valid!
        Ethernet Address a:         Not Valid!
        Ethernet Address b:         Not Valid!
        Ethernet Address c:         Not Valid!
        Ethernet Address d:         Not Valid!
        Ethernet Address e:         Not Valid!
        Ethernet Address f:         Not Valid!

    PHY Registers:
        Phy Control:                0x1140
        Phy Status:                 0x7969
        Phy ID 1:                   0x0141
        Phy ID 2:                   0x0c25
        Phy Autoneg Advertise:      0x01e1
        Phy Link Partner Ability:   0x41e1
        Phy Autoneg Expansion:      0x0007
        Phy Next Page TX:           0x2801
        Phy Link Partnr Next Page:  0x0000
        Phy 1000T Control:          0x0200
        Phy 1000T Status:           0x4000
        Phy Extended Status:        0x3000

    Detailed Output - RX Descriptor Ring:

    rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
    rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

   ........
```

다음은 ASA 5512-X~ASA 5555-X의 내부 인터페이스에 대한 **show controller detail** 명령의 샘플 출력입니다.

```
ciscoasa# show controller detail

Internal-Control0/0:
   ASA IPS/VM Back Plane TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap1
         Num of Transmit Rings : 1
```

```
        Num of Receive Rings  : 1
        Ring Size             : 128
        Max Frame Length      : 1550
        Out of Buffer         : 0
        Reset                 : 0
        Drop                  : 0
    Transmit Ring [0]:
        tx_pkts_in_queue      : 0
        tx_pkts               : 176
        tx_bytes              : 9664
    Receive Ring [0]:
        rx_pkts_in_queue      : 0
        rx_pkts               : 0
        rx_bytes              : 0
        rx_drops              : 0

Internal-Data0/1:
   ASA IPS/VM Management Channel TunTap Interface , port id 9
     Major Configuration Parameters
        Device Name           : en_vtun
        Linux Tun/Tap Device  : /dev/net/tun/tap2
        Num of Transmit Rings : 1
        Num of Receive Rings  : 1
        Ring Size             : 128
        Max Frame Length      : 1550
        Out of Buffer         : 0
        Reset                 : 0
        Drop                  : 0
    Transmit Ring [0]:
        tx_pkts_in_queue      : 0
        tx_pkts               : 176
        tx_bytes              : 9664
    Receive Ring [0]:
        rx_pkts_in_queue      : 0
        rx_pkts               : 0
        rx_bytes              : 0
        rx_drops              : 0
```

다음은 **show controller slot** 명령의 샘플 출력입니다.

```
Slot  Card Description                                PCI-e Bandwidth Cap.
----  ----------------                                ----------------------
3.    ASA 5580 2 port 10GE SR Fiber Interface Card    Bus: x4, Card: x8

4.    ASA 5580 4 port GE Copper Interface Card        Bus: x4, Card: x4

5.    ASA 5580 2 port 10GE SR Fiber Interface Card    Bus: x8, Card: x8

6.    ASA 5580 4 port GE Fiber Interface Card         Bus: x4, Card: x4

7.    empty                                           Bus: x8

8.    empty                                           Bus: x8
```

다음은 **show controller pci** 명령의 샘플 출력입니다.

```
ciscoasa# show controller pci

PCI Evaluation Log:
  ------------------------------------------------------------------------------
    Empty

  PCI Bus:Device.Function (hex): 00:00.0 Vendor ID: 0x8086 Device ID: 0x3406
  ------------------------------------------------------------------------------
```

```
PCI Configuration Space (hex):
0x00: 86 80 06 34 00 00 10 00 22 00 00 06 10 00 00 00
0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x20: 00 00 00 00 00 00 00 00 00 00 00 00 86 80 00 00
0x30: 00 00 00 00 60 00 00 00 00 00 00 00 05 01 00 00
0x40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x60: 05 90 02 01 00 00 00 00 00 00 00 00 00 00 00 00
0x70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x90: 10 e0 42 00 20 80 00 00 00 00 00 00 41 3c 3b 00
0xa0: 00 00 41 30 00 00 00 00 c0 07 00 01 00 00 00 00
0xb0: 00 00 00 00 3e 00 00 00 09 00 00 00 00 00 00 00
0xc0: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe0: 01 00 03 c8 08 00 00 00 00 00 00 00 00 00 00 00
0xf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Link Capabilities: x4, Gen1
Link Status: x4, Gen1
```

관련 명령

명령	설명
show interface	인터페이스 통계를 표시합니다.
show tech-support	Cisco TAC에서 문제를 진단할 수 있도록 정보를 표시합니다.

show coredump filesystem

코어 덤프 파일 시스템의 내용을 표시하려면 **show coredump filesystem** 명령을 입력합니다.

show coredump filesystem

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 코어 덤프는 활성화되어 있지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 코어 덤프 파일 시스템의 내용을 표시합니다.

예

최근에 생성된 모든 코어 덤프의 내용을 표시하려면 **show coredump filesystem** 명령을 입력합니다.

```
ciscoasa(config)# show coredump filesystem
Coredump Filesystem Size is 100 MB
Filesystem type is FAT for disk0
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/loop0 102182 75240 26942 74% /mnt/disk0/coredumpfsys
Directory of disk0:/coredumpfsys/
246 -rwx 20205386 19:14:53 Nov 26 2008 core_lina.2008Nov26_191244.203.11.gz
247 -rwx 36707919 19:17:27 Nov 26 2008 core_lina.2008Nov26_191456.203.6.gz
```

관련 명령

명령	설명
coredump enable	코어 덤프 기능을 활성화합니다.
clear configure coredump	코어 덤프 파일 시스템에 현재 저장된 모든 코어 덤프를 제거하고 코어 덤프 로그를 지웁니다. 코어 덤프 파일 시스템 자체는 건드리지 않으며, 코어 덤프 컨피그레이션을 변경하거나 영향을 주지 않습니다.
clear coredump	코어 덤프 파일 시스템에 현재 저장된 모든 코어 덤프를 제거하고 코어 덤프 로그를 지웁니다. 코어 덤프 파일 시스템 자체는 건드리지 않으며, 코어 덤프 컨피그레이션을 변경하거나 영향을 주지 않습니다.
show coredump log	코어 덤프 로그를 표시합니다.

show coredump log

코어 덤프 로그의 내용을 가장 최근 내용부터 표시하려면 **show coredump log** 명령을 입력합니다. 코어 덤프 로그의 내용을 가장 오래된 내용부터 표시하려면 **show coredump log** 명령을 입력합니다.

show coredump log

show coredump log [**reverse**]

구문 설명

reverse	가장 오래된 코어 덤프 로그를 표시합니다.

기본값

기본적으로 코어 덤프는 활성화되어 있지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 코어 덤프 로그의 내용을 표시합니다. 로그는 현재 디스크에 있는 내용을 반영해야 합니다.

예

다음 예에서는 이 명령의 출력을 보여 줍니다.

```
ciscoasa(config)# show coredump log
[ 1 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
[ 2 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 5 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0'
```

참고 이전 코어 덤프 파일은 새 코어 덤프를 위한 공간을 확보하기 위해 삭제됩니다. 이는 코어 덤프 파일 시스템이 가득 차 현재 코어 덤프의 공간이 필요한 경우 ASA에서 자동으로 수행됩니다. 따라서 코어 덤프를 가능한 빨리 보관하여 충돌 시 덮어쓰지 않도록 해야 합니다.

```
ciscoasa(config)# show coredump log reverse
[ 1 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0''
[ 2 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump
record 'core_lina.2009Feb18_213558.203.11.gz'
[ 5 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
```

관련 명령

명령	설명
coredump enable	코어 덤프 기능을 활성화합니다.
clear configure coredump	코어 덤프 파일 시스템에 현재 저장된 모든 코어 덤프를 제거하고 코어 덤프 로그를 지웁니다. 코어 덤프 파일 시스템 자체는 건드리지 않으며, 코어 덤프 컨피그레이션을 변경하거나 영향을 주지 않습니다.
clear coredump	코어 덤프 파일 시스템에 현재 저장된 모든 코어 덤프를 제거하고 코어 덤프 로그를 지웁니다. 코어 덤프 파일 시스템 자체는 건드리지 않으며, 코어 덤프 컨피그레이션을 변경하거나 영향을 주지 않습니다.
show coredump filesystem	코어 덤프 파일 시스템의 내용을 표시합니다.

show counters

프로토콜 스택 카운터를 표시하려면 특권 EXEC 모드에서 **show counters** 명령을 사용합니다.

show counters [all | context *context-name* **| summary | top** *N* **] [detail] [protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

구문 설명

all	필터 세부사항을 표시합니다.
context *context-name*	상황 이름을 지정합니다.
:*counter_name*	이름으로 카운터를 지정합니다.
detail	추가 카운터 정보를 표시합니다.
protocol *protocol_name*	지정된 프로토콜에 대한 카운터를 표시합니다.
summary	카운터 요약을 표시합니다.
threshold *N*	지정된 임계값에 도달하거나 이를 초과하는 카운터만 표시합니다. 범위는 1~4294967295입니다.
top *N*	지정된 임계값에 도달하거나 이를 초과하는 카운터를 표시합니다. 범위는 1~4294967295입니다.

기본값

show counters summary detail threshold 1

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.
9.2(1)	이벤트 관리자에 대한 카운터가 추가되었습니다.

예

다음 예에서는 모든 카운터를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf

ciscoasa# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
UAUTH        IPV6_UNSUPPORTED     27   Summary
IDFW         HIT_USER_LIMIT        2   Summary
```

다음 예에서는 카운터 요약을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show counters summary
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   Summary
IOS_IPC      OUT_PKTS              2   Summary
```

다음 예에서는 상황에 대한 카운터를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show counters context single_vf
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               4   single_vf
IOS_IPC      OUT_PKTS              4   single_vf
```

다음 예에서는 이벤트 관리자에 대한 카운터를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show counters protocol eem
Protocol     Counter           Value   Context
EEM          SYSLOG            22      Summary
EEM          COMMANDS          6       Summary
EEM          FILES             3       Summary
```

관련 명령

명령	설명
clear counters	프로토콜 스택 카운터를 지웁니다.

show cpu

CPU 사용률 정보를 표시하려면 특권 EXEC 모드에서 **show cpu** 명령을 사용합니다.

[**cluster exec**] **show cpu** [**usage** *core-id* | **profile** | **dump** | **detailed**]

다중 상황 모드의 시스템 컨피그레이션:

[**cluster exec**] **show cpu** [**usage**] [**context** {**all** | *context_name*}]

구문 설명

all	모든 상황을 표시하도록 지정합니다.
cluster exec	(선택 사항) 클러스터링 환경에서 하나의 디바이스에서 **show cpu** 명령을 실행하고 나머지 모든 디바이스에서 동시에 이 명령을 실행할 수 있도록 합니다.
context	하나의 상황을 표시하도록 지정합니다.
context_name	표시할 상황의 이름을 지정합니다.
core-id	프로세서 코어 번호를 지정합니다.
detailed	(선택 사항) CPU 사용에 대한 내부 세부사항을 표시합니다.
dump	(선택 사항) TTY에 대한 덤프 프로파일링 데이터를 표시합니다.
profile	(선택 사항) CPU 프로파일링 데이터를 표시합니다.
usage	(선택 사항) CPU 사용량을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.6(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X를 지원하기 위해 *core-id* 옵션이 추가되었습니다.
9.1(2)	**show cpu profile** 및 **show cpu profile dump** 명령에 대한 출력이 업데이트되었습니다.
9.2(1)	가상 플랫폼 CPU 사용량이 ASAv 출력에 추가되었습니다.

사용 지침

CPU 사용량은 5초 단위의 부하 근사값을 계산한 다음 이 근사값을 이동 평균에 따라 두 개로 나눈 값으로 계산됩니다.

show cpu 명령을 사용하여 프로세스 관련 부하(즉, 단일 모드와 다중 상황 모드 시스템 컨피그레이션의 **show process** 명령 출력에 나열된 항목을 대신한 활동)를 찾을 수 있습니다.

또한 다중 상황 모드에서는 각 상황을 변경하고 **show cpu** 명령을 입력하거나 **show cpu context** 명령을 입력하여 프로세스 관련 부하를 구성된 모든 상황에서 사용한 CPU로 세분화하도록 요청할 수 있습니다.

프로세스 관련 부하는 가장 가까운 정수로 반올림되지만 상황 관련 부하에는 소수 자릿수 하나가 추가됩니다. 예를 들어 시스템 상황에서 **show cpu** 명령을 입력하면 **show cpu context system** 명령을 입력할 때와 다른 숫자가 생성됩니다. 전자는 **show cpu context all** 명령에 표시되는 모든 내용의 대략적인 요약이고, 후자는 해당 요약에 일부에 불과합니다.

CPU 문제를 해결할 때 **show cpu profile dump** 명령을 **cpu profile activate** 명령과 함께 사용하여 TAC 사용에 대한 정보를 수집할 수 있습니다. **show cpu profile dump** 명령 출력은 16진수 형식입니다.

CPU 프로파일러가 시작 조건이 발생하기를 대기하는 경우 **show cpu profile** 명령은 다음 출력을 표시합니다.

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

ASAv의 경우 다음 라이센싱 지침에 유의하십시오.

- 허용되는 vCPU 수는 설치된 vCPU 플랫폼 라이센스에 따라 결정됩니다.
  - 라이센스가 있는 vCPU 수가 프로비전된 vCPU 수와 일치하는 경우에는 상태가 Compliant입니다.
  - 라이센스가 있는 vCPU 수가 프로비전된 vCPU 수보다 적은 경우에는 상태가 Noncompliant: Over-provisioned입니다.
  - 라이센스가 있는 vCPU 수가 프로비전된 vCPU 수보다 많은 경우에는 상태가 Compliant: Under-provisioned입니다.
- 메모리 제한은 프로비전된 vCPU 수에 따라 결정됩니다.
  - 프로비전된 메모리가 허용 한도에 도달한 경우에는 상태가 Compliant입니다.
  - 프로비전된 메모리가 허용 한도를 초과한 경우에는 상태가 Noncompliant: Over-provisioned입니다.
  - 프로비전된 메모리가 허용 한도에 미달하는 경우에는 상태가 Compliant: Under-provisioned입니다.
- 주파수 예약 제한은 프로비전된 vCPU 수에 따라 결정됩니다.
  - 주파수 예약 메모리가 필수 최소값(1000MHz)이거나 이를 초과하는 경우에는 상태가 Compliant입니다.
  - 주파수 예약 메모리가 필수 최소값(1000MHz)에 미달하는 경우에는 상태가 Under-provisioned입니다.

예를 들어 적용된 라이센스가 없는 경우 다음 출력이 표시됩니다. 허용되는 vCPU 수는 라이센스가 있는 수를 의미하며, Noncompliant: Over-provisioned는 제품이 라이센스보다 더 많은 리소스로 실행되고 있음을 나타냅니다.

```
Virtual platform CPU resources
------------------------------
Number of vCPUs              :        1
Number of allowed vCPUs      :        0
vCPU Status                  :        Noncompliant: Over-provisioned
```

예

다음 예에서는 CPU 사용률을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

다음 예에서는 자세한 CPU 사용률 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)

Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%

CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%

Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

참고

"Current control point elapsed versus the maximum control point elapsed for" 문은 현재 제어 지점 부하가 정의된 기간 내에 표시된 최대 부하와 비교됨을 의미합니다. 이는 절대값이 아니라 비율입니다. 5초 간격의 경우 99%는 현재 제어 지점 부하가 이 5초 간격 동안 표시될 수 있는 최대 부하의 99%임을 의미합니다. 부하가 계속 증가하는 경우에는 항상 100%로 유지됩니다. 그러나 최대 절대값이 정의되지 않았으므로 실제 CPU에는 여유 공간이 많이 있을 수 있습니다.

다음 예에서는 다중 모드의 시스템 상황에 대한 CPU 사용률을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

다음 예에서는 모든 상황에 대한 CPU 사용률을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

다음 예에서는 "one"이라는 상황에 대한 CPU 사용률을 표시하는 방법을 보여 줍니다.

```
ciscoasa/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

다음 예에서는 프로파일러를 활성화하여 1000개의 샘플을 저장하도록 지시합니다.

```
ciscoasa# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

다음 예에서는 프로파일링 상태(in-progress 및 completed)를 표시합니다.

```
ciscoasa# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.

ciscoasa# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
---------------------------
…
---------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

다음 예에서는 ASAv에 대한 CPU 사용량을 보여 줍니다.

```
ciscoasa# show cpu
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

Virtual platform CPU resources
------------------------------
Number of vCPUs              :     2
Number of allowed vCPUs      :     2
vCPU Status                  :  Compliant

Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  4000 MHz
Maximum allowed              :  56000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :   136 MHz
```

다음 예에서는 ASAv에 대한 자세한 CPU 사용량을 보여 줍니다.

```
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.2 (0.2 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.1 (0.0 + 0.1)  0.0 (0.0 + 0.0)

Current control point elapsed versus the maximum control point elapsed for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%


CPU utilization of external processes for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%


Total CPU utilization for:
     5 seconds = 0.1%; 1 minute: 0.1%; 5 minutes: 0.1%

Virtual platform CPU resources
```

```
------------------------------
Number of vCPUs              :     4
Number of allowed vCPUs      :     4
vCPU Status                  :  Compliant

Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  20000 MHz
Maximum allowed              :  20000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :    99 MHz
```

이 정보를 복사하여 기록을 위해 TAC에 제공하십시오.

관련 명령

명령	설명
show counters	프로토콜 스택 카운터를 표시합니다.
cpu profile activate	CPU 프로파일링을 활성화합니다.

5 장

show crashinfo through show curpriv 명령

show crashinfo

플래시 메모리에 저장된 충돌 파일의 내용을 표시하려면 특권 EXEC 모드에서 **show crashinfo** 명령을 입력합니다.

show crashinfo [**save**]

구문 설명

save	(선택 사항) ASA가 충돌 정보를 플래시 메모리에 저장하도록 구성되었는지 여부를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.1(5)	출력에 **show process** 명령의 TID(스레드 ID)가 표시됩니다.

사용 지침

충돌 파일이 테스트 충돌로 인해 발생(**crashinfo test** 명령에서 생성)한 경우 충돌 파일의 첫 번째 문자열은 "**: Saved_Test_Crash**"이고 마지막 문자열은 "**: End_Test_Crash**"입니다. 충돌 파일이 실제 충돌로 인해 발생한 경우 충돌 파일의 첫 번째 문자열은 "**: Saved_Crash**"이고 마지막 문자열은 "**: End_Crash**"입니다. 여기에는 **crashinfo force page-fault** 또는 **crashinfo force watchdog** 명령 사용으로 인한 충돌이 포함됩니다.

플래시에 저장된 충돌 데이터가 없거나, **clear crashinfo** 명령을 입력하여 충돌 데이터를 지운 경우 **show crashinfo** 명령은 오류 메시지를 표시합니다.

예

다음 예에서는 현재 충돌 정보 컨피그레이션을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show crashinfo save
crashinfo save enable
```

다음 예에서는 충돌 파일 테스트에 대한 출력을 보여 줍니다. 그러나 이 테스트에서는 실제로 ASA가 충돌하지 않습니다. 시뮬레이션된 예제 파일을 제공할 뿐입니다.

```
ciscoasa(config)# crashinfo test
ciscoasa(config)# exit
ciscoasa# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        Cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
F-flags  : 0x2
F-flags2: 0x0
F-flags3: 0x10000
F-flags4: 0x0
F-bytes  : 0
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
```

```
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
```

```
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
```

```
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
```

```
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show vpn-sessiondb summary ------------------

Active Session Summary

Sessions:
                          Active : Cumulative : Peak Concurrent : Inactive
  SSL VPN               :       2 :          2 :               2
    Clientless only     :       0 :          0 :               0
    With client         :       2 :          2 :               2 :        0
  Email Proxy           :       0 :          0 :               0
  IPsec LAN-to-LAN      :       1 :          1 :               1
  IPsec Remote Access   :       0 :          0 :               0
  VPN Load Balancing    :       0 :          0 :               0
  Totals                :       3 :          3

License Information:
  Shared VPN License Information:
    SSL VPN                   :     1500
      Allocated to this device :       50
      Allocated in network     :       50
      Device limit             :      750

  IPsec   :    750    Configured :    750    Active :      1    Load :   0%
  SSL VPN :     52    Configured :     52    Active :      2    Load :   4%
                         Active : Cumulative : Peak Concurrent
  IPsec               :          1 :          1 :               1
  SSL VPN             :          2 :         10 :               2
    AnyConnect Mobile :          0 :          0 :               0
    Linksys Phone     :          0 :          0 :               0
  Totals              :          3 :         11

Tunnels:
                    Active : Cumulative : Peak Concurrent
  IKE         :          1 :          1 :               1
```

```
  IPsec       :          1 :          1 :              1
  Clientless  :          2 :          2 :              2
  SSL-Tunnel  :          2 :          2 :              2
  DTLS-Tunnel :          2 :          2 :              2
  Totals      :          8 :          8
------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------

PC  SP       STATE    Runtime  SBASE Stack              Process   TID
Hsi 001e3329 00763e7c 0053e5c8 0     00762ef4 3784/4096 arp_timer 0x000000000000000a
Lsi 001e80e9 00807074 0053e5c8 0     008060fc 3792/4096 FragDBGC  0x000000000000006b
```

```
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPsec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
```

```
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

관련 명령

명령	설명
clear crashinfo	충돌 파일의 내용을 삭제합니다.
crashinfo force	ASA를 강제로 충돌시킵니다.
crashinfo save disable	플래시 메모리에 쓰기에서 충돌 정보를 비활성화합니다.
crashinfo test	충돌 정보를 플래시 메모리의 파일에 저장하는 ASA의 기능을 테스트합니다.

show crashinfo console

crashinfo console 명령의 컨피그레이션 설정을 표시하려면 **show crashinfo console** 명령을 입력합니다.

show crashinfo console

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(4)	이 명령이 도입되었습니다.

사용 지침

FIPS 140-2에서는 중요한 보안 파라미터(키, 비밀번호 등)를 암호화 경계(섀시) 외부에 배포하는 것을 금지하고 있습니다. 어설션 또는 checkheap 오류로 인해 디바이스가 충돌하는 경우 콘솔에 덤프된 스택 또는 메모리 영역에 민감한 데이터를 포함할 수 있습니다. 이 출력은 FIPS 모드에서 무시되어야 합니다.

예

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

관련 명령

명령	설명
clear configure fips	NVRAM에 저장된 시스템 또는 모듈 FIPS 컨피그레이션 정보를 지웁니다.
crashinfo console disable	플래시에 대한 충돌 쓰기 정보 읽기, 쓰기 및 컨피그레이션을 비활성화합니다.
fips enable	시스템 또는 모듈에서 FIPS 규정 준수를 적용하는 정책 확인을 활성화하거나 비활성화합니다.
show running-config fips	ASA에서 실행 중인 FIPS 컨피그레이션을 표시합니다.

show crypto accelerator statistics

하드웨어 암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 표시하려면 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto accelerator statistics** 명령을 사용합니다.

show crypto accelerator statistics

구문 설명

이 명령에는 키워드 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

출력 통계는 다음과 같이 정의됩니다.

Accelerator 0은 소프트웨어 기반 암호화 엔진에 대한 통계를 표시합니다.

Accelerator 1은 하드웨어 기반 암호화 엔진에 대한 통계를 표시합니다.

RSA 통계는 기본적으로 소프트웨어에서 실행되는 2048비트 키에 대한 RSA 작업을 표시합니다. 즉, 2048비트 키가 있는 경우 IKE/SSL VPN은 IPsec/SSL 협상 단계 중에 소프트웨어에서 RSA 작업을 수행합니다. 실제 IPsec/SSL 트래픽은 여전히 하드웨어를 통해 처리됩니다. 이로 인해 동시에 시작하는 동시 세션이 많은 경우 CPU 사용량이 높아져 여러 RSA 키 작업이 수행되고 CPU 사용량이 증가할 수 있습니다. 따라서 CPU 사용량이 많은 조건에서 실행할 경우 1024비트 키를 사용하여 하드웨어에서 RSA 키 작업을 처리해야 합니다. 이렇게 하려면 ID 인증서를 다시 등록해야 합니다. 릴리스 8.3(2) 이상에서는 5510~5550 플랫폼에서 crypto engine large-mod-accel 명령을 사용하여 이러한 작업을 하드웨어에서 수행할 수도 있습니다.

2048비트 RSA 키를 사용하고 RSA 처리를 소프트웨어에서 수행하는 경우 CPU 프로파일링을 사용하여 CPU 사용량을 증가시키는 기능을 확인할 수 있습니다. 일반적으로 bn_* 및 BN_* 함수는 RSA에 사용된 대용량 데이터 집합에 대한 수학 연산이며, 소프트웨어에서 RSA 작업을 수행하는 동안 CPU 사용량을 검사할 때 가장 유용합니다. 예를 들면 다음과 같습니다.

```
@@@@@@@@@@@@@@@@@@@@..............................  36.50% : _bn_mul_add_words
@@@@@@@@@@.....................................  19.75% : _bn_sqr_comba8
```

Diffie-Hellman 통계는 모듈러스 크기가 1024보다 큰 암호화 작업이 소프트웨어에서 수행되고 있음을 보여 줍니다(예: DH5(Diffie-Hellman 그룹 5에서 1536 사용)). 이 경우 2048비트 키 인증서는 소프트웨어에서 처리되며, 이로 인해 많은 세션이 실행 중인 경우 CPU 사용량이 증가할 수 있습니다.

참고 ASA 5505(Cavium CN505 프로세서 탑재)는 하드웨어 가속화 768비트 및 1024비트 키 생성에 대해 Diffie-Hellman 그룹 1 및 2만 지원합니다. Diffie-Hellman 그룹 5(1536비트 키 생성)는 소프트웨어에서 수행됩니다.

Adaptive Security Appliance의 단일 암호화 엔진은 IPsec 및 SSL 작업을 수행합니다. 부팅 시 하드웨어 암호화 가속기에 로드된 암호화(Cavium) 마이크로코드의 버전을 표시하려면 **show version** 명령을 입력합니다. 예를 들면 다음과 같습니다.

```
ciscoasa(config) show version

Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is "disk0:/interim/asa804-8-k8.bin"
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.05
```

DSA 통계는 2단계로 키 생성을 보여 줍니다. 첫 번째 단계에서는 시스템의 여러 사용자 간에 공유할 수 있는 알고리즘 파라미터를 선택합니다. 두 번째 단계에서는 단일 사용자의 개인 키 및 공개 키를 계산합니다.

SSL 통계는 하드웨어 암호화 가속기에 대한 SSL 트랜잭션에 포함된 프로세서 중심적 공개 키 암호화 알고리즘에 대한 기록을 보여 줍니다.

RNG 통계는 키로 사용할 동일한 난수 집합을 자동으로 생성할 수 있는 발신자 및 수신자에 대한 기록을 보여 줍니다.

예 글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 전역 암호화 가속기 통계를 보여 줍니다.

```
ciscoasa # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
```

```
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
```

```
   Output hashed packets: 700
   Output hashed bytes: 744800
   Encrypted packets: 700
   Encrypted bytes: 728352
[Diffie-Hellman statistics]
   Keys generated: 97
   Secret keys derived: 1
[RSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
   Encrypted packets: 0
   Encrypted bytes: 0
   Decrypted packets: 0
   Decrypted bytes: 0
[DSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[SSL statistics]
   Outbound records: 0
   Inbound records: 0
[RNG statistics]
   Random number requests: 1
   Random number request failures: 0
```

다음 표에는 출력 항목의 의미가 설명되어 있습니다.

출력	설명
Capacity	이 섹션은 ASA에서 지원할 수 있는 암호화 가속과 관련이 있습니다.
Supports hardware crypto	(True/False) ASA에서 하드웨어 암호화 가속을 지원할 수 있습니다.
Supports modular hardware crypto	(True/False) 지원되는 하드웨어 암호화 가속기를 별도의 플러그인 카드 또는 모듈로 삽입할 수 있습니다.
Max accelerators	ASA에서 지원하는 하드웨어 암호화 가속기의 최대 개수입니다.
Mac crypto throughput	ASA에 대한 최대 정격 VPN 처리량입니다.
Max crypto connections	ASA에 대해 지원되는 최대 VPN 터널 수입니다.
Global Statistics	이 섹션은 ASA에 통합된 하드웨어 암호화 가속기와 관련이 있습니다.
Number of active accelerators	활성 하드웨어 가속기 수입니다. 활성 하드웨어 가속기가 초기화되었으며, 암호화 명령을 처리할 수 있습니다.
Number of non-operational accelerators	비활성 하드웨어 가속기 수입니다. 비활성 하드웨어 가속기가 감지되었지만 초기화를 완료하지 않았거나 실패하여 더 이상 사용할 수 없습니다.
Input packets	모든 하드웨어 암호화 가속기에서 처리된 인바운드 패킷 수입니다.
Input bytes	처리된 인바운드 패킷의 데이터 바이트 수입니다.
Output packets	모든 하드웨어 암호화 가속기에서 처리된 아웃바운드 패킷 수입니다.

출력(계속)	설명(계속)
Output error packets	모든 하드웨어 암호화 가속기에서 처리된 아웃바운드 패킷 중 오류가 감지된 패킷 수입니다.
Output bytes	처리된 아웃바운드 패킷의 데이터 바이트 수입니다.
Accelerator 0	이 섹션은 각각 암호화 가속기와 관련이 있습니다. 첫 번째(Accelerator 0)는 항상 소프트웨어 암호화 엔진입니다. 하드웨어 가속기가 아니지만 ASA는 이를 사용하여 특정 암호화 작업을 수행하며 해당 통계가 여기에 표시됩니다. Accelerator 1 이상은 항상 하드웨어 암호화 가속기입니다.
Status	가속기가 초기화 중인지, 활성 상태인지 또는 실패했는지를 나타내는 가속기의 상태입니다.
Software crypto engine	가속기 유형 및 펌웨어 버전(해당되는 경우)입니다.
Slot	가속기의 슬롯 번호(해당 되는 경우)입니다.
Active time	가속기가 활성 상태로 유지된 기간입니다.
Total crypto transforms	가속기가 수행한 총 암호화 명령 수입니다.
Total dropped packets	오류로 인해 가속기에서 삭제된 총 패킷 수입니다.
Input statistics	이 섹션은 가속기에서 처리된 입력 트래픽과 관련이 있습니다. 입력 트래픽은 해독 및/또는 인증해야 하는 암호 텍스트로 간주됩니다.
Input packets	가속기에서 처리된 입력 패킷 수입니다.
Input bytes	가속기에서 처리된 입력 바이트 수입니다.
Input hashed packets	가속기에서 해시 작업을 수행한 패킷 수입니다.
Input hashed bytes	가속기에서 해시 작업을 수행한 바이트 수입니다.
Decrypted packets	가속기에서 대칭 암호 해독 작업을 수행한 패킷 수입니다.
Decrypted bytes	가속기에서 대칭 암호 해독 작업을 수행한 바이트 수입니다.
Output statistics	이 섹션은 가속기에서 처리된 출력 트래픽과 관련이 있습니다. 입력 트래픽은 암호화 및/또는 해시되어야 하는 일반 텍스트로 간주됩니다.
Output packets	가속기에서 처리된 출력 패킷 수입니다.
Output bad packets	가속기에서 처리된 출력 패킷 중 오류가 감지된 패킷 수입니다.
Output bytes	가속기에서 처리된 출력 패킷 수입니다.
Output hashed packets	가속기에서 아웃바운드 해시 작업을 수행한 패킷 수입니다.
Output hashed bytes	가속기에서 아웃바운드 해시 작업을 수행한 바이트 수입니다.
Encyrpted packets	가속기에서 대칭 암호화 작업을 수행한 패킷 수입니다.
Encyrpted bytes	가속기에서 대칭 암호화 작업을 수행한 바이트 수입니다.
Diffie-Hellman statistics	이 섹션은 Diffie-Hellman 키 교환 작업과 관련이 있습니다.
Keys generated	가속기에서 생성된 Diffie-Hellman 키 집합 수입니다.
Secret keys derived	가속기에서 파생된 Diffie-Hellman 공유 암호 수입니다.
RSA statistics	이 섹션은 RSA 암호화 작업과 관련이 있습니다.
Keys generated	가속기에서 생성된 RSA 키 집합 수입니다.
Signatures	가속기에서 수행된 RSA 서명 작업 수입니다.

출력(계속)	설명(계속)
Verifications	가속기에서 수행된 RSA 서명 확인 수입니다.
Encrypted packets	가속기에서 RSA 암호화 작업을 수행한 패킷 수입니다.
Decrypted packets	가속기에서 RSA 암호 해독 작업을 수행한 패킷 수입니다.
Decrypted bytes	가속기에서 RSA 암호 해독 작업을 수행한 데이터의 바이트 수입니다.
DSA statistics	이 섹션은 DSA 작업과 관련이 있습니다. DSA는 현재 버전 8.2에서 지원되지 않으므로 이러한 통계는 더 이상 표시되지 않습니다.
Keys generated	가속기에서 생성된 DSA 키 집합 수입니다.
Signatures	가속기에서 수행된 DSA 서명 작업 수입니다.
Verifications	가속기에서 수행된 DSA 서명 확인 수입니다.
SSL statistics	이 섹션은 SSL 레코드 처리 작업과 관련이 있습니다.
Outbound records	가속기에서 암호화 및 인증된 SSL 레코드 수입니다.
Inbound records	가속기에서 암호 해독 및 인증된 SSL 레코드 수입니다.
RNG statistics	이 섹션은 난수 생성과 관련이 있습니다.
Random number requests	가속기에 대한 난수 요청 수입니다.
Random number request failures	가속기에 대한 성공하지 못한 난수 요청 수입니다.

관련 명령

명령	설명
clear crypto accelerator statistics	암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 지웁니다.
clear crypto protocol statistics	암호화 가속기 MIB에서 프로토콜 관련 통계를 지웁니다.
show crypto protocol statistics	암호화 가속기 MIB에서 프로토콜 관련 통계를 표시합니다.

show crypto ca certificates

특정 신뢰 지점과 연계된 인증서를 표시하거나, 시스템에 설치된 모든 인증서를 표시하려면 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ca certificates** 명령을 사용합니다.

show crypto ca certificates [*trustpointname*]

구문 설명

trustpointname	(선택 사항) 신뢰 지점의 이름입니다. 이름을 지정하지 않은 경우 이 명령은 ASA에 설치된 모든 인증서를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show crypto ca certificates** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = example.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
```

```
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ca authenticate	지정된 신뢰 지점에 대한 CA 인증서를 가져옵니다.
crypto ca crl request	지정된 신뢰 지점의 컨피그레이션 파라미터에 따라 CRL을 요청합니다.
crypto ca enroll	CA 등록 프로세스를 시작합니다.
crypto ca import	지정된 신뢰 지점으로 인증서를 내보냅니다.
crypto ca trustpoint	지정된 신뢰 지점에 대한 신뢰 지점 컨피그레이션 모드를 시작합니다.

show crypto ca crl

캐시된 모든 CRL을 표시하거나, 지정된 신뢰 지점에 대해 캐시된 모든 CRL을 표시하려면 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ca crl** 명령을 사용합니다.

show crypto ca crl [trustpool | trustpoint <*trustpointname*>]

구문 설명

trustpoint *trustpointname*	(선택 사항) 신뢰 지점의 이름입니다. 이름을 지정하지 않은 경우 이 명령은 ASA에 캐시된 모든 CRL을 표시합니다.
trustpool	신뢰 풀의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show crypto ca crl** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show crypto ca crl tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ca authenticate	지정된 신뢰 지점에 대한 CA 인증서를 가져옵니다.
crypto ca crl request	지정된 신뢰 지점의 컨피그레이션 파라미터에 따라 CRL을 요청합니다.
crypto ca enroll	CA 등록 프로세스를 시작합니다.
crypto ca import	지정된 신뢰 지점으로 인증서를 내보냅니다.
crypto ca trustpoint	지정된 신뢰 지점에 대한 신뢰 지점 컨피그레이션 모드를 시작합니다.

show crypto ca server

ASA의 로컬 CA 컨피그레이션 상태를 표시하려면 CA 서버 컨피그레이션, 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ca server** 명령을 사용합니다.

show crypto ca server

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

예

다음은 **show crypto ca server** 명령의 샘플 출력입니다.

```
ciscoasa# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 2009
    CRL not present.
    Current primary storage dir: nvram:
ciscoasa#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스할 수 있도록 합니다.
debug crypto ca server	로컬 CA 서버를 구성할 때 디버깅 메시지를 표시합니다.
show crypto ca server certificate	base64 형식의 로컬 CA 인증서를 표시합니다.
show crypto ca server crl	로컬 CA CRL의 수명을 표시합니다.

show crypto ca server cert-db

특정 사용자에게 발급된 것을 포함하여 모든 로컬 CA 서버 인증서 또는 로컬 CA 서버 인증서의 하위 집합을 표시하려면 CA 서버 컨피그레이션, 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ca server cert-db** 명령을 사용합니다.

show crypto ca server cert-db [**username** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]

구문 설명

allowed	해당 인증서의 상태에 상관없이 등록이 허용된 사용자가 표시되도록 지정합니다 .
enrolled	유효한 인증서를 가진 사용자가 표시되도록 지정합니다.
expired	만료된 인증서를 보유한 사용자가 표시되도록 지정합니다.
on-hold	아직 등록하지 않은 사용자가 표시되도록 지정합니다.
serial *certificate-serial-number*	표시되는 특정 인증서의 일련 번호를 지정합니다. 일련 번호는 16진수 형식이어야 합니다.
username *username*	인증서 소유자를 지정합니다. username은 사용자 이름 또는 이메일 주소일 수 있습니다. 이메일 주소의 경우 엔드 유저에게 연락하고 OTP(일회성 비밀번호)를 제공하는 데 사용되는 이메일 주소입니다. 엔드 유저에 대한 이메일 알림을 활성화하려면 이메일 주소가 필요합니다.

기본값

사용자 이름 또는 인증서 일련 번호를 지정하지 않은 경우 기본적으로 발급된 인증서의 전체 데이터베이스가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

show crypto ca server cert-db 명령은 로컬 CA 서버에서 발급한 사용자 인증서 목록을 표시합니다. 하나 이상의 선택적 certificate-type 키워드 및/또는 선택적 인증서 일련 번호와 함께 특정 사용자 이름을 지정하여 인증서 데이터베이스의 하위 집합을 표시할 수 있습니다.

키워드나 일련 번호 없이 사용자 이름을 지정하면 해당 사용자에 대해 발급된 모든 인증서가 표시됩니다. 각 사용자에 대해 사용자 이름, 이메일 주소, 도메인 이름, 등록이 허용되는 기간, 사용자가 등록 초대장과 함께 알림을 받은 횟수 가 출력에 표시됩니다.

또한 다음 정보가 출력에 표시됩니다.

- NOTIFIED 필드는 여러 미리 알림을 지원하는 데 필요합니다. 사용자에게 등록을 위한 OTP 알림을 보내야 하는 경우 및 미리 알림을 시도하는 경우를 추적합니다. 이 필드는 초기에는 0으로 설정됩니다. 사용자 항목이 등록 허용으로 표시될 때마다 1씩 증가합니다. 현재는 초기 OTP 알림이 생성되었습니다.
- NOTIFY 필드는 미리 알림이 전송될 때마다 증분됩니다. OTP가 만료되기 전에 세 개의 알림이 전송됩니다. 사용자가 등록하도록 허용된 경우, 만료 중간 시점 및 만료 시간의 ¾이 경과했을 때 알림이 전송됩니다. 이 필드는 관리자가 시작하는 등록에만 사용됩니다. 자동 인증서 갱신의 경우 인증서 데이터베이스의 NOTIFY 필드가 사용됩니다.

참고 이 명령의 알림 카운터는 사용자에게 만료 전 인증서 갱신 알림이 전송된 횟수를 추적하는 데 사용되는 반면, show crypto ca server user-db의 알림 카운터는 사용자에게 인증서 등록 알림이 전송된 횟수를 추적하는 데 사용됩니다. 갱신 알림은 cert-db를 통해 추적되며, user-db에 포함되지 않습니다.

각 인증서에는 인증서 일련 번호, 발급 및 만료 날짜, 인증서 상태(Revoked/Not Revoked)가 표시됩니다.

예

다음 예에서는 CA 서버에서 asa에 발급한 모든 인증서를 표시하도록 요청합니다.

```
ciscoasa# show crypto ca server cert-db username asa
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

다음 예에서는 로컬 CA 서버에서 발급한 일련 번호가 0x2인 모든 인증서를 표시하도록 요청합니다.

```
ciscoasa# show crypto ca server cert-db serial 2

Username:asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

다음 예에서는 로컬 CA 서버에서 발급한 모든 인증서를 표시하도록 요청합니다.

```
ciscoasa# show crypto ca server cert-db
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스할 수 있도록 합니다.
crypto ca server revoke	로컬 CA 서버에서 발급한 인증서를 인증서 데이터베이스와 CRL 모두에서 해지된 것으로 표시합니다.
lifetime crl	CRL 수명을 지정합니다.

show crypto ca server certificate

base64 형식의 로컬 CA 서버 인증서를 표시하려면 CA 서버 컨피그레이션, 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ca server certificate** 명령을 사용합니다.

show crypto ca server certificate

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

show crypto ca server certificate 명령은 base64 형식의 로컬 CA 서버 인증서를 표시합니다. 이를 통해 로컬 CA 서버를 신뢰해야 하는 다른 디바이스로 내보내는 동안 인증서를 잘라내어 붙여넣을 수 있습니다.

예

다음은 **show crypto ca server certificate** 명령의 샘플 출력입니다.

```
ciscoasa# show crypto ca server certificate

The base64 encoded local CA certificate follows:

MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

ciscoasa#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스할 수 있도록 합니다.
issuer-name	인증서 인증 기관의 주체 이름 DN을 지정합니다.
keysize	사용자 인증서 등록 시 생성되는 공개 및 개인 키의 크기를 지정합니다.
lifetime	CA 인증서 및 발급된 인증서의 수명을 지정합니다.
show crypto ca server	ASCII 텍스트 형식으로 로컬 CA 컨피그레이션을 표시합니다.

show crypto ca server crl

로컬 CA의 현재 CRL을 표시하려면 CA 서버 컨피그레이션, 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ca server crl** 명령을 사용합니다.

show crypto ca server crl

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

예

다음은 **show crypto ca server crl** 명령의 샘플 출력입니다.

```
ciscoasa# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
ciscoasa#
```

관련 명령

명령	설명
cdp-url	CA에서 발급한 인증서에 CDP(CRL 배포 지점)를 포함하도록 지정합니다.
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스할 수 있도록 합니다.
crypto ca server revoke	로컬 CA 서버에서 발급한 인증서를 인증서 데이터베이스와 CRL에서 해지된 것으로 표시합니다.
lifetime crl	CRL 수명을 지정합니다.
show crypto ca server	CA 컨피그레이션의 상태를 표시합니다.

show crypto ca server user-db

로컬 CA 서버 사용자 데이터베이스에 포함된 사용자를 표시하려면 CA 서버 컨피그레이션, 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ca server user-db** 명령을 사용합니다.

show crypto ca server user-db [expired | allowed | on-hold | enrolled]

구문 설명

allowed	(선택 사항) 해당 인증서의 상태에 상관없이 등록이 허용된 사용자가 표시되도록 지정합니다.
enrolled	(선택 사항) 유효한 인증서를 가진 사용자가 표시되도록 지정합니다.
expired	(선택 사항) 만료된 인증서를 보유한 사용자가 표시되도록 지정합니다.
on-hold	(선택 사항) 아직 등록하지 않은 사용자가 표시되도록 지정합니다.

기본값

아무 키워드도 입력하지 않으면 기본적으로 데이터베이스의 모든 사용자가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

예

다음 예에서는 현재 등록된 사용자를 표시합니다.

```
ciscoasa# show crypto ca server user-db enrolled
Username    DN                Certificate issued    Certificate expiration
exampleusercn=Example User,o=...5/31/2009           5/31/2010

ciscoasa#
```

사용 지침

이 명령의 알림 카운터는 사용자에게 인증서 등록 알림이 전송된 횟수를 추적하는 데 사용되는 반면, show crypto ca server cert-db의 알림 카운터는 사용자에게 만료 전 인증서 갱신 알림이 전송된 횟수를 추적하는 데 사용됩니다. 갱신 알림은 cert-db를 통해 추적되며, user-db에 포함되지 않습니다.

관련 명령

명령	설명
crypto ca server user-db add	CA 서버 사용자 데이터베이스에 사용자를 추가합니다.
crypto ca server user-db allow	특정 사용자 또는 CA 서버 데이터베이스의 사용자 하위 집합이 로컬 CA에 등록하도록 허용합니다.
crypto ca server user-db remove	CA 서버 사용자 데이터베이스에서 사용자를 제거합니다.
crypto ca server user-db write	로컬 CA 데이터베이스에 구성된 사용자 정보를 저장소에 기록합니다.
show crypto ca server cert-db	로컬 CA에서 발급한 모든 인증서를 표시합니다.

show crypto ca trustpool

신뢰 풀을 구성하는 인증서를 표시하려면 특권 EXEC 모드에서 **show crypto ca trustpool** 명령을 사용합니다.

show crypto ca trustpool [detail]

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령은 모든 신뢰 풀 인증서를 축약된 형식으로 표시합니다. “detail” 옵션을 지정하면 추가 정보가 포함됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show crypto ca trustpool 명령의 출력에 각 인증서의 지문 값이 포함됩니다. 이러한 값은 제거 작업에 필요합니다.

예

```
ciscoasa# show crypto ca trustpool

CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024
```

```
CA Certificate
Status: Available
Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

관련 명령

명령	설명
clear crypto ca trustpool	신뢰 풀에서 모든 인증서를 제거합니다.
crypto ca trustpool import	PKI 신뢰 풀을 구성하는 인증서를 가져옵니다.
crypto ca trustpool remove	지정된 단일 인증서를 신뢰 풀에서 제거합니다.

show crypto ca trustpool policy

구성된 신뢰 풀 정책을 표시하고, 적용된 인증서 맵을 처리하여 정책에 미치는 영향을 확인하려면 특권 EXEC 모드에서 **show crypto ca trustpool policy** 명령을 사용합니다.

show crypto ca trustpool policy

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

예

```
ciscoasa(config)# sh run cry ca cert map
crypto ca certificate map map1 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca
crypto ca certificate map map 2 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca2
ciscoasa(config)#

ciscoasa(config)# sh run crypto ca trustpool policy
crypto ca trustpool policy
revocation-check none
match certificate map2 allow expired-certificate
match certificate map1 skip revocation-check
crl cache-time 123
ciscoasa(config)#

ciscoasa# show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
```

```
action:skip revocation-check

map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates

ciscoasa(config)#
```

관련 명령

명령	설명
crypto ca trustpool policy	신뢰 풀 정책을 정의하는 명령을 제공하는 하위 모드를 시작합니다.

show crypto debug-condition

현재 구성된 필터, 일치하지 않는 상태, IPsec 및 ISAKMP 디버깅 메시지의 오류 상태를 표시하려면 글로벌 컨피그레이션 모드에서 **show crypto debug-condition** 명령을 사용합니다.

show crypto debug-condition

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

예

다음 예에서는 필터링 조건을 보여 줍니다.

```
ciscoasa(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON

IKE peer IP address filters:
1.1.1.0/24   2.2.2.2

IKE user name filters:
my_user
```

관련 명령

명령	설명
debug crypto condition	IPsec 및 ISAKMP 디버깅 메시지에 대한 필터링 조건을 설정합니다.
debug crypto condition error	필터링 조건이 지정되었는지 여부에 상관없이 디버깅 메시지를 표시합니다.
debug crypto condition unmatched	상황 정보가 부족하여 필터링할 수 없는 IPsec 및 ISAKMP에 대한 디버깅 메시지를 표시합니다.

show crypto ikev1 sa

IKEv1 런타임 SA 데이터베이스를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto ikev1 sa** 명령을 사용합니다.

show crypto ikev1 sa [**detail**]

구문 설명

detail	SA 데이터베이스에 대한 자세한 출력을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

이 명령의 출력에는 다음 필드가 포함됩니다.

Detail이 지정되지 않은 경우

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail이 지정된 경우

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 SA 데이터베이스에 대한 자세한 정보를 표시합니다.

```
ciscoasa(config)# show crypto ikev1 sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

관련 명령

명령	설명
show crypto ikev2 sa	IKEv2 런타임 SA 데이터베이스를 표시합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show crypto ikev2 sa

IKEv2 런타임 SA 데이터베이스를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto ikev2 sa** 명령을 사용합니다.

show crypto ikev2 sa [**detail**]

구문 설명

detail	SA 데이터베이스에 대한 자세한 출력을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

이 명령의 출력에는 다음 필드가 포함됩니다.

Detail이 지정되지 않은 경우

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail이 지정된 경우

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 SA 데이터베이스에 대한 자세한 정보를 표시합니다.

```
ciscoasa(config)# show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status          Role
671069399                10.0.0.0/500 10.255.255.255/500      READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

관련 명령

명령	설명
show crypto ikev1 sa	IKEv1 런타임 SA 데이터베이스를 표시합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show crypto ipsec df-bit

지정된 인터페이스에 대한 IPsec 패킷의 IPsec DF 비트 정책을 표시하려면 글로벌 컨피그레이션 모드 및 특권 EXEC 모드에서 **show crypto ipsec df-bit** 명령을 사용합니다.

show crypto ipsec df-bit *interface*

구문 설명

interface	인터페이스 이름을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 inside라는 인터페이스에 대한 IPsec DF 비트 정책을 표시합니다.

```
ciscoasa(config)# show crypto ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ipsec df-bit	IPsec 패킷에 대한 IPsec DF 비트 정책을 구성합니다.
crypto ipsec fragmentation	IPsec 패킷에 대한 조각화 정책을 구성합니다.
show crypto ipsec fragmentation	IPsec 패킷에 대한 조각화 정책을 표시합니다.

show crypto ipsec fragmentation

IPsec 패킷에 대한 조각화 정책을 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto ipsec fragmentation** 명령을 사용합니다.

show crypto ipsec fragmentation *interface*

구문 설명

interface	인터페이스 이름을 지정합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 inside라는 인터페이스에 대한 IPsec 조각화 정책을 표시합니다.

```
ciscoasa(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ipsec fragmentation	IPsec 패킷에 대한 조각화 정책을 구성합니다.
crypto ipsec df-bit	IPsec 패킷에 대한 DF 비트 정책을 구성합니다.
show crypto ipsec df-bit	지정된 인터페이스에 대한 DF 비트 정책을 표시합니다.

show crypto ipsec policy

OSPFv3에서 제공된 IPsec SS API(보안 소켓 API) 보안 정책 정보를 표시하려면 글로벌 컨피그레이션 또는 특권 EXEC 모드에서 **show crypto ipsec policy** 명령을 사용합니다. 이 명령의 대체 형식인 **show ipsec policy**를 사용할 수도 있습니다.

show crypto ipsec policy [name]

구문 설명

name	정책 이름을 지정합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 CSSU-UTF라는 정책에 대한 암호화 보안 소켓 API에서 설치된 정책 정보를 표시합니다.

```
ciscoasa(config)# show crypto ipsec policy
Crypto IPsec client security policy data

       Policy name:      CSSU-UTF
       Policy refcount:  0
       Inbound  ESP SPI:        1031 (0x407)
       Outbound ESP SPI:        1031 (0x407)
       Inbound  ESP Auth Key:   0123456789abcdef
       Outbound ESP Auth Key:   0123456789abcdef
       Inbound  ESP Cipher Key:
       Outbound ESP Cipher Key:
       Transform set:    esp-sha-hmac
```

관련 명령

명령	설명
show crypto ipsec fragmentation	IPsec 패킷에 대한 조각화 정책을 표시합니다.
show crypto ipsec sa	IPsec SA 목록을 표시합니다.
show crypto ipsec df-bit	지정된 인터페이스에 대한 DF 비트 정책을 표시합니다.
show crypto sockets	암호화 보안 소켓 및 소켓 상태를 표시합니다.

show crypto ipsec sa

IPsec SA 목록을 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto ipsec sa** 명령을 사용합니다. 이 명령의 대체 형식인 **show ipsec sa**를 사용할 수도 있습니다.

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

구문 설명

detail	(선택 사항) 표시된 항목에 대한 자세한 오류 정보를 표시합니다.
entry	(선택 사항) 피어 주소별로 정렬된 IPsec SA를 표시합니다.
identity	(선택 사항) ESP를 포함하지 않고 ID별로 정렬된 IPsec SA를 표시합니다. 이는 축소된 형식입니다.
map *map-name*	(선택 사항) 지정된 암호화 맵에 대한 IPsec SA를 표시합니다.
peer *peer-addr*	(선택 사항) 지정된 피어 IP 주소에 대한 IPsec SA를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	OSPFv3, 다중 상황 모드, 변형 및 IV 크기 부분의 Suite B 알고리즘, ESPV3 IPsec 출력에 대한 지원이 추가되었습니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 OSPFv3으로 식별된 터널을 포함하는 IPsec SA를 표시합니다.

```
ciscoasa(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

참고 조각화 통계는 IPsec SA 정책에 IPsec 처리 전 조각화가 발생하도록 규정된 경우 사전 조각화 통계입니다. 사후 조각화 통계는 SA 정책에 IPsec 처리 후 조각화가 발생하도록 규정된 경우에 표시됩니다.

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 def라는 암호화 맵에 대한 IPsec SA를 표시합니다.

```
ciscoasa(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
```

```
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 480
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 480
        IV size: 8 bytes
        replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 4, crypto-map: def
        sa timing: remaining key lifetime (sec): 263
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 4, crypto-map: def
        sa timing: remaining key lifetime (sec): 263
        IV size: 8 bytes
        replay detection support: Y
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 키워드 **entry**에 대한 IPsec SA를 보여 줍니다.

```
ciscoasa(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 키워드 **entry detail**에 대한 IPsec SA를 보여줍니다.

```
ciscoasa(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
```

```
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

다음 예에서는 키워드 **identity**에 대한 IPsec SA를 보여 줍니다.

```
ciscoasa(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

다음 예에서는 키워드 **identity** 및 **detail**에 대한 IPsec SA를 보여 줍니다.

```
ciscoasa(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show crypto ipsec stats

IPsec 통계 목록을 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto ipsec stats** 명령을 사용합니다.

show crypto ipsec stats

구문 설명

이 명령에는 키워드 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 IPsec 통계를 표시합니다.

```
ciscoasa(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
```

```
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#
```

관련 명령

명령	설명
clear ipsec sa	지정된 파라미터를 기반으로 IPsec SA 또는 카운터를 지웁니다.
crypto ipsec transform-set	변형 집합을 정의합니다.
show ipsec sa	지정된 파라미터를 기반으로 IPsec SA를 표시합니다.
show ipsec sa summary	IPsec SA 요약을 표시합니다.

예

글로벌 컨피그레이션 모드에서 실행된 다음 예에서는 ISAKMP 통계를 표시합니다.

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
crypto isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show crypto isakmp sa

IKE 런타임 SA 데이터베이스를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto isakmp sa** 명령을 사용합니다.

show crypto isakmp sa [**detail**]

구문 설명

detail	SA 데이터베이스에 대한 자세한 출력을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	**show isakmp sa** 명령이 도입되었습니다.
7.2(1)	이 명령의 사용이 중단되었습니다. **show crypto isakmp sa** 명령이 이를 대체합니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

이 명령의 출력에는 다음 필드가 포함됩니다.

Detail이 지정되지 않은 경우

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail이 지정된 경우

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 SA 데이터베이스에 대한 자세한 정보를 표시합니다.

```
ciscoasa(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
crypto isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show crypto isakmp stats

런타임 통계를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto isakmp stats** 명령을 사용합니다.

show crypto isakmp stats

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	**show isakmp stats** 명령이 도입되었습니다.
7.2(1)	**show isakmp stats** 명령의 사용이 중단되었습니다. **show crypto isakmp stats** 명령이 이를 대체합니다.

사용 지침

이 명령의 출력에는 다음 필드가 포함됩니다.

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

예 글로벌 컨피그레이션 모드에서 실행된 다음 예에서는 ISAKMP 통계를 표시합니다.

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
crypto isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show crypto key mypubkey

ECDSA 키의 키 이름, 사용 현황 및 타원 곡선 크기를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto key mypubkey** 명령을 사용합니다.

show crypto key mypubkey dsa | rsa

구문 설명

dsa	키 이름을 지정합니다.
rsa	키 이름을 지정합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	**show crypto key mypubkey** 명령이 도입되었습니다.

show crypto protocol statistics

암호화 가속기 MIB의 프로토콜 관련 통계를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto protocol statistics** 명령을 사용합니다.

show crypto protocol statistics *protocol*

구문 설명

protocol	통계를 표시할 프로토콜의 이름을 지정합니다. 프로토콜 선택 항목은 다음과 같습니다. **ikev1** - 인터넷 키 교환국 버전 1 **ipsec** - IP 보안 Phase-2 프로토콜 **ssl** - Secure Sockets Layer **other** - 새 프로토콜용으로 예약됨 **all** - 현재 지원되는 모든 프로토콜

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 지정된 프로토콜에 대한 암호화 가속기 통계를 표시합니다.

```
ciscoasa # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
```

```
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0

ciscoasa # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

ciscoasa # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

ciscoasa # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

ciscoasa # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
```

```
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
ciscoasa #
```

관련 명령

명령	설명
clear crypto accelerator statistics	암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 지웁니다.
clear crypto protocol statistics	암호화 가속기 MIB에서 프로토콜 관련 통계를 지웁니다.
show crypto accelerator statistics	암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 표시합니다.

show crypto sockets

암호화 보안 소켓 정보를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show crypto sockets** 명령을 사용합니다.

show crypto sockets

구문 설명

이 명령에는 키워드 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 암호화 보안 소켓 정보를 표시합니다.

```
ciscoasa(config)# show crypto sockets

Number of Crypto Socket connections 1

       Gi0/1  Peers: (local): 2001:1::1
                     (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)

       Crypto Sockets in Listen state:
```

다음 표에는 **show crypto sockets** 명령 출력의 필드에 대한 설명이 나와 있습니다.

필드	설명
Number of Crypto Socket connections	시스템의 암호화 소켓 수입니다.
Socket State	이 상태는 활성 IPsec SA(Security Association: 보안 연계)가 존재하는 경우 Open이고, 활성 IPsec SA가 존재하지 않는 경우 Closed입니다.
Client	애플리케이션 이름과 해당 상태입니다.
Flags	이 필드에 “shared”가 표시된 경우 소켓이 둘 이상의 터널 인터페이스와 공유됩니다.
Crypto Sockets in Listen state	암호화 IPsec 프로파일의 이름입니다.

관련 명령

명령	설명
show crypto ipsec policy	암호화 보안 소켓 API에서 설치된 정책 정보를 표시합니다.

show csc node-count

CSC SSM에서 트래픽을 스캔한 노드 수를 표시하려면 특권 EXEC 모드에서 **show csc node-count** 명령을 사용합니다.

show csc node-count [**yesterday**]

구문 설명

yesterday	(선택 사항) CSC SSM에서 지난 24시간(자정부터 자정까지) 동안 트래픽을 스캔한 노드 수를 표시합니다.

기본값

기본적으로 표시되는 노드 수는 자정부터 스캔된 노드 수입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

노드는 고유한 소스 IP 주소이거나 ASA로 보호된 네트워크에 있는 디바이스의 주소입니다. ASA에서는 일일 노드 수를 추적하여 사용자 라이센스 적용을 위해 이 정보를 CSC SSM에 전달합니다.

예

다음은 CSC SSM에서 자정 이후 트래픽을 스캔한 노드 수를 표시하는 **show csc node-count** 명령의 샘플 출력입니다.

```
ciscoasa# show csc node-count
Current node count is 1
```

다음은 CSC SSM에서 지난 24시간(자정부터 자정까지) 동안 트래픽을 스캔한 노드 수를 표시하는 **show csc node-count** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show csc node-count yesterday
Yesterday's node count is 2
```

관련 명령

csc	CSC SSM에 구성된 대로 FTP, HTTP, POP3 및 SMTP의 스캐닝에 대해 CSC SSM에 네트워크 트래픽을 보냅니다.
show running-config class-map	현재 클래스 맵 구성을 보여 줍니다.
show running-config policy-map	현재 정책 맵 구성을 보여 줍니다.
show running-config service-policy	현재 서비스 정책 구성을 보여 줍니다.

show ctiqbe

ASA에 설정된 CTIQBE 세션에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show ctiqbe** 명령을 사용합니다.

show ctiqbe

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show ctiqbe 명령은 ASA에 설정된 CTIQBE 세션의 정보를 표시합니다. 이 명령은 **debug ctiqbe** 및 **show local-host**와 함께 CTIQBE 검사 엔진 문제를 해결하는 데 사용됩니다.

참고 **show ctiqbe** 명령을 사용하기 전에 **pager** 명령을 구성하는 것이 좋습니다. 많은 CTIQBE 세션이 있는 경우 **pager** 명령을 구성하지 않으면 **show ctiqbe** 명령 출력이 끝에 도달하는 데 약간의 시간이 걸릴 수 있습니다.

예

다음은 아래 조건에 따른 **show ctiqbe** 명령의 샘플 출력입니다. 하나의 활성 CTIQBE 세션만 ASA에 설정되어 있습니다. 이 세션은 로컬 주소 10.0.0.99의 내부 CTI 디바이스(예: Cisco IP SoftPhone)와 172.29.1.77의 외부 Cisco Call Manager(여기서는 TCP 포트 2748이 Cisco CallManager) 간에 설정되어 있습니다. 세션의 하트비트 간격은 120초입니다.

```
ciscoasa# | show ctiqbe

Total: 1
| LOCAL | FOREIGN | STATE | HEARTBEAT
-----------------------------------------------------------------
1 | 10.0.0.99/1117  172.29.1.77/2748 | 1 | 120
| RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 | 1029)
| MEDIA: Device ID 27 | Call ID 0
| Foreign 172.29.1.99 | (1028 | 1029)
| Local | 172.29.1.88 | (26822 | 26823)
| ---------------------------------------------
```

CTI 디바이스는 CallManager에 이미 등록되었습니다. 디바이스 내부 주소와 RTP 수신 대기 포트는 172.29.1.99 UDP 포트 1028로 PAT 변환됩니다. 해당 RTCP 수신 대기 포트는 UDP 1029로 PAT 변환됩니다.

`RTP/RTCP: PAT xlates:`로 시작하는 줄은 내부 CTI 디바이스가 외부 CallManager에 등록되고 CTI 디바이스 주소 및 포트가 해당 외부 인터페이스로 PAT 변환된 경우에만 표시됩니다. CallManager가 내부 인터페이스에 있거나, 내부 CTI 디바이스 주소 및 포트가 CallManager에서 사용하는 것과 동일한 외부 인터페이스로 NAT 변환된 경우에는 표시되지 않습니다.

출력은 이 CTI 디바이스와 172.29.1.88의 다른 디바이스 간에 통화가 설정되었음을 나타냅니다. 다른 전화의 RTP 및 RTCP 수신 대기 포트는 UDP 26822 및 26823입니다. ASA는 두 번째 전화 및 CallManager와 연계된 CTIQBE 세션 레코드를 유지하지 않기 때문에 다른 전화는 CallManager와 동일한 인터페이스에 있습니다. CTI 디바이스 쪽의 활성 통화 레그는 디바이스 ID 27 및 통화 ID 0으로 식별될 수 있습니다.

다음은 이러한 CTIBQE 연결에 대한 xlate 정보입니다.

```
ciscoasa# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
ciscoasa#
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
inspect ctiqbe	CTIQBE 애플리케이션 검사를 활성화합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.
show conn	여러 연결 유형에 대한 연결 상태를 표시합니다.
timeout	여러 프로토콜 및 세션 유형에 대한 최대 유휴 시간을 설정합니다.

show ctl-file

Phone Proxy에서 사용하는 CTL 파일의 내용을 표시하려면 글로벌 컨피그레이션 모드에서 **show ctl-file** 명령을 사용합니다.

show ctl-file *filename* [**parsed**]

구문 설명

filename	데이터베이스에 저장된 보안 모드를 지원하는 전화를 표시합니다.
parsed	(선택 사항) 지정된 CTL 파일에서 자세한 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

플래시 메모리에 저장된 CTL 파일의 파일 이름을 지정할 때는 디스크 번호, 파일 이름 및 내선 번호를 지정합니다(예: `disk0: /testctl.tlv`). **show ctl-file** 명령은 Phone Proxy 인스턴스를 구성할 때 디버깅하는 데 유용합니다.

예

다음 예에서는 **show ctl-file** 명령을 사용하여 CTL 파일에 대한 일반적인 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show ctl-file disk0:/ctlfile.tlv
Total Number of Records: 1
CTL Record Number 1
  Subject Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Issuer Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Function:
     cucm
  IP Address:
     192.168.52.102
  Associated Trustpoint:
     cucm_primary
```

다음 예에서는 **show ctl-file** 명령을 사용하여 CTL 파일에 대한 자세한 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show ctl-file disk0:/ctlfile.tlv parsed
TAG 0x01: Version: Maj 1, Min 2
TAG 0x02: Header Len: Len 288
TAG 0x03: Signer ID: Len 103
TAG 0x04: Signer Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x05: Cert SN: Len 4 SN: c43c9048
TAG 0x06: CA Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x07: Signature: Len 15
TAG 0x08: Digest Alg: Len 1 Name: SHA-1
TAG 0x09: Sig Alg Info: Len 8
TAG 0x0A: Sig Alg: Len 1 Name: RSA
TAG 0x0B: Modulus: Len 1 Name: 1024
TAG 0x0C: Sig Block: Len 128 Signature:
    521debcf b7a77ea8 94eba5f7 f3c8b0d8 3337a9fa 267ce1a7 202b2c8b 2ac980d3
    9608f64d e7cd82df e205e5bf 74a1d9c4 fae20f90 f3d2746a e90f439e ef93fca7
    d4925551 72daa414 2c55f249 ef7e6dc2 bcb9f9b5 39be8238 5011eecb ce37e4d1
    866e6550 6779c3fd 25c8bab0 6e9be32c 7f79fe34 5575e3af ea039145 45ce3158

TAG 0x0E: File Name: Len 12 Name: <CTLFile.tlv>
TAG 0x0F: Timestamp: Len 4 Timestamp: 48903cc6

 ### CTL RECORD No. 1 ###
TAG 0x01: Rcd Len: Len 731
TAG 0x03: Sub Name: Len 43 Sub Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x04: Function: Len 2 Func: CCM
TAG 0x05: Cert Issuer: Len 43 Issuer Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x06: Cert SN: Len 4 Cert SN: 15379048
TAG 0x07: Pub Key: Len 140 Pub Key:
    30818902 818100ad a752b4e6 89769a49 13115e52 1209b3ef 96a179af 728c29d7
    af7fed4e c759d0ea cebd7587 dd4f7c4c 322da86b 3a677c08 ce39ce60 2525f6d2
    50fe87cf 2aea60a5 690ec985 10706e5a 30ad26db e6fdb243 159758ed bb487525
    f901ef4a 658445de 29981546 3867d2d1 ce519ee4 62c7be32 51037c3c 751c0ad6
    040bedbb 3e984502 03010001
TAG 0x09: Cert: Len 469 X.509v3 Cert:
    308201d1 3082013a a0030201 02020415 37904830 0d06092a 864886f7 0d010104
    0500302d 312b3012 06035504 05130b4a 4d583132 31354c32 54583015 06092a86
    4886f70d 01090216 08636973 636f6173 61301e17 0d303830 37333030 39343033
    375a170d 31383037 32383039 34303337 5a302d31 2b301206 03550405 130b4a4d
    58313231 354c3254 58301506 092a8648 86f70d01 09021608 63697363 6f617361
    30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ada752
    b4e68976 9a491311 5e521209 b3ef96a1 79af728c 29d7af7f ed4ec759 d0eacebd
    7587dd4f 7c4c322d a86b3a67 7c08ce39 ce602525 f6d250fe 87cf2aea 60a5690e
    c9851070 6e5a30ad 26dbe6fd b2431597 58edbb48 7525f901 ef4a6584 45de2998
    15463867 d2d1ce51 9ee462c7 be325103 7c3c751c 0ad6040b edbb3e98 45020301
    0001300d 06092a86 4886f70d 01010405 00038181 005d82b7 ac45dbf8 bd911d4d
    a330454a a2784a4b 5ef898b1 482e0bbf 4a86ed86 9019820b 00e80361 fd7b2518
    9efa746c b98b1e23 fcc0793c de48de6d 6b1a4998 cd6f4e66 ba661d3a d200739a
    ae679c7c 94f550fb a6381b94 1eae389e a9ec4b11 30ba31f3 33cd184e 25647174
    ce00231d 102d5db3 c9c111a6 df37eb43 66f3d2d5 46
TAG 0x0A: IP Addr: Len 4 IP Addr: 192.168.52.102
```

관련 명령

명령	설명
ctl-file(전역)	Phone Proxy용으로 만들 CTL 인스턴스를 지정하거나, 플래시 메모리에 저장된 CTL 파일을 구문 분석합니다.
ctl-file(phone-proxy)	Phone Proxy를 구성할 때 사용할 CTL 인스턴스를 지정합니다.
phone proxy	Phone Proxy 인스턴스를 구성합니다.

show cts environment-data

Cisco TrustSec에 대한 ASA의 환경 데이터 새로 고침 작업 상태를 표시하려면 특권 EXEC 모드에서 **show cts environment-data** 명령을 사용합니다.

show cts environment-data

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 대체작동 컨피그레이션의 대기 디바이스에서는 지원되지 않습니다. 대기 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
ERROR: This command is only permitted on the active device.
```

이 명령은 클러스터링 컨피그레이션의 마스터 디바이스에서만 지원됩니다. 슬레이브 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
This command is only permitted on the master device.
```

예

다음은 **show cts environment-data** 명령의 샘플 출력입니다.

```
ciscoasa# show cts environment-data

CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 1200 secs
Last update time:          18:12:07 EST Feb 27 2012
Env-data expires in:       0:00:12:24 (dd:hr:mm:sec)
Env-data refreshes in:     0:00:02:24 (dd:hr:mm:sec)
```

관련 명령

명령	설명
show running-config cts	실행 중인 컨피그레이션에 대한 SXP 연결을 표시합니다.
show cts pac	PAC의 구성 요소를 표시합니다.

show cts environment-data sg-table

Cisco TrustSec에 대한 ASA의 상주 보안 그룹 테이블을 표시하려면 특권 EXEC 모드에서 **show cts environment-data sg-table** 명령을 사용합니다.

show cts environment-data sg-table

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 대체작동 컨피그레이션의 대기 디바이스에서는 지원되지 않습니다. 대기 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
ERROR: This command is only permitted on the active device.
```

이 명령은 클러스터링 컨피그레이션의 마스터 디바이스에서만 지원됩니다. 슬레이브 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
This command is only permitted on the master device.
```

예

다음은 **show cts environment-data sg-table** 명령의 샘플 출력입니다.

```
ciscoasa# show cts environment-data sg-table

Security Group Table:
Valid until: 18:32:07 EST Feb 27 2012
Showing 9 of 9 entries

SG Name                         SG Tag     Type
-------                         ------     -------------
ANY                              65535     unicast
ExampleSG1                           2     unicast
ExampleSG13                         14     unicast
ExampleSG14                         15     unicast
ExampleSG15                         16     unicast
```

```
ExampleSG16                          17     unicast
ExampleSG17                          18     unicast
ExampleSG18                          19     unicast
Unknown                               0     unicast
```

관련 명령

명령	설명
show running-config cts	실행 중인 컨피그레이션에 대한 SXP 연결을 표시합니다.
show cts pac	PAC의 구성 요소를 표시합니다.

show cts pac

Cisco TrustSec에 대한 ASA의 PAC(Protected Access Credential) 구성 요소를 표시하려면 특권 EXEC 모드에서 **show cts pac** 명령을 사용합니다.

show cts pac

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show cts pac 명령은 만료 시간을 비롯한 PAC 정보를 표시합니다. 만료 시간은 ASA에서 PAC 수명이 경과한 후 보안 그룹 테이블 업데이트를 검색할 수 없기 때문에 중요합니다. 관리자는 이전 PAC가 만료되기 전에 새 PAC를 요청하고 설치하여 ISE(Identity Services Engine)의 보안 그룹 테이블과 동기화 상태를 유지해야 합니다.

이 명령은 대체작동 컨피그레이션의 대기 디바이스에서는 지원되지 않습니다. 대기 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
ERROR: This command is only permitted on the active device.
```

이 명령은 클러스터링 컨피그레이션의 마스터 디바이스에서만 지원됩니다. 슬레이브 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
This command is only permitted on the master device.
```

예

다음은 **show cts pac** 명령의 샘플 출력입니다.

```
ciscoasa# show cts pac
PAC-Info:
    Valid until: Jul 28 2012 08:03:23
    AID:         6499578bc0240a3d8bd6591127ab270c
    I-ID:        BrianASA36
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
```

```
PAC-Opaque:
  000200b000030001000400106499578bc0240a3d8bd6591127ab270c00060094000301
  00d75a3f2293ff3b1310803b9967540ff7000000134e2d2deb00093a803d227383e2b9
  7db59ed2eeac4e469fcb1eeb0ac2dd84e76e13342a4c2f1081c06d493e192616d43611
  8ff93d2af9b9135bb95127e8b9989db36cf1667b4fe6c284e220c11e1f7dbab91721d1
  00e9f47231078288dab83a342ce176ed2410f1249780882a147cc087942f52238fc9b4
  09100e1758
```

관련 명령

명령	설명
show running-config cts	실행 중인 컨피그레이션에 대한 SXP 연결을 표시합니다.
show cts environment	환경 데이터 새로 고침 작업의 상태를 표시합니다.

show cts sgt-map

제어 경로의 IP 주소-보안 그룹 테이블 관리자 항목을 표시하려면 특권 EXEC 모드에서 **show cts sgt-map** 명령을 사용합니다.

show cts sgt-map [**sgt** *sgt*] [**address** *ipv4* | **address** *ipv6* [*/prefix*] | **ipv4** | **ipv6**] [**name**] [**brief** | **detail**]

구문 설명

address i*pv4*/*ipv6* /*prefix*	특정 IPv4 또는 IPv6 주소나 서브넷에 대한 IP 주소-보안 그룹 테이블 매핑만 표시합니다.
brief	IP 주소-보안 그룹 테이블 매핑 요약을 표시합니다.
detail	IP 주소-보안 그룹 테이블 매핑을 표시합니다.
ipv4	IPv4 주소-보안 그룹 테이블 매핑을 표시합니다. 기본적으로 IPv4 주소-보안 그룹 테이블 매핑만 표시됩니다.
ipv6	IPv6 주소-보안 그룹 테이블 매핑을 표시합니다.
name	보안 그룹 이름이 일치하는 IP 주소-보안 그룹 테이블 매핑을 표시합니다.
sgt *sgt*	보안 그룹 테이블이 일치하는 IP 주소-보안 그룹 테이블 매핑만 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.01)	이 명령이 도입되었습니다.
9.3(1)	**cts role-based sgt-map** 명령으로 채워지는 “CLI-HI” 소스의 IP-SGT 바인딩 정보를 포함하도록 출력이 업데이트되었습니다.

사용 지침

이 명령은 제어 경로의 IP 주소-보안 그룹 테이블 관리자 항목을 표시합니다.

예

다음은 **show cts sgt-map** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address    SGT Source
============================================
<IP address> <SGT value> <Source type>
```

```
IP-SGT Active Bindings Summary
==========================================
Total number of <Source type> bindings = <Total number of the entries from a source type>
Total number of active CONFIG bindings = <Total number of mapping entries>

ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address    SGT Source
==========================================
1.1.1.1       7 CLI-HI
10.10.10.1    7 CLI-HI
10.10.10.10   3 LOCAL
10.10.100.1   7 CLI-HI
198.26.208.31 7   SXP
IP-SGT Active Bindings Summary
==========================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

다음은 **show cts sgt-map ipv6** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sgt-map ipv6
Active IP-SGT Bindings Information

IP Address                                SGT     Source
============================================================
3330::1                                   17      SXP
FE80::A8BB:CCFF:FE00:110                  17      SXP

IP-SGT Active Bindings Summary
==========================================
Total number of SXP    bindings = 2
Total number of active   bindings = 2
```

다음은 **show cts sgt-map ipv6 detail** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sgt-map ipv6 detail
Active IP-SGT Bindings Information

IP Address                 Security Group                          Source
============================================================================
3330::1                     2345                                    SXP
1280::A8BB:CCFF:FE00:110    Security Tech Business Unit(12345)      SXP

IP-SGT Active Bindings Summary
==================================
Total number of SXP    bindings = 2
Total number of active bindings = 2
```

다음은 **show cts sgt-map ipv6 brief** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sgt-map ipv6 brief
Active IP-SGT Bindings Information

IP-SGT Active Bindings Summary
==================================
Total number of SXP    bindings = 2
Total number of active bindings = 2
```

다음은 **show cts sgt-map address** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sgt-map address 10.10.10.5 mask 255.255.255.255
```

```
Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================================
10.10.10.5              1234    SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 1
Total number of active   bindings = 1
```

관련 명령

명령	설명
show running-config cts	실행 중인 컨피그레이션에 대한 SXP 연결을 표시합니다.
show cts environment	환경 데이터 새로 고침 작업의 상태를 표시합니다.

show cts sxp connections

ASA의 SXP(Security eXchange Protocol) 연결을 표시하려면 특권 EXEC 모드에서 **show cts sxp connections** 명령을 사용합니다.

show cts sxp connections [**peer** *peer addr*] [**local** *local addr*] [**ipv4 | ipv6**] [**status** {**on | off | delete-hold-down | pending-on**}] [**mode** {**speaker | listener**}] [**brief**]

구문 설명

brief	(선택 사항) SXP 연결 요약을 표시합니다.
delete-hold-down	(선택 사항) TCP 연결이 ON 상태에서 종료되었습니다(TCP의 작동이 중지됨). 수신기 모드에서 구성된 ASA만 이 상태에 있을 수 있습니다.
ipv4	(선택 사항) IPv4 주소와의 SXP 연결을 표시합니다.
ipv6	(선택 사항) IPv6 주소와의 SXP 연결을 표시합니다.
listener	(선택 사항) 수신기 모드에서 구성된 ASA를 표시합니다.
local *local addr*	(선택 사항) 로컬 IP 주소가 일치하는 SXP 연결을 표시합니다.
mode	(선택 사항) 모드가 일치하는 SXP 연결을 표시합니다.
off	(선택 사항) TCP 연결이 시작되지 않았습니다. ASA는 이 상태에서만 TCP 연결을 다시 시도합니다.
on	(선택 사항) SXP OPEN 또는 SXP OPEN RESP 메시지가 수신되었습니다. SXP 연결이 성공적으로 설정되었습니다. ASA는 이 상태에서만 SXP 메시지를 교환합니다.
peer *peer addr*	(선택 사항) 피어 IP 주소가 일치하는 SXP 연결을 표시합니다.
pending-on	(선택 사항) SXP OPEN 메시지가 피어에 전송되었으며, 피어의 응답을 대기하는 중입니다.
speaker	(선택 사항) 스피커 모드에서 구성된 ASA를 표시합니다.
status	(선택 사항) 상태가 일치하는 SXP 연결을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

SXP 상태는 다음 조건에 따라 변경됩니다.

- 해당 피어가 SXP를 구성하지 않았거나 비활성화했기 때문에 SXP 수신기가 SXP 연결을 끊은 경우 SXP 수신기는 OFF 상태로 전환됩니다.
- 해당 피어가 충돌하거나 인터페이스를 종료했기 때문에 SXP 수신기가 SXP 연결을 끊은 경우 SXP 수신기는 DELETE_HOLD_DOWN 상태로 전환됩니다.
- SXP 스피커는 처음 두 조건 하나가 발생하는 경우 OFF 상태로 전환됩니다.

이 명령은 대체작동 컨피그레이션의 대기 디바이스에서는 지원되지 않습니다. 대기 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
ERROR: This command is only permitted on the active device.
```

이 명령은 클러스터링 컨피그레이션의 마스터 디바이스에서만 지원됩니다. 슬레이브 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
This command is only permitted on the master device.
```

예

다음은 **show cts sxp connections** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sxp connections
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local IP   : Not Set
Reconcile period   : 120 secs
Retry open period  : 10 secs
Retry open timer   : Not Running
Total number of SXP connections : 3
Total number of SXP connection shown : 3
----------------------------------------------
Peer IP            : 2.2.2.1
Local IP           : 2.2.2.2
Conn status        : On
Local mode         : Listener
Ins number         : 1
TCP conn password  : Default
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 3.3.3.1
Local IP           : 3.3.3.2
Conn status        : On
Local mode         : Listener
Ins number         : 2
TCP conn password  : None
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:01:02:20 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 4.4.4.1
Local IP           : 4.4.4.2
Conn status        : On
Local mode         : Speaker
Ins number         : 1
TCP conn password  : Set
Delete hold down timer : Not Running
Reconciliation timer   : Not Running
Duration since last state change: 0:03:01:20 (dd:hr:mm:sec)
```

관련 명령

명령	설명
show running-config cts	실행 중인 컨피그레이션에 대한 SXP 연결을 표시합니다.
show cts environment	환경 데이터 새로 고침 작업의 상태를 표시합니다.

show cts sxp sgt-map

Cisco TrustSec에 대한 ASA의 SXP(Security eXchange Protocol)에 있는 현재 IP 주소-보안 그룹 테이블 매핑 데이터베이스 항목을 표시하려면 특권 EXEC 모드에서 **show cts sxp sgt-map** 명령을 사용합니다.

show cts sxp sgt-map [**peer** *peer_addr*] [**sgt** *sgt*] [**address** *ipv4* | **address** *ipv6* [*/prefix*] | **ipv4** | **ipv6**] [**name**] [**brief** | **detail**] [**status**]

구문 설명

address i*pv4*/*ipv6* /*prefix*	특정 IPv4 또는 IPv6 주소나 서브넷에 대한 IP 주소-보안 그룹 테이블 매핑만 표시합니다.
brief	IP 주소-보안 그룹 테이블 매핑 요약을 표시합니다.
detail	보안 그룹 테이블 정보를 표시합니다. 보안 그룹 이름을 사용할 수 없는 경우 대괄호 없이 보안 그룹 테이블 값만 표시됩니다.
ipv4	IPv4 주소와의 IP 주소-보안 그룹 테이블 매핑을 표시합니다. 기본적으로 IPv4 주소와의 IP 주소-보안 그룹 테이블 매핑만 표시됩니다.
ipv6	IPv6 주소와의 IP 주소-보안 그룹 테이블 매핑을 표시합니다.
name	보안 그룹 이름이 일치하는 IP 주소-보안 그룹 테이블 매핑을 표시합니다.
peer *peer addr*	피어 IP 주소가 일치하는 IP 주소-보안 그룹 테이블 매핑만 표시합니다.
sgt *sgt*	보안 그룹 테이블이 일치하는 IP 주소-보안 그룹 테이블 매핑만 표시합니다.
status	활성 또는 비활성 매핑 항목을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.01)	이 명령이 도입되었습니다.

사용 지침

이 명령은 SXP에서 통합된 활성 IP 주소-보안 그룹 테이블 매핑 항목을 표시합니다.

이 명령은 대체작동 컨피그레이션의 대기 디바이스에서는 지원되지 않습니다. 대기 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
ERROR: This command is only permitted on the active device.
```

이 명령은 클러스터링 컨피그레이션의 마스터 디바이스에서만 지원됩니다. 슬레이브 디바이스에서 이 명령을 입력한 경우 다음 오류 메시지가 표시됩니다.

```
This command is only permitted on the master device.
```

예

다음은 **show cts sxp sgt-map** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sxp sgt-map
Total number of IP-SGT mappings : 3

SGT        : 7
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1

SGT        : 7
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1

SGT        : 7
IPv6       : FE80::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
```

다음은 **show cts sxp sgt-map detail** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sxp sgt-map detail
Total number of IP-SGT mappings : 3

SGT        : STBU(7)
IPv4       : 2.2.2.1
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active

SGT        : STBU(7)
IPv4       : 2.2.2.0
Peer IP    : 3.3.3.1
Ins Num    : 1
Status     : Inactive

SGT        : 6
IPv6       : 1234::A8BB:CCFF:FE00:110
Peer IP    : 2.2.2.1
Ins Num    : 1
Status     : Active
```

다음은 **show cts sxp sgt-map brief** 명령의 샘플 출력입니다.

```
ciscoasa# show cts sxp sgt-map brief
Total number of IP-SGT mappings : 3
SGT, IPv4: 7, 2.2.2.1
SGT, IPv4: 7, 3.3.3.0
SGT, IPv6: 7, FE80::A8BB:CCFF:FE00:110
```

관련 명령

명령	설명
show running-config cts	실행 중인 컨피그레이션에 대한 SXP 연결을 표시합니다.
show cts environment	환경 데이터 새로 고침 작업의 상태를 표시합니다.

show curpriv

현재 사용자 권한을 표시하려면 **show curpriv** 명령을 사용합니다.

show curpriv

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	—	—	• 예
특권 EXEC	• 예	• 예	—	—	• 예
사용자 EXEC	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	CLI 지침을 준수하기 위해 수정되었습니다.

사용 지침

show curpriv 명령은 현재 권한 수준을 표시합니다. 더 낮은 권한 수준 번호는 더 낮은 권한 수준을 나타냅니다.

예

다음 예에서는 enable_15라는 사용자에게 서로 다른 권한 수준이 있는 경우 **show curpriv** 명령의 출력을 보여 줍니다. username은 사용자가 로그인할 때 입력한 이름입니다. P_PRIV는 사용자가 **enable** 명령을 입력했음을 나타냅니다. P_CONF는 사용자가 **config terminal** 명령을 입력했음을 나타냅니다.

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit

ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa(config)# exit

ciscoasa(config)# show curpriv
Username : enable_1
```

```
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa(config)#
```

다음 예에서는 알려진 동작을 보여 줍니다. enable 모드일 때 disable 모드로 전환하면 초기에 로그인한 username이 enable_1로 바뀝니다.

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# exit

Logoff

Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa#
```

관련 명령

명령	설명
clear configure privilege	컨피그레이션에서 권한 명령문을 제거합니다.
show running-config privilege	명령에 대한 권한 수준을 표시합니다.

6 장

show ddns update interface through show environmentevent manager 명령

show ddns update interface

ASA 인터페이스에 할당된 DDNS 방법을 표시하려면 특권 EXEC 모드에서 **show ddns update interface** 명령을 사용합니다.

show ddns update interface [*interface-name*]

구문 설명

interface-name	(선택 사항) 네트워크 인터페이스의 이름입니다.

기본값

interface-name 문자열을 생략하면 각 인터페이스에 할당된 DDNS 방법이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예에서는 내부 인터페이스에 할당된 DDNS 방법을 표시합니다.

```
ciscoasa# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
ciscoasa#
```

관련 명령

명령	설명
ddns (DDNS-update-method mode)	생성된 DDNS 방법에 대한 DDNS 업데이트 방법 유형을 지정합니다.
ddns update (interface config mode)	ASA 인터페이스를 DDNS 업데이트 방법 또는 DDNS 업데이트 호스트 이름과 연계시킵니다.
ddns update method (global config mode)	DNS 리소스 레코드를 동적으로 업데이트하는 방법을 생성합니다.
show ddns update method	DDNS 업데이트를 수행할 DHCP 서버에 구성된 각 DDNS 방법에 대한 유형 및 간격을 표시합니다.
show running-config ddns	실행 중인 컨피그레이션에 구성된 모든 DDNS 방법의 유형 및 간격을 표시합니다.

show ddns update method

실행 중인 컨피그레이션의 DDNS 업데이트 방법을 표시하려면 특권 EXEC 모드에서 **show ddns update method** 명령을 사용합니다.

show ddns update method [*method-name*]

구문 설명

method-name	(선택 사항) 구성된 DDNS 업데이트 방법의 이름입니다.

기본값

method-name 문자열을 생략하면 구성된 모든 DDNS 업데이트 방법이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예에서는 ddns-2라는 DDNS 방법을 표시합니다.

```
ciscoasa(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
ciscoasa(config)#
```

관련 명령

명령	설명
ddns (DDNS-update-method mode)	생성된 DDNS 방법에 대한 DDNS 업데이트 방법 유형을 지정합니다.
ddns update (interface config mode)	ASA 인터페이스를 DDNS(동적 DNS) 업데이트 방법 또는 DDNS 업데이트 호스트 이름과 연계시킵니다.
ddns update method (global config mode)	DNS 리소스 레코드를 동적으로 업데이트하는 방법을 생성합니다.
show ddns update interface	구성된 각 DDNS 방법과 연계된 인터페이스를 표시합니다.
show running-config ddns	실행 중인 컨피그레이션에 구성된 모든 DDNS 방법의 유형 및 간격을 표시합니다.

show debug

현재 디버깅 컨피그레이션을 표시하려면 **show debug** 명령을 사용합니다.

show debug [*command* [*keywords*]]

구문 설명

command	(선택 사항) 현재 컨피그레이션을 확인할 **debug** 명령을 지정합니다.
keywords	(선택 사항) 각 *command*에 대해 *command*의 뒤에 오는 *keyword*는 연계된 **debug** 명령에서 지원하는 *keyword*와 동일합니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.0(2)	가능한 명령 값 목록에 **eigrp** 키워드가 추가되었습니다.
8.4(1)	가능한 명령 값 목록에 **route** 키워드가 추가되었습니다.
9.2(1)	가능한 명령 값 목록에 **event manager** 키워드가 추가되었습니다.

사용 지침

각 *command*에 대해 *command*의 뒤에 오는 *keyword*는 연계된 *debug* 명령에서 지원하는 *keyword*와 동일합니다. 지원되는 구문에 대한 자세한 내용은 연계된 **debug** 명령을 참고하십시오.

참고 각 *command*의 사용 가능성은 적용 가능한 **debug** 명령을 지원하는 명령 모드에 따라 다릅니다.

유효한 *command* 값은 다음과 같습니다.

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **cxsc**

- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- **event manager**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**

- **route**
- **rtsp**
- **sdi**
- **sequence**
- **sfr**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

예

show debug 명령을 사용하여 모든 디버깅 컨피그레이션, 특정 기능에 대한 디버깅 컨피그레이션 및 기능의 일부에 대한 디버깅 컨피그레이션을 볼 수 있습니다.

다음 명령은 인증, 계정 관리 및 플래시 메모리에 대한 디버깅을 활성화합니다.

```
ciscoasa# debug aaa authentication
debug aaa authentication enabled at level 1
ciscoasa# debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa# debug disk filesystem
debug disk filesystem enabled at level 1
ciscoasa# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
ciscoasa# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
ciscoasa# show debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa#
```

관련 명령

명령	설명
디버그	모든 **debug** 명령을 표시합니다.

show debug mmp

MMP 검사 모듈에 대한 현재 디버그 설정을 표시하려면 특권 EXEC 모드에서 **show debug mmp** 명령을 사용합니다.

show debug mmp

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.

예

다음 예에서는 **show debug mmp** 명령을 사용하여 MMP 검사 모듈에 대한 현재 디버그 설정을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show debug mmp
debug mmp  enabled at level 1
```

관련 명령

명령	설명
debug mmp	MMP 검사 이벤트를 표시합니다.
inspect mmp	MMP 검사 엔진을 구성합니다.

show dhcpd

DHCP 바인딩, 상태 및 통계 정보를 보려면 특권 EXEC 모드에서 **show dhcpd** 명령을 사용합니다.

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

구문 설명

binding	지정된 서버 IP 주소에 대한 바인딩 정보 및 연계된 클라이언트 하드웨어 주소와 임대 기간을 표시합니다.
IP_address	지정된 IP 주소에 대한 바인딩 정보를 표시합니다.
state	DHCP 서버의 상태(예: 현재 상황에서 활성화되어 있는지 여부 및 각 인터페이스에서 활성화되어 있는지 여부)를 표시합니다.
statistics	주소 풀, 바인딩, 만료된 바인딩, 잘못된 형식의 메시지, 보낸 메시지, 받은 메시지 등의 개수와 같은 통계 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show dhcpd binding 명령에 선택적 IP 주소를 포함하면 해당 IP 주소에 대한 바인딩만 표시됩니다.

또한 **show dhcpd binding | state | statistics** 명령을 글로벌 컨피그레이션 모드에서 사용할 수 있습니다.

예

다음은 **show dhcpd binding** 명령의 샘플 출력입니다.

```
ciscoasa# show dhcpd binding
IP Address Client-id       Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

다음은 **show dhcpd state** 명령의 샘플 출력입니다.

```
ciscoasa# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

다음은 **show dhcpd statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
clear dhcpd	DHCP 서버 바인딩 및 통계 카운터를 지웁니다.
dhcpd lease	클라이언트에 부여된 DHCP 정보에 대한 임대 기간을 정의합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

show dhcprelay state

DHCP 릴레이 에이전트의 상태를 보려면 특권 EXEC 또는 글로벌 컨피그레이션 모드에서 **show dhcprelay state** 명령을 사용합니다.

show dhcprelay state

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 현재 상황 및 각 인터페이스에 대한 DHCP 릴레이 에이전트 상태 정보를 표시합니다.

예

다음은 **show dhcprelay state** 명령의 샘플 출력입니다.

```
ciscoasa# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

관련 명령

명령	설명
show dhcpd	DHCP 서버 통계 및 상태 정보를 표시합니다.
show dhcprelay statistics	DHCP 릴레이 통계를 표시합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

show dhcprelay statistics

DHCP 릴레이 통계를 표시하려면 특권 EXEC 모드에서 **show dhcprelay statistics** 명령을 사용합니다.

show dhcprelay statistics

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show dhcprelay statistics 명령의 출력은 **clear dhcprelay statistics** 명령을 입력할 때까지 증분됩니다.

예

다음은 **show dhcprelay statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
ciscoasa#
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
clear dhcprelay statistics	DHCP 릴레이 에이전트 통계 카운터를 지웁니다.
debug dhcprelay	DHCP 릴레이 에이전트에 대한 디버그 정보를 표시합니다.
show dhcprelay state	DHCP 릴레이 에이전트의 상태를 표시합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

show disk

ASA 전용 플래시 메모리의 내용을 표시하려면 특권 EXEC 모드에서 **show disk** 명령을 사용합니다.

show disk[**0** | **1**] [**filesys** | **all**] **controller**

구문 설명

0	**1**	내부 플래시 메모리(0, 기본값) 또는 외부 플래시 메모리(1)를 지정합니다.
all	플래시 메모리의 내용 및 파일 시스템 정보를 표시합니다.
controller	플래시 컨트롤러 모델 번호를 지정합니다.
filesys	컴팩트 플래시 카드에 대한 정보를 표시합니다.

기본값

기본적으로 이 명령은 내부 플래시 메모리를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show disk** 명령의 샘플 출력입니다.

```
ciscoasa# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
```

```
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

다음은 **show disk filesys** 명령의 샘플 출력입니다.

```
ciscoasa# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

다음은 **show disk controller** 명령의 샘플 출력입니다.

```
ciscoasa# show disk:1 controller
Flash Model: TOSHIBA THNCF064MBA
```

관련 명령

명령	설명
dir	디렉토리 내용을 표시합니다.

show dns

모든 또는 지정된 FQDN(정규화된 도메인 이름) 호스트의 현재 확인된 DNS 주소를 표시하려면 특권 EXEC 모드에서 **show dns** 명령을 사용합니다.

show dns [**host** *fqdn_name*]

구문 설명

fqdn_name	(선택 사항) 선택한 호스트의 FQDN을 지정합니다.
host	(선택 사항) 지정된 호스트의 IP 주소를 나타냅니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show dns** 명령의 샘플 출력입니다.

```
ciscoasa# show dns
Name:   www.example1.com
  Address: 10.1.3.1                          TTL 00:03:01
  Address: 10.1.3.3                          TTL 00:00:36
  Address: 10.4.1.2                          TTL 00:01:01
Name: www.example2.com
  Address: 10.2.4.1                          TTL 00:25:13
  Address: 10.5.2.1                          TTL 00:25:01
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa          TTL 00:00:41
  Address: 10.10.10.2                        TTL 00:25:01
```

참고 FQDN 호스트가 아직 활성화되지 않은 경우에는 이 명령에서 아무 출력도 표시되지 않습니다.

다음은 **show dns host** 명령의 샘플 출력입니다.

```
ciscoasa# show dns host www.example.com
Name:   www.example.com
Address: 10.1.3.1 TTL 00:03:01
Address: 10.1.9.5 TTL 00:00:36
Address: 10.1.1.2 TTL 00:01:01
```

관련 명령

명령	설명
clear dns-hosts	DNS 캐시를 지웁니다.
dns domain-lookup	ASA에서 이름 조회를 수행할 수 있도록 합니다.
dns name-server	DNS 서버 주소를 구성합니다.

show dns-hosts

DNS 캐시를 표시하려면 특권 EXEC 모드에서 **show dns-hosts** 명령을 사용합니다. DNS 캐시에는 DNS 서버에서 동적으로 학습된 항목과 수동으로 입력한 이름 및 IP 주소가 포함됩니다.

show dns-hosts

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show dns-hosts** 명령의 샘플 출력입니다.

```
ciscoasa# show dns-hosts
Host                    Flags      Age Type   Address(es)
ns2.example.com         (temp, OK) 0    IP    10.102.255.44
ns1.example.com         (temp, OK) 0    IP    192.168.241.185
snowmass.example.com    (temp, OK) 0    IP    10.94.146.101
server.example.com      (temp, OK) 0    IP    10.94.146.80
```

관련 명령

명령	설명
clear dns-hosts	DNS 캐시를 지웁니다.
dns domain-lookup	ASA에서 이름 조회를 수행할 수 있도록 합니다.
dns name-server	DNS 서버 주소를 구성합니다.
dns retries	ASA가 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수를 지정합니다.
dns timeout	다음 DNS 서버를 시도하기 전에 대기할 시간을 지정합니다.

표 11에는 각 필드에 대한 설명이 나와 있습니다.

표 6-1 show dns-hosts 필드

필드	설명
Host	호스트 이름을 표시합니다.
Flags	다음의 조합으로 항목 상태를 표시합니다. • temp - DNS 서버에서 가져온 항목이므로 임시 항목입니다. ASA에서는 비활성 시간이 72시간을 경과하면 이 항목을 제거합니다. • perm - **name** 명령을 통해 추가된 항목이므로 영구 항목입니다. • OK - 유효한 항목입니다. • ?? - 의심스러운 항목이므로 재활성화해야 합니다. • EX - 만료된 항목입니다.
Age	이 항목을 마지막으로 참조한 이후에 경과한 시간을 표시합니다.
Type	DNS 레코드 유형을 표시합니다. 이 값은 항상 IP입니다.
Address(es)	IP 주소입니다.

관련 명령

명령	설명
clear dns-hosts	DNS 캐시를 지웁니다.
dns domain-lookup	ASA에서 이름 조회를 수행할 수 있도록 합니다.
dns name-server	DNS 서버 주소를 구성합니다.
dns retries	ASA가 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수를 지정합니다.
dns timeout	다음 DNS 서버를 시도하기 전에 대기할 시간을 지정합니다.

show dynamic-filter data

동적 데이터베이스가 마지막으로 다운로드된 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등 봇네트(Botnet) 트래픽 필터 동적 데이터베이스에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show dynamic-filter data** 명령을 사용합니다.

show dynamic-filter data

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

동적 데이터베이스 정보를 보려면 먼저 **dynamic-filter use-database** 및 **dynamic-filter updater-client enable** 명령으로 데이터베이스 사용 및 다운로드를 활성화합니다.

예

다음은 **show dynamic-filter data** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter data

Traffic filter is using downloaded database version '907'
Fetched at 18:00:16 UTC Jan 22 2009, size: 674381
Sample names from downloaded database:
  example.com, example.net, example.org,
cisco.example, cisco.invalid, bad.example.com
bad.example.net, bad.example.org, bad.cisco.example
bad.cisco.ivalid
Total entries in Dynamic Filter database:
  Dynamic data: 40909 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
  Dynamic data: 0 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
```

관련 명령

명령	설명
address	차단 목록 또는 허용 목록에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇네트 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇네트 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇네트 트래픽 필터 통계를 지웁니다.
dns domain-lookup	ASA에서 DNS 요청을 DNS 서버로 보내 지원되는 명령에 대한 이름 조회를 수행할 수 있도록 합니다.
dns server-group	ASA의 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 유보 목록(greylist)의 트래픽을 차단 목록의 트래픽으로 처리합니다.
dynamic-filter blacklist	봇네트 트래픽 필터 차단 목록을 수정합니다.
dynamic-filter database fetch	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter drop blacklist	차단 목록의 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않은 모든 트래픽 또는 트래픽의 클래스에 봇네트 트래픽 필터를 사용합니다.
dynamic-filter updater-client enable	동적 데이터베이스 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스 사용을 활성화합니다.
dynamic-filter whitelist	봇네트 트래픽 필터 허용 목록을 수정합니다.
inspect dns dynamic-filter-snoop	봇네트 트래픽 필터 스누핑을 통한 DNS 검사를 활성화합니다.
name	차단 목록 또는 허용 목록에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇네트 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등을 포함하여 동적 데이터베이스에 대한 정보를 표시합니다.
show dynamic-filter reports	상위 10개의 봇네트 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇네트 트래픽 필터로 모니터링된 연결 수 및 이러한 연결 중 허용 목록, 차단 목록 및 유보 목록과 일치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	서버 IP 주소, 다음에 ASA에서 서버에 연결할 시간, 마지막으로 설치된 데이터베이스 버전 등 업데이터 서버에 대한 정보를 표시합니다.
show running-config dynamic-filter	봇네트 트래픽 필터에서 실행 중인 컨피그레이션을 표시합니다.

show dynamic-filter dns-snoop

봇네트 트래픽 필터 DNS 스누핑 요약 또는 실제 IP 주소 및 이름을 표시하려면 특권 EXEC 모드에서 **show dynamic-filter dns-snoop** 명령을 사용합니다.

show dynamic-filter dns-snoop [**detail**]

구문 설명

detail	(선택 사항) DNS 응답에서 스누핑된 IP 주소 및 이름을 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

차단 목록의 일치하는 이름뿐 아니라 검사된 모든 DNS 데이터가 이 출력에 포함됩니다. 정적 항목의 DNS 데이터는 포함되지 않습니다.

DNS 스누핑 데이터를 지우려면 **clear dynamic-filter dns-snoop** 명령을 입력합니다.

예

다음은 **show dynamic-filter dns-snoop** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter dns-snoop

DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
```

다음은 **show dynamic-filter dns-snoop detail** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter dns-snoop detail

DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
DNS reverse Cache Information:
[10.67.22.34] flags=0x22, cat=2, unit=0 b:g:w=3:0:0, cookie=0xda148218
    [www3.example.com] cat=2, ttl=3
    [www.bad.example.com] cat=2, ttl=3
    [www.example.com] cat=2, ttl=3
[10.6.68.133] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda13ed60
    [cisco.example] cat=2, ttl=73
[10.166.226.25] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda608cb8
    [cisco.invalid] cat=2, ttl=2
```

관련 명령

명령	설명
address	차단 목록 또는 허용 목록에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇네트 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇네트 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇네트 트래픽 필터 통계를 지웁니다.
dns domain-lookup	ASA에서 DNS 요청을 DNS 서버로 보내 지원되는 명령에 대한 이름 조회를 수행할 수 있도록 합니다.
dns server-group	ASA의 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 유보 목록(greylist)의 트래픽을 차단 목록의 트래픽으로 처리합니다.
dynamic-filter blacklist	봇네트 트래픽 필터 차단 목록을 수정합니다.
dynamic-filter database fetch	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter drop blacklist	차단 목록의 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않은 모든 트래픽 또는 트래픽의 클래스에 봇네트 트래픽 필터를 사용합니다.
dynamic-filter updater-client enable	동적 데이터베이스 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스 사용을 활성화합니다.
dynamic-filter whitelist	봇네트 트래픽 필터 허용 목록을 수정합니다.
inspect dns dynamic-filter-snoop	봇네트 트래픽 필터 스누핑을 통한 DNS 검사를 활성화합니다.
name	차단 목록 또는 허용 목록에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇네트 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등을 포함하여 동적 데이터베이스에 대한 정보를 표시합니다.
show dynamic-filter reports	상위 10개의 봇네트 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇네트 트래픽 필터로 모니터링된 연결 수 및 이러한 연결 중 허용 목록, 차단 목록 및 유보 목록과 일치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	서버 IP 주소, 다음에 ASA에서 서버에 연결할 시간, 마지막으로 설치된 데이터베이스 버전 등 업데이터 서버에 대한 정보를 표시합니다.
show running-config dynamic-filter	봇네트 트래픽 필터에서 실행 중인 컨피그레이션을 표시합니다.

show dynamic-filter reports top

봇네트 트래픽 필터별로 분류된 상위 10개 악성코드 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성하려면 특권 EXEC 모드에서 **show dynamic-filter reports top** 명령을 사용합니다.

show dynamic-filter reports top [**malware-sites** | **malware-ports** | **infected-hosts**]

구문 설명

malware-ports	(선택 사항) 상위 10 개의 악성코드 포트에 대한 보고서를 표시합니다.
malware-sites	(선택 사항) 상위 10 개의 악성코드 사이트에 대한 보고서를 표시합니다.
infected-hosts	(선택 사항) 상위 10 개의 감염된 호스트에 대한 보고서를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.
8.2(2)	**botnet-sites** 및 **botnet-ports** 키워드가 **malware-sites** 및 **malware-ports** 로 변경되었습니다. 이제 악성코드 사이트 보고서에 끊어진 연결 수와 각 사이트의 위협 수준 및 범주가 포함됩니다. 마지막 지우기 타임스탬프가 추가되었습니다. 위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

이 보고서는 데이터의 스냅샷이며, 통계 수집이 시작된 이후의 상위 10개 항목과 일치하지 않을 수 있습니다.

보고서 데이터를 지우려면 **clear dynamic-filter reports top** 명령을 입력합니다.

예

다음은 **show dynamic-filter reports top malware-sites** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter reports top malware-sites
Site                                Connections logged dropped Threat Level Category
-------------------------------------------------------------------------------------
bad1.example.com (10.67.22.34)                  11      0          2       Botnet
bad2.example.com (209.165.200.225)               8      8          3       Virus
bad1.cisco.example(10.131.36.158)                6      6          3       Virus
bad2.cisco.example(209.165.201.1)                2      2          3       Trojan
horrible.example.net(10.232.224.2)               2      2          3       Botnet
nono.example.org(209.165.202.130)                1      1          3       Virus
```

```
Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

다음은 **show dynamic-filter reports top malware-ports** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter reports top malware-ports
Port                                        Connections logged
------------------------------------------------------------------------
tcp 1000                                                 617
tcp 2001                                                 472
tcp 23                                                    22
tcp 1001                                                  19
udp 2000                                                  17
udp 2001                                                  17
tcp 8080                                                   9
tcp 80                                                     3
tcp >8192                                                  2

Last clearing of the top ports report: at 13:41:06 UTC Jul 15 2009
```

다음은 **show dynamic-filter reports top infected-hosts** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter reports top infected-hosts
Host                                        Connections logged
------------------------------------------------------------------------
10.10.10.51(inside)                                     1190
10.12.10.10(inside)                                       10
10.10.11.10(inside)                                        5

Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009
```

관련 명령

명령	설명
address	차단 목록 또는 허용 목록에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇네트 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇네트 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇네트 트래픽 필터 통계를 지웁니다.
dns domain-lookup	ASA에서 DNS 요청을 DNS 서버로 보내 지원되는 명령에 대한 이름 조회를 수행할 수 있도록 합니다.
dns server-group	ASA의 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 유보 목록(greylist)의 트래픽을 차단 목록의 트래픽으로 처리합니다.
dynamic-filter blacklist	봇네트 트래픽 필터 차단 목록을 수정합니다.
dynamic-filter database fetch	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter drop blacklist	차단 목록의 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않은 모든 트래픽 또는 트래픽의 클래스에 봇네트 트래픽 필터를 사용합니다.
dynamic-filter updater-client enable	동적 데이터베이스 다운로드를 활성화합니다.

명령	설명
dynamic-filter use-database	동적 데이터베이스 사용을 활성화합니다.
dynamic-filter whitelist	봇네트 트래픽 필터 허용 목록을 수정합니다.
inspect dns dynamic-filter-snoop	봇네트 트래픽 필터 스누핑을 통한 DNS 검사를 활성화합니다.
name	차단 목록 또는 허용 목록에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇네트 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등을 포함하여 동적 데이터베이스에 대한 정보를 표시합니다.
show dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 요약을 표시하거나, **detail** 키워드를 사용하여 실제 IP 주소 및 이름을 표시합니다.
show dynamic-filter statistics	봇네트 트래픽 필터로 모니터링된 연결 수 및 이러한 연결 중 허용 목록, 차단 목록 및 유보 목록과 일치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	서버 IP 주소, 다음에 ASA에서 서버에 연결할 시간, 마지막으로 설치된 데이터베이스 버전 등 업데이터 서버에 대한 정보를 표시합니다.
show running-config dynamic-filter	봇네트 트래픽 필터에서 실행 중인 컨피그레이션을 표시합니다.

show dynamic-filter reports infected-hosts

봇네트 트래픽 필터별로 분류된 감염된 호스트에 대한 보고서를 생성하려면 특권 EXEC 모드에서 **show dynamic-filter reports infected-hosts** 명령을 사용합니다.

show dynamic-filter reports infected-hosts {**max-connections** | **latest-active** | **highest-threat** | **subnet** *ip_address netmask* | **all**}

구문 설명

all	버퍼된 모든 감염된 호스트 정보를 표시합니다. 여기에는 수천 개의 항목이 포함될 수 있습니다. CLI를 사용하는 대신 ASDM을 사용하여 PDF 파일을 생성할 수도 있습니다.
highest-threat	위협 수준이 가장 높은 악성코드 사이트와 연결된 호스트 20개를 표시합니다.
latest-active	가장 최근 활동이 있는 호스트 20개를 표시합니다. 각 호스트에 대해 방문한 악성코드 사이트 5개에 대한 자세한 정보가 표시됩니다.
max-connections	연결 횟수가 가장 많은 감염된 호스트 20개를 표시합니다.
subnet *ip_address netmask*	지정된 서브넷에 속한 최대 20개의 호스트를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(2)	이 명령이 도입되었습니다.

사용 지침

이러한 보고서에는 감염된 호스트, 방문한 악성코드 사이트 및 악성코드 포트 간의 상관 관계를 보여 주는 감염된 호스트에 대한 자세한 기록이 포함됩니다.

보고서 데이터를 지우려면 **clear dynamic-filter reports infected-hosts** 명령을 입력합니다.

예

다음은 **show dynamic-filter reports infected hosts all** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter reports infected-hosts all

Total 2 infected-hosts in buffer
Host (interface)                        Latest malicious conn time, filter action  Conn logged, dropped
=============================================================================================================
192.168.1.4 (internal)                  15:39:40 UTC Sep 17 2009, dropped                    3      3
Malware-sites connected to (not ordered)
Site                       Latest conn port, time, filter action   Conn logged, dropped Threat-level Category
-------------------------------------------------------------------------------------------------------------
10.73.210.27 (bad.example.com)     80, 15:39:31 UTC Sep 17 2009, dropped      2   2     very-high Malware
10.65.2.119 (bad2.example.com)     0, 15:39:40 UTC Sep 17 2009, dropped       1   1     very-high admin-added
=============================================================================================================
192.168.1.2 (internal)                  15:39:01 UTC Sep 17 2009, dropped                    5      5
Malware-sites connected to (not ordered)
Site                       Latest conn port, time, filter action   Conn logged, dropped Threat-level Category
-------------------------------------------------------------------------------------------------------------
10.131.36.158 (bad.example.com)    0, 15:37:46 UTC Sep 17 2009, dropped      1    1    very-high admin-added
10.65.2.119 (bad2.example.com)     0, 15:37:53 UTC Sep 17 2009, dropped      1    1   very-high  admin-added
20.73.210.27 (bad3.example.com)   80, 15:39:01 UTC Sep 17 2009, dropped      3    3   very-high  Malware
=============================================================================================================

Last clearing of the infected-hosts report: Never
```

관련 명령

명령	설명
address	차단 목록 또는 허용 목록에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇네트 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇네트 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇네트 트래픽 필터 통계를 지웁니다.
dns domain-lookup	ASA에서 DNS 요청을 DNS 서버로 보내 지원되는 명령에 대한 이름 조회를 수행할 수 있도록 합니다.
dns server-group	ASA의 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 유보 목록(greylist)의 트래픽을 차단 목록의 트래픽으로 처리합니다.
dynamic-filter blacklist	봇네트 트래픽 필터 차단 목록을 수정합니다.
dynamic-filter database fetch	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter drop blacklist	차단 목록의 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않은 모든 트래픽 또는 트래픽의 클래스에 봇네트 트래픽 필터를 사용합니다.
dynamic-filter updater-client enable	동적 데이터베이스 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스 사용을 활성화합니다.
dynamic-filter whitelist	봇네트 트래픽 필터 허용 목록을 수정합니다.

명령	설명
inspect dns dynamic-filter-snoop	봇네트 트래픽 필터 스누핑을 통한 DNS 검사를 활성화합니다.
name	차단 목록 또는 허용 목록에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇네트 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등을 포함하여 동적 데이터베이스에 대한 정보를 표시합니다.
show dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 요약을 표시하거나, **detail** 키워드를 사용하여 실제 IP 주소 및 이름을 표시합니다.
show dynamic-filter statistics	봇네트 트래픽 필터로 모니터링된 연결 수 및 이러한 연결 중 허용 목록, 차단 목록 및 유보 목록과 일치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	서버 IP 주소, 다음에 ASA에서 서버에 연결할 시간, 마지막으로 설치된 데이터베이스 버전 등 업데이터 서버에 대한 정보를 표시합니다.
show running-config dynamic-filter	봇네트 트래픽 필터에서 실행 중인 컨피그레이션을 표시합니다.

show dynamic-filter statistics

봇네트 트래픽 필터를 사용하여 허용 목록, 차단 목록 및 유보 목록 연결로 분류된 연결 수를 표시하려면 특권 EXEC 모드에서 **show dynamic-filter statistics** 명령을 사용합니다.

show dynamic-filter statistics [**interface** *name*] [**detail**]

구문 설명

detail	(선택 사항) 각 위협 수준에서 분류되거나 삭제된 패킷 수를 표시합니다.
interface *name*	(선택 사항) 특정 인터페이스에 대한 통계를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.
8.2(2)	각 위협 수준에서 분류되거나 삭제된 패킷 수를 표시하는 **detail** 키워드가 추가되었습니다. 위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

유보 목록에는 여러 도메인 이름과 연계된 주소가 포함되지만 이 모든 도메인 이름이 차단 목록에 있는 것은 아닙니다.

통계를 지우려면 **clear dynamic-filter statistics** 명령을 입력합니다.

예

다음은 **show dynamic-filter statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter statistics
Enabled on interface outside
 Total conns classified 11, ingress 11, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
 Total conns classified 1182, ingress 1182, egress 0
 Total whitelist classified 3, ingress 3, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

다음은 **show dynamic-filter statistics interface outside detail** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter statistics interface outside detail
Enabled on interface outside
 Total conns classified 2108, ingress 2108, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 1, dropped 1, ingress 0, egress 0
   Threat level 5 classified 1, dropped 1, ingress 0, egress 0
   Threat level 4 classified 0, dropped 0, ingress 0, egress 0
   ...
Total blacklist classified 30, dropped 20, ingress 11, egress 2
   Threat level 5 classified 6, dropped 6, ingress 4, egress 2
   Threat level 4 classified 5, dropped 5, ingress 5, egress 0
```

관련 명령

명령	설명
address	차단 목록 또는 허용 목록에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇네트 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇네트 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇네트 트래픽 필터 통계를 지웁니다.
dns domain-lookup	ASA에서 DNS 요청을 DNS 서버로 보내 지원되는 명령에 대한 이름 조회를 수행할 수 있도록 합니다.
dns server-group	ASA의 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 유보 목록(greylist)의 트래픽을 차단 목록의 트래픽으로 처리합니다.
dynamic-filter blacklist	봇네트 트래픽 필터 차단 목록을 수정합니다.
dynamic-filter database fetch	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter drop blacklist	차단 목록의 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않은 모든 트래픽 또는 트래픽의 클래스에 봇네트 트래픽 필터를 사용합니다.
dynamic-filter updater-client enable	동적 데이터베이스 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스 사용을 활성화합니다.
dynamic-filter whitelist	봇네트 트래픽 필터 허용 목록을 수정합니다.
inspect dns dynamic-filter-snoop	봇네트 트래픽 필터 스누핑을 통한 DNS 검사를 활성화합니다.
name	차단 목록 또는 허용 목록에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇네트 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등을 포함하여 동적 데이터베이스에 대한 정보를 표시합니다.
show dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 요약을 표시하거나, **detail** 키워드를 사용하여 실제 IP 주소 및 이름을 표시합니다.

명령	설명
show dynamic-filter reports	상위 10개의 봇네트 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter updater-client	서버 IP 주소, 다음에 ASA에서 서버에 연결할 시간, 마지막으로 설치된 데이터베이스 버전 등 업데이터 서버에 대한 정보를 표시합니다.
show running-config dynamic-filter	봇네트 트래픽 필터에서 실행 중인 컨피그레이션을 표시합니다.

show dynamic-filter updater-client

서버 IP 주소, 다음에 ASA에서 서버에 연결할 시간, 마지막으로 설치된 데이터베이스 버전 등 봇넷 트래픽 필터 업데이터 서버에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show dynamic-filter updater-client** 명령을 사용합니다.

show dynamic-filter updater-client

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

예

다음은 **show dynamic-filter updater-client** 명령의 샘플 출력입니다.

```
ciscoasa# show dynamic-filter updater-client

Traffic Filter updater client is enabled
Updater server url is https://10.15.80.240:446
Application name: trafmon, version: 1.0
Encrypted UDI:
0bb93985f42d941e50dc8f022350d1a8de96ba6c1f6d45f4bc0ead02a7d5990be32f483b
5715cd80a215cedadd4e5ffe
Next update is in 00:02:00
Database file version is '907' fetched at 22:51:41 UTC Oct 16 2006,
size: 521408
```

관련 명령

명령	설명
address	차단 목록 또는 허용 목록에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇넷 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇넷 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇넷 트래픽 필터 통계를 지웁니다.

명령	설명
dns domain-lookup	ASA에서 DNS 요청을 DNS 서버로 보내 지원되는 명령에 대한 이름 조회를 수행할 수 있도록 합니다.
dns server-group	ASA의 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 유보 목록(greylist)의 트래픽을 차단 목록의 트래픽으로 처리합니다.
dynamic-filter blacklist	봇네트 트래픽 필터 차단 목록을 수정합니다.
dynamic-filter database fetch	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇네트 트래픽 필터 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter drop blacklist	차단 목록의 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않은 모든 트래픽 또는 트래픽의 클래스에 봇네트 트래픽 필터를 사용합니다.
dynamic-filter updater-client enable	동적 데이터베이스 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스 사용을 활성화합니다.
dynamic-filter whitelist	봇네트 트래픽 필터 허용 목록을 수정합니다.
inspect dns dynamic-filter-snoop	봇네트 트래픽 필터 스누핑을 통한 DNS 검사를 활성화합니다.
name	차단 목록 또는 허용 목록에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇네트 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시간, 데이터베이스 버전, 데이터베이스에 포함된 항목 수, 샘플 항목 10개 등을 포함하여 동적 데이터베이스에 대한 정보를 표시합니다.
show dynamic-filter dns-snoop	봇네트 트래픽 필터 DNS 스누핑 요약을 표시하거나, **detail** 키워드를 사용하여 실제 IP 주소 및 이름을 표시합니다.
show dynamic-filter reports	상위 10개의 봇네트 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇네트 트래픽 필터로 모니터링된 연결 수 및 이러한 연결 중 허용 목록, 차단 목록 및 유보 목록과 일치하는 연결 수를 표시합니다.
show running-config dynamic-filter	봇네트 트래픽 필터에서 실행 중인 컨피그레이션을 표시합니다.

show eigrp events

EIGRP 이벤트 로그를 표시하려면 특권 EXEC 모드에서 **show eigrp events** 명령을 사용합니다.

show eigrp [*as-number*] **events** [{*start end*} | **type**]

구문 설명

as-number	(선택 사항) 이벤트 로그를 확인할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. ASA는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
end	(선택 사항) *start* 인덱스 번호로 시작하고 *end* 인덱스 번호로 끝나는 항목으로 출력을 제한합니다.
start	(선택 사항) 로그 항목 인덱스 번호를 지정하는 숫자입니다. 시작 번호를 지정하면 출력이 지정된 이벤트에서 시작하고 *end* 인수로 지정된 이벤트에서 끝납니다. 유효한 값은 1~4294967295입니다.
type	(선택 사항) 기록할 이벤트를 표시합니다.

기본값

start 및 *end*를 지정하지 않으면 모든 로그 항목이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

show eigrp events 출력에는 최대 500개의 이벤트가 표시됩니다. 최대 이벤트 수에 도달하면 출력 맨 아래에 새 이벤트가 추가되고 출력 맨 위에서 이전 이벤트가 제거됩니다.

clear eigrp events 명령을 사용하여 EIGRP 이벤트 로그를 지울 수 있습니다.

show eigrp events type 명령은 EIGRP 이벤트 기록 상태를 표시합니다. 기본적으로 네이버 변경, 네이버 경고 및 DUAL FSM 메시지가 기록됩니다. **no eigrp log-neighbor-changes** 명령을 사용하여 네이버 변경 이벤트 기록을 비활성화할 수 있습니다. **no eigrp log-neighbor-warnings** 명령을 사용하여 네이버 경고 이벤트 기록을 비활성화할 수 있습니다. DUAL FSM 이벤트 기록은 비활성화할 수 없습니다.

예

다음은 **show eigrp events** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

다음은 시작 및 중지 번호가 지정된 **show eigrp events** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

다음은 EIGRP 이벤트 로그에 항목이 없는 경우 **show eigrp events** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp events

Event information for AS 100:  Event log is empty.
```

다음은 **show eigrp events type** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

관련 명령

명령	설명
clear eigrp events	EIGRP 이벤트 기록 버퍼를 지웁니다.
eigrp log-neighbor-changes	네이버 변경 이벤트 기록을 활성화합니다.
eigrp log-neighbor-warnings	네이버 경고 이벤트 기록을 활성화합니다.

show eigrp interfaces

EIGRP 라우팅에 참여한 인터페이스를 표시하려면 특권 EXEC 모드에서 **show eigrp interfaces** 명령을 사용합니다.

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

구문 설명

as-number	(선택 사항) 활성 인터페이스를 표시할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. ASA는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
detail	(선택 사항) 자세한 정보를 표시합니다.
if-name	(선택 사항) **nameif** 명령을 통해 지정된 인터페이스 이름입니다. 인터페이스 이름을 지정하면 지정된 인터페이스에 대한 정보만 표시됩니다.

기본값

인터페이스 이름을 지정하지 않으면 모든 EIGRP 인터페이스에 대한 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

show eigrp interfaces 명령을 사용하여 EIGRP가 활성화된 인터페이스를 확인하고 해당 인터페이스와 관련된 EIGRP에 대한 정보를 파악할 수 있습니다.

인터페이스를 지정한 경우 해당 인터페이스만 표시됩니다. 그렇지 않으면 EIGRP가 실행 중인 모든 인터페이스가 표시됩니다.

자동 시스템을 지정한 경우 지정된 자동 시스템에 대한 라우팅 프로세스만 표시됩니다. 그렇지 않으면 모든 EIGRP 프로세스가 표시됩니다.

예

다음은 **show eigrp interfaces** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface    Peers  Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
mgmt           0        0/0          0      11/434          0          0
outside        1        0/0        337       0/10           0          0
inside         1        0/0         10       1/63         103          0
```

표 6-2에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 6-2 show eigrp interfaces 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Peers	직접 연결된 피어 수입니다.
Xmit Queue Un/Reliable	Unreliable 및 Reliable 전송 대기열에 남아 있는 패킷 수입니다.
Mean SRTT	원활한 평균 왕복 시간 간격(초)입니다.
Pacing Time Un/Reliable	EIGRP 패킷을 인터페이스 외부로 전송해야 하는 경우(신뢰할 수 없는 패킷 및 신뢰할 수 있는 패킷)를 결정하는 데 사용되는 페이싱 시간(초)입니다.
Multicast Flow Timer	ASA에서 멀티캐스트 EIGRP 패킷을 전송할 최대 시간(초)입니다.
Pending Routes	전송 대기열에서 전송을 대기 중인 패킷의 경로 수입니다.

관련 명령

명령	설명
network	EIGRP 라우팅 프로세스에 참여하는 네트워크 및 인터페이스를 정의합니다.

show eigrp neighbors

EIGRP 네이버 테이블을 표시하려면 특권 EXEC 모드에서 **show eigrp neighbors** 명령을 사용합니다.

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

구문 설명

as-number	(선택 사항) 네이버 항목을 삭제할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. ASA는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
detail	(선택 사항) 자세한 네이버 정보를 표시합니다.
if-name	(선택 사항) **nameif** 명령을 통해 지정된 인터페이스 이름입니다. 인터페이스 이름을 지정하면 해당 인터페이스를 통해 학습된 모든 네이버 테이블 항목이 표시됩니다.
static	(선택 사항) **neighbor** 명령을 정적으로 정의된 EIGRP 네이버를 표시합니다.

기본값

인터페이스 이름을 지정하지 않으면 모든 인터페이스를 통해 학습된 네이버가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

clear eigrp neighbors 명령을 사용하여 EIGRP 네이버 테이블에서 동적으로 학습된 네이버를 지울 수 있습니다.

static 키워드를 사용하지 않는 한 정적 네이버는 출력에 포함되지 않습니다.

예

다음은 **show eigrp neighbors** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100
Address                 Interface       Holdtime Uptime   Q      Seq  SRTT  RTO
                                        (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1       13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0       14       0:02:01  0      10   12    24
172.16.80.31            Ethernet0       12       0:02:02  0      4    5     20
```

표 6-2에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 6-3 show eigrp neighbors 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Address	EIGRP 네이버의 IP 주소입니다.
Interface	ASA가 네이버에서 hello 패킷을 수신하는 인터페이스입니다.
Holdtime	ASA에서 작동 중지된 것으로 선언하기 전에 네이버를 수신 대기할 시간(초)입니다. 이 보류 시간은 hello 패킷을 통해 네이버에서 수신되며, 네이버에서 다른 hello 패킷이 수신될 때까지는 감소됩니다. 네이버에서 기본 보류 시간을 사용하는 경우 이 숫자는 15보다 작습니다. 피어가 기본이 아닌 보류 시간을 구성하는 경우에는 기본이 아닌 보류 시간이 표시됩니다. 이 값이 0에 도달한 경우 ASA는 해당 네이버를 연결할 수 없는 것으로 간주합니다.
Uptime	ASA가 이 네이버에서 처음 수신한 이후에 경과한 시간(시간:분:초)입니다.
Q Count	ASA가 전송 대기 중인 EIGRP 패킷(업데이트, 쿼리 및 응답) 수입니다.
Seq Num	네이버에서 마지막으로 수신된 업데이트, 쿼리 또는 응답 패킷의 시퀀스 번호입니다.
SRTT	평균 왕복 시간입니다. EIGRP 패킷을 이 네이버로 전송하고 ASA가 해당 패킷에 대한 확인 응답을 받는 데 소요되는 시간(초)입니다.
RTO	재전송 시간 제한(밀리초)입니다. ASA가 재전송 대기열에서 네이버로 패킷을 다시 전송하기 전에 대기할 시간입니다.

다음은 **show eigrp neighbors static** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                  Interface
192.168.1.5                     management
```

표 6-4에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 6-4 show ip eigrp neighbors static 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Static Address	EIGRP 네이버의 IP 주소입니다.
Interface	ASA가 네이버에서 hello 패킷을 수신하는 인터페이스입니다.

다음은 **show eigrp neighbors detail** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

표 6-5에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 6-5 show ip eigrp neighbors details 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
H	이 열에는 지정된 네이버와의 피어링 세션이 설정된 순서가 나열됩니다. 이 순서는 0에서 시작하는 순차적 번호 매기기로 지정됩니다.
Address	EIGRP 네이버의 IP 주소입니다.
Interface	ASA가 네이버에서 hello 패킷을 수신하는 인터페이스입니다.
Holdtime	ASA에서 작동 중지된 것으로 선언하기 전에 네이버를 수신 대기할 시간 시간(초)입니다. 이 보류 시간은 hello 패킷을 통해 네이버에서 수신되며, 네이버에서 다른 hello 패킷이 수신될 때까지는 감소됩니다. 네이버에서 기본 보류 시간을 사용하는 경우 이 숫자는 15보다 작습니다. 피어가 기본이 아닌 보류 시간을 구성하는 경우에는 기본이 아닌 보류 시간이 표시됩니다. 이 값이 0에 도달한 경우 ASA는 해당 네이버를 연결할 수 없는 것으로 간주합니다.
Uptime	ASA가 이 네이버에서 처음 수신한 이후에 경과한 시간(시간:분:초)입니다.
SRTT	평균 왕복 시간입니다. EIGRP 패킷을 이 네이버로 전송하고 ASA가 해당 패킷에 대한 확인 응답을 받는 데 소요되는 시간(초)입니다.
RTO	재전송 시간 제한(밀리초)입니다. ASA가 재전송 대기열에서 네이버로 패킷을 다시 전송하기 전에 대기할 시간입니다.

표 6-5 show ip eigrp neighbors details 필드 설명

필드	설명
Q Count	ASA가 전송 대기 중인 EIGRP 패킷(업데이트, 쿼리 및 응답) 수입니다.
Seq Num	네이버에서 마지막으로 수신된 업데이트, 쿼리 또는 응답 패킷의 시퀀스 번호입니다.
Version	지정된 피어에서 실행 중인 소프트웨어 버전입니다.
Retrans	패킷이 재전송된 횟수입니다.
Retries	패킷 재전송을 시도한 횟수입니다.
Restart time	지정된 네이버가 재시작된 이후에 경과한 시간(시간:분:초)입니다.

관련 명령

명령	설명
clear eigrp neighbors	EIGRP 네이버 테이블을 지웁니다.
debug eigrp neighbors	EIGRP 네이버 디버깅 메시지를 표시합니다.
debug ip eigrp	EIGRP 패킷 디버깅 메시지를 표시합니다.

show eigrp topology

EIGRP 토폴로지 테이블을 표시하려면 특권 EXEC 모드에서 **show eigrp topology** 명령을 사용합니다.

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

구문 설명

active	(선택 사항) EIGRP 토폴로지 테이블의 활성 항목만 표시합니다.
all-links	(선택 사항) 실행 가능한 successor가 아닌 경로를 포함하여 EIGRP 토폴로지 테이블의 모든 경로를 표시합니다.
as-number	(선택 사항) EIGRP 프로세스의 자동 시스템 번호를 지정합니다. ASA는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
ip-addr	(선택 사항) 표시할 토폴로지 테이블의 IP 주소를 정의합니다. 마스크와 함께 지정하면 항목에 대한 자세한 설명이 제공됩니다.
mask	(선택 사항) *ip-addr* 인수에 적용할 네트워크 마스크를 정의합니다.
pending	(선택 사항) EIGRP 토폴로지 테이블에서 네이버로부터의 업데이트를 대기 중이거나 네이버에 응답하기를 대기 중인 모든 항목을 표시합니다.
summary	(선택 사항) EIGRP 토폴로지 테이블에 대한 요약을 표시합니다.
zero-successors	(선택 사항) EIGRP 토폴로지 테이블에서 사용 가능한 경로를 표시합니다.

기본값

실행 가능한 successor 경로만 표시됩니다. 실행 가능한 successor가 아닌 경로를 포함하여 모든 경로를 표시하려면 **all-links** 키워드를 사용합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

clear eigrp topology 명령을 사용하여 토폴로지 테이블에서 동적 항목을 제거할 수 있습니다.

예

다음은 **show eigrp topology** 명령의 샘플 출력입니다.

명령 기록

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

표 6-6에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 6-6 show eigrp topology 필드 정보

필드	설명
Codes	이 토폴로지 테이블 항목의 상태입니다. Passive와 Active는 이 대상에 대한 EIGRP 상태를 나타내고, Update, Query 및 Reply는 전송할 패킷의 유형을 나타냅니다.
P - Passive	경로가 정상으로 알려져 있으므로 이 대상에 대한 EIGRP 계산은 수행되지 않습니다.
A - Active	이 대상에 대한 EIGRP 계산이 수행됩니다.
U - Update	이 대상으로 업데이트 패킷이 전송되었음을 나타냅니다.
Q - Query	이 대상으로 쿼리 패킷이 전송되었음을 나타냅니다.
R - Reply	이 대상으로 응답 패킷이 전송되었음을 나타냅니다.
r - Reply status	소프트웨어가 쿼리를 전송하고 응답을 대기 중인 후에 설정되는 플래그입니다.
address mask	대상 IP 주소와 마스크입니다.
successors	successor 수입니다. 이 수는 IP 라우팅 테이블에 있는 다음 홉 수에 해당합니다. "successor"가 대문자로 표시된 경우에는 경로 또는 다음 홉이 전환 상태에 있습니다.
FD	실행 가능한 거리입니다. 실행 가능한 거리는 대상에 도달할 수 있는 최상의 메트릭 또는 경로가 활성 상태가 된 경우에 알려진 최상의 메트릭입니다. 이 값은 실행 가능성 조건 확인에 사용됩니다. 라우터의 보고된 거리(뒤에 슬래시가 있는 메트릭)가 실행 가능한 거리보다 짧은 경우 실행 가능성 조건이 충족되고 해당 경로가 실행 가능한 successor가 됩니다. 소프트웨어에서 실행 가능한 successor가 있는 것으로 확인한 후에는 해당 대상에 대한 쿼리를 보내도록 요구하지 않습니다.
via	소프트웨어에 이 대상에 대해 알려 준 피어의 IP 주소입니다. 이러한 항목의 첫 번째 *n*은 현재 successor입니다(여기서 *n*은 successor 수). 목록의 나머지 항목은 실행 가능한 successor입니다.
(*cost*/*adv_cost*)	첫 번째 숫자는 대상에 대한 비용을 나타내는 EIGRP 메트릭입니다. 두 번째 숫자는 이 피어에서 알려 준 EIGRP 메트릭입니다.
interface	정보가 학습된 인터페이스입니다.

다음은 IP 주소와 함께 사용된 **show eigrp topology** 명령의 샘플 출력입니다. 표시된 출력은 내부 경로에 대한 것입니다.

```
ciscoasa# show eigrp topology 10.2.1.0 255.255.255.0

EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

다음은 IP 주소와 함께 사용된 **show eigrp topology** 명령의 샘플 출력입니다. 표시된 출력은 외부 경로에 대한 것입니다.

```
ciscoasa# show eigrp topology 10.4.80.0 255.255.255.0


EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

관련 명령

명령	설명
clear eigrp topology	EIGRP 토폴로지 테이블에서 동적으로 검색된 항목을 지웁니다.

show eigrp traffic

전송 및 수신된 EIGRP 패킷 수를 표시하려면 특권 EXEC 모드에서 **show eigrp traffic** 명령을 사용합니다.

show eigrp [*as-number*] **traffic**

구문 설명

as-number	(선택 사항) 이벤트 로그를 확인할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. ASA는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

clear eigrp traffic 명령을 사용하여 EIGRP 트래픽 통계를 지울 수 있습니다.

예

다음은 **show eigrp traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

표 6-4에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 6-7 show eigrp traffic 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Hellos sent/received	전송 및 수신된 hello 패킷 수입니다.
Updates sent/received	전송 및 수신된 업데이트 패킷 수입니다.
Queries sent/received	전송 및 수신된 쿼리 패킷 수입니다.
Replies sent/received	전송 및 수신된 응답 패킷 수입니다.
Acks sent/received	전송 및 수신된 확인 응답 패킷 수입니다.
Input queue high water mark/drops	최대 수신 임계값에 근접한 수신된 패킷 수 및 삭제된 패킷 수입니다.
SIA-Queries sent/received	전송 및 수신된 SIA(Stuck-In-Active) 쿼리입니다.
SIA-Replies sent/received	전송 및 수신된 SIA(Stuck-In-Active) 응답입니다.

관련 명령

명령	설명
debug eigrp packets	전송 및 수신된 EIGRP 패킷에 대한 디버깅 정보를 표시합니다.
debug eigrp transmit	전송된 EIGRP 메시지에 대한 디버깅 정보를 표시합니다.

show environment

시스템 구성 요소에 대한 시스템 환경 정보를 표시하려면 특권 EXEC 모드에서 **show environment** 명령을 사용합니다.

show environment [**driver** | **fans** | **power-supply** | **temperature**] [**chassis** | **cpu** | **voltage**]

구문 설명

chassis	(선택 사항) 온도 표시를 섀시로 제한합니다.
cpu	(선택 사항) 온도 표시를 프로세서로 제한합니다. ASA 5580-40은 4개의 프로세서에 대한 정보를 표시합니다. ASA 5580-20은 2개의 프로세서에 대한 정보를 표시합니다.
driver	(선택 사항) 환경 모니터링 IPMI 드라이버 상태를 표시합니다. 드라이버 상태는 다음 중 하나일 수 있습니다. • RUNNING - 드라이버가 작동 중입니다. • STOPPED - 오류가 발생하여 드라이버가 중지되었습니다.
fans	(선택 사항) 냉각 팬의 작동 상태를 표시합니다. 상태는 다음 중 하나입니다. • OK - 팬이 정상적으로 작동하고 있습니다. • Failed - 장애가 발생하여 팬을 교체해야 합니다.
power-supply	(선택 사항) 전원 공급 디바이스의 작동 상태를 표시합니다. 각 전원 공급 디바이스의 상태는 다음 중 하나입니다. • OK - 전원 공급 디바이스가 정상적으로 작동하고 있습니다. • Failed - 장애가 발생하여 전원 공급 디바이스를 교체해야 합니다. • Not Present - 지정된 전원 공급 디바이스가 설치되어 있지 않습니다. 전원 공급 디바이스 이중화 상태도 표시됩니다. 이중화 상태는 다음 중 하나입니다. • OK - 디바이스가 완전한 리소스로 정상적으로 작동하고 있습니다. • Lost - 디바이스에서 이중화가 손실되었지만 최소 리소스로 정상적으로 작동하고 있습니다. 추가 장애 시 시스템이 종료됩니다. • N/A - 디바이스에 전원 공급 디바이스 이중화가 구성되어 있지 않습니다.
temperature	(선택 사항) 프로세서 및 섀시의 온도 및 상태를 표시합니다. 온도는 섭씨로 제공됩니다. 상태는 다음 중 하나입니다. • OK - 온도가 정상 작동 범위 내에 속합니다. • Critical - 온도가 정상 작동 범위를 벗어났습니다. 작동 범위는 다음과 같이 분류됩니다. • 70도 미만 - OK • 70~80 - Warm • 80~90 - Critical • 90 초과 - Unrecoverable
voltage	(선택 사항) CPU 전압 채널 값(1~24)을 표시합니다. 작동 상태를 제외합니다.

기본값

키워드를 지정하지 않으면 드라이버를 제외하고 모든 작동 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.1(1)	이 명령이 도입되었습니다.
8.4(2)	ASA 5585-X SSP에 대한 출력이 추가되었습니다. 또한 이중 SSP 설치에 대한 지원이 추가되었습니다.
8.4.4(1)	ASA 5515-X, ASA 5525-X, ASA 5545-X 및 ASA 5555-X에 대해 표시되는 전원 공급 디바이스 온도 값이 출력에서 변경되었습니다.
8.6(1)	ASA 5545-X 및 ASA 5555-X의 CPU 전압 조정기 열 이벤트에 대한 출력이 추가되었습니다. 전원 공급 디바이스 입력 상태에 대한 출력이 추가되었습니다. 전압 센서에 대한 출력이 추가되었습니다.

사용 지침

ASA 5545-X, 5555-X, 5580 및 5585-X에 대한 작동 환경 정보를 표시할 수 있습니다. 이 정보에는 팬 및 전원 공급 디바이스의 작동 상태, CPU 및 섀시의 온도 및 상태 등이 포함됩니다. ASA 5580-40은 4개의 CPU에 대한 정보를 표시하고, ASA 5580-20은 2개의 CPU에 대한 정보를 표시합니다.

참고 이중 SSP 설치의 경우 섀시 마스터에 대한 센서만 냉각 팬 및 전원 공급 디바이스에 대한 출력을 표시합니다.

예

다음은 **show environment** 명령의 일반적인 샘플 출력입니다.

```
ciscoasa# show environment

Cooling Fans:
---------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
---------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
```

```
-----------------------------------
   Processors:
   -------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   -------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   -------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

다음은 **show environment driver** 명령의 샘플 출력입니다.

```
ciscoasa# show environment driver

Cooling Fans:
-----------------------------------

   Chassis Fans:
   -------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK

   Power Supplies:
   -------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK

Power Supplies:
-----------------------------------

   Left Slot (PS0): Not Present
   Right Slot (PS1): Present

   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK

   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK

Temperature:
-----------------------------------

   Processors:
   -------------------------------
   Processor 1: 70.0 C - OK

   Chassis:
   -------------------------------
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)

   Power Supplies:
   -------------------------------
   Left Slot (PS0): N/A
```

```
   Right Slot (PS1): 33 C - OK

Voltage:
---------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
   Channel 5:  1.496 V -  (DDR3 1.5V)
   Channel 6:  1.048 V -  (PCH 1.5V)
```

다음은 ASA 5555-X에 대한 **show environment** 명령의 샘플 출력입니다.

```
ciscoasa# show environment

Cooling Fans:
---------------------------------

   Chassis Fans:
   -------------------------------

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 9728 RPM - OK
   Right Slot (PS1): 0 RPM - OK

Power Supplies:
 ---------------------------------

    Left Slot (PS0): Present
    Right Slot (PS1): Present

    Power Input:
    -------------------------------
    Left Slot (PS0): OK
    Right Slot (PS1): Failure Detected

    Temperature:
    -------------------------------
    Left Slot (PS0): 29 C - OK
    Right Slot (PS1): N/A

   Processors:
   -------------------------------
   Processor 1: 81.0 C - OK

   Chassis:
   -------------------------------
   Ambient 1: 39.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 32.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 47.0 C - OK  (Chassis Back Left Temperature)

   Power Supplies:
   -------------------------------
   Left Slot (PS0): 33 C - OK
   Right Slot (PS1): -128 C - OK
```

다음은 이중 SSP 설치의 ASA 5585-X 섀시 마스터에 대한 **show environment** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show environment

Cooling Fans:
---------------------------------
```

```
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)

Power Supplies:
-----------------------------------
   Power Supply Unit Redundancy: N/A

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)

Temperature:
-----------------------------------

   Processors:
   --------------------------------
   Processor 1: 48.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 47.0 C - OK  (CPU2 Core Temperature)

   Chassis:
   --------------------------------
   Ambient 1: 25.5 C - OK  (Chassis Front Temperature)
   Ambient 2: 37.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 31.50 C - OK  (CPU1 Back Temperature)
   Ambient 4: 27.75 C - OK  (CPU1 Front Temperature)
   Ambient 5: 38.25 C - OK  (CPU2 Back Temperature)
   Ambient 6: 34.0 C - OK  (CPU2 Front Temperature)

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)

Voltage:
-----------------------------------
   Channel 1:  3.310 V -  (3.3V (U142 VX1))
   Channel 2:  1.492 V -  (1.5V (U142 VX2))
   Channel 3:  1.053 V -  (1.05V (U142 VX3))
   Channel 4:  3.328 V -  (3.3V_STDBY (U142 VP1))
   Channel 5: 11.675 V -  (12V (U142 VP2))
   Channel 6:  4.921 V -  (5.0V (U142 VP3))
   Channel 7:  6.713 V -  (7.0V (U142 VP4))
   Channel 8:  9.763 V -  (IBV (U142 VH))
   Channel 9:  1.048 V -  (1.05VB (U209 VX2))
   Channel 10:  1.209 V -  (1.2V (U209 VX3))
   Channel 11:  1.109 V -  (1.1V (U209 VX4))
   Channel 12:  0.999 V -  (1.0V (U209 VX5))
   Channel 13:  3.324 V -  (3.3V STDBY (U209 VP1))
   Channel 14:  2.504 V -  (2.5V (U209 VP2))
   Channel 15:  1.799 V -  (1.8V (U209 VP3))
   Channel 16:  1.899 V -  (1.9V (U209 VP4))
   Channel 17:  9.763 V -  (IBV (U209 VH))
   Channel 18:  2.048 V -  (VTT CPU0 (U83 VX2))
   Channel 19:  2.048 V -  (VTT CPU1 (U83 VX3))
   Channel 20:  2.048 V -  (VCC CPU0 (U83 VX4))
```

```
Channel 21:  2.048 V -  (VCC CPU1 (U83 VX5))
Channel 22:  1.516 V -  (1.5VA (U83 VP1))
Channel 23:  1.515 V -  (1.5VB (U83 VP2))
Channel 24:  8.937 V -  (IBV (U83 VH))
```

CPU 전압 조정기 열 이벤트로 인해 ASA가 종료된 경우 다음 경고 메시지가 표시됩니다.

```
WARNING: ASA was previously shut down due to a CPU Voltage Regulator running beyond the
max thermal operating temperature. The chassis and CPU need to be inspected immediately
for ventilation issues.
```

자세한 내용은 syslog 메시지 설명서에서 syslog 메시지 735024를 참고하십시오.

관련 명령

명령	설명
show version	하드웨어 및 소프트웨어 버전을 표시합니다.

show event manager

구성된 각 이벤트 관리자 애플릿에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show event manager** 명령을 사용합니다.

show event manager

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

예

다음은 **show event manager** 명령의 샘플 출력입니다.

```
ciscoasa# show event manager

event manager applet 21, hits 1, last 2014/01/19 06:47:46
  last file disk0:/eem-21-20140119-064746.log
  event countdown 21 secs, left 0 secs, hits 1, last 2014/01/19 06:47:47
  action 1 cli command "sh ver", hits 1, last 2014/01/19 06:47:46
```

관련 명령

명령	설명
show running-config event manager	이벤트 관리자에서 실행 중인 컨피그레이션을 표시합니다.

7 장

show failover through show ipsec stats traffic 명령

show failover

디바이스의 대체작동 상태에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show failover** 명령을 사용합니다.

show failover [**group** *num* | **history** | **interface** | **state** | **statistics**]

구문 설명

group	지정된 대체작동 그룹의 실행 상태를 표시합니다.
history	대체작동 기록을 표시합니다. 대체작동 기록에는 이전 대체작동 상태 변경 및 해당 사유가 표시됩니다. 기록 정보는 디바이스를 재부팅하면 지워집니다.
interface	대체작동 및 상태 저장 링크 정보를 표시합니다.
num	대체작동 그룹 번호입니다.
state	두 대체작동 디바이스 모두의 대체작동 상태를 표시합니다. 표시되는 정보에는 디바이스의 기본 또는 보조 상태, 디바이스의 활성/대기 상태 및 마지막으로 보고된 대체작동 사유가 포함됩니다. 실패 사유는 장애 사유가 지워진 경우에도 출력에 그대로 유지됩니다.
statistics	대체작동 명령 인터페이스의 전송 및 수신 패킷 수를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 수정되었습니다. 출력에 추가 정보가 포함되었습니다.
8.2(2)	이 명령이 수정되었습니다. 출력에 방화벽 및 대체작동 인터페이스에 대한 IPv6 주소가 포함되었습니다. 상태 저장 대체작동 통계 출력에 IPv6 네이버 검색 테이블(IPv6 ND tbl) 업데이트 정보가 포함되었습니다.

사용 지침

show failover 명령은 동적 대체작동 정보, 인터페이스 상태 및 상태 저장 대체작동 통계를 표시합니다.

인터페이스에 IPv4 주소와 IPv6 주소가 둘 다 구성된 경우 두 주소 모두 출력에 표시됩니다. 인터페이스에 둘 이상의 IPv6 주소가 구성되어 있을 수 있으므로 링크-로컬 주소만 표시됩니다. 인터페이스에 구성된 IPv4 주소가 없는 경우 IPv4 주소는 출력에 0.0.0.0으로 표시됩니다. 인터페이스에 구성된 IPv6 주소가 없는 경우 이 주소는 출력에서 생략됩니다.

Stateful Failover Logical Update Statistics 출력은 상태 저장 대체작동이 활성화된 경우에만 표시됩니다. “xerr” 및 “rerr” 값은 대체작동 오류를 나타내는 것이 아니라 패킷 전송 또는 수신 오류 수를 나타냅니다.

참고 ASA 5505에서는 상태 저장 대체작동을 사용할 수 없으므로 상태 저장 대체작동 통계 출력이 제공되지 않습니다.

show failover 명령 출력에서 상태 저장 대체작동 필드의 값은 다음과 같습니다.

- 상태 저장 개체 값은 다음과 같습니다.
  - xmit - 전송된 패킷 수를 나타냅니다.
  - xerr - 전송 오류 수를 나타냅니다.
  - rcv - 수신된 패킷 수를 나타냅니다.
  - rerr - 수신 오류 수를 나타냅니다.
- 각 행은 다음과 같은 특정 개체 정적 개수에 대한 행입니다.
  - General - 모든 상태 저장 개체의 합계를 나타냅니다.
  - sys cmd - **login** 또는 **stay alive**와 같은 논리적 업데이트 시스템 명령을 참조합니다.
  - up time - 활성 ASA에서 대기 ASA로 전달되는 ASA 가동 시간 값을 나타냅니다.
  - RPC services - 원격 프로시저 호출 연결 정보입니다.
  - TCP conn - 동적 TCP 연결 정보입니다.
  - UDP conn - 동적 UDP 연결 정보입니다.
  - ARP tbl - 동적 ARP 테이블 정보입니다.
  - Xlate_Timeout - 연결 변환 시간 제한 정보를 나타냅니다.
  - IPv6 ND tbl - IPv6 네이버 검색 테이블 정보입니다.
  - VPN IKE upd - IKE 연결 정보입니다.
  - VPN IPSEC upd - IPsec 연결 정보입니다.
  - VPN CTCP upd - cTCP 터널 연결 정보입니다.
  - VPN SDI upd - SDI AAA 연결 정보입니다.
  - VPN DHCP upd - 터널링된 DHCP 연결 정보입니다.
  - SIP Session - SIP 신호 처리 세션 정보입니다.
  - Route Session - 경로 동기화 업데이트에 대한 LU 통계입니다.

대체작동 IP 주소를 입력하지 않은 경우 **show failover** 명령은 IP 주소를 0.0.0.0으로 표시하며, 인터페이스 모니터링이 “waiting” 상태로 유지됩니다. 대체작동이 작동하려면 대체작동 IP 주소를 설정해야 합니다.

표 7-1에는 대체작동에 대한 인터페이스 상태가 설명되어 있습니다.

표 7-1 대체작동 인터페이스 상태

상태	설명
Normal	인터페이스가 작동하며, 피어 디바이스의 해당 인터페이스에서 hello 패킷을 받고 있습니다.
Normal (Waiting)	인터페이스가 작동하지만 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 못했습니다. 인터페이스에 대해 대기 IP 주소가 구성되어 있는지, 그리고 두 인터페이스가 연결되어 있는지 확인하십시오.
Normal (Not-Monitored)	인터페이스가 작동하지만 대체작동 프로세스에서 모니터링되지 않습니다. 모니터링되지 않는 인터페이스의 대체작동에서는 대체작동을 트리거하지 않습니다.
No Link	물리적 링크의 작동이 중지되었습니다.
No Link (Waiting)	물리적 링크의 작동이 중지되고 인터페이스가 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 못했습니다. 링크를 복원한 후 인터페이스에 대해 대기 IP 주소가 구성되고 두 인터페이스가 서로 연결되어 있는지 확인하십시오.
No Link (Not-Monitored)	물리적 링크의 작동이 중지되었지만 대체작동 프로세스에서 모니터링되지 않습니다. 모니터링되지 않는 인터페이스의 대체작동에서는 대체작동을 트리거하지 않습니다.
Link Down	물리적 링크가 작동하지만 관리자에 의해 인터페이스의 작동이 중지되었습니다.
Link Down (Waiting)	물리적 링크가 작동하지만 관리자에 의해 인터페이스의 작동이 중지되고 인터페이스가 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 못했습니다. 인터페이스를 작동시킨 후(인터페이스 컨피그레이션 모드에서 **no shutdown** 명령 사용) 해당 인터페이스에 대해 대기 IP 주소가 구성되고 두 인터페이스가 서로 연결되어 있는지 확인하십시오.
Link Down (Not-Monitored)	물리적 링크가 작동하지만 관리자에 의해 인터페이스의 작동이 중지되고 대체작동 프로세스에서 모니터링되지 않습니다. 모니터링되지 않는 인터페이스의 대체작동에서는 대체작동을 트리거하지 않습니다.
Testing	피어 디바이스의 해당 인터페이스에서 hello 패킷이 누락되어 인터페이스가 테스트 모드에 있습니다.
Failed	인터페이스 테스트에 실패했으며 인터페이스가 장애가 발생한 것으로 표시되어 있습니다. 인터페이스 장애로 인해 대체작동 조건이 충족되는 경우 보조 디바이스 또는 대체작동 그룹으로 대체작동됩니다.

다중 컨피그레이션 모드에서는 보안 상황에서만 **show failover** 명령을 사용할 수 있습니다. 선택적 키워드는 입력할 수 없습니다.

예

다음은 활성/대기 대체작동에 대한 **show failover** 명령의 샘플 출력입니다. ASA는 ASA 5500 Series ASA이며, 각 ASA의 슬롯 1에 대한 세부사항에 표시된 대로 각각 CSC SSM이 탑재되어 있습니다. 보안 어플라이언스는 대체작동 링크(folink)와 내부 인터페이스에서 IPv6 주소를 사용합니다.

```
ciscoasa# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: folink Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3/FE80::20d:29ff:fe1d:69f0): Normal
                  Interface outside (10.132.9.3): Normal
                  Interface folink (0.0.0.0/fe80::2a0:c9ff:fe03:101): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4/FE80::20d:29ff:fe2b:7ba6): Normal
                  Interface outside (10.132.9.4): Normal
                  Interface folink (0.0.0.0/fe80::2e0:b6ff:fe07:3096): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.4/24
                  CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     22         0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0
        Route Session   165        0          70         6

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

다음은 활성/활성 대체작동에 대한 **show failover** 명령의 샘플 출력입니다. 이 예에서는 관리 상황에서만 인터페이스에 IPv6 주소가 할당되었습니다.

```
ciscoasa# show failover

Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface folink (10.132.9.5/fe80::2a0:c9ff:fe03:101): Normal
                admin Interface inside (10.130.8.5/fe80::2a0:c9ff:fe01:101): Normal
                admin Interface fourth (10.130.9.5/fe80::3eff:fe11:6670): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface folink (10.132.9.6/fe80::2a0:c9ff:fe03:102): Normal
                admin Interface inside (10.130.8.6/fe80::2a0:c9ff:fe01:102): Normal
                admin Interface fourth (10.130.9.6/fe80::3eff:fe11:6671): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     22         0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
```

```
        VPN CTCP upd    0           0           0           0
        VPN SDI upd     0           0           0           0
        VPN DHCP upd    0           0           0           0
       SIP Session    0           0           0           0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

다음은 ASA 5505에서 실행한 **show failover** 명령의 샘플 출력입니다.

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty

        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

다음은 활성-활성 설정에 대한 **show failover state** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

다음은 활성-대기 설정에 대한 **show failover state** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

표 7-2에는 **show failover state** 명령의 출력이 설명되어 있습니다.

표 7-2 show failover state 출력 설명

필드	설명
Configuration State	컨피그레이션 동기화의 상태를 표시합니다. 대기 디바이스의 가능한 컨피그레이션 상태는 다음과 같습니다. • **Config Syncing - STANDBY** - 동기화된 컨피그레이션이 실행되는 동안 설정됩니다. • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY** - 대기 디바이스가 활성 디바이스로부터의 컨피그레이션 동기화를 완료한 경우에 설정됩니다. 활성 디바이스의 가능한 컨피그레이션 상태는 다음과 같습니다. • **Config Syncing** - 활성 디바이스가 대기 디바이스로 컨피그레이션 동기화를 수행할 때 활성 디바이스에 설정됩니다. • **Interface Config Syncing** • **Sync Done** - 활성 디바이스가 대기 디바이스로의 성공적인 컨피그레이션 동기화를 완료한 경우에 설정됩니다. • **Ready for Config Sync** - 대기 디바이스에서 컨피그레이션 동기화를 수신할 준비가 완료되었다는 신호를 보낸 경우 활성 디바이스에 설정됩니다.
Communication State	MAC 주소 동기화의 상태를 표시합니다. • **Mac set** - MAC 주소가 피어 디바이스에서 이 디바이스로 동기화되었습니다. • **Updated Mac** - MAC 주소가 업데이트되어 다른 디바이스로 동기화해야 하는 경우에 사용됩니다. 또한 디바이스가 피어 디바이스에서 동기화된 로컬 MAC 주소를 업데이트하는 전환 기간 동안에도 사용됩니다.
Date/Time	장애가 발생한 날짜 및 타임스탬프를 표시합니다.

표 7-2 show failover state 출력 설명(계속)

필드	설명
Last Failure Reason	마지막으로 보고된 장애에 대한 사유를 표시합니다. 이 정보는 장애 조건이 삭제된 경우에도 지워지지 않습니다. 대체작동이 발생한 경우에만 변경됩니다. 가능한 실패 사유는 다음과 같습니다. • **Ifc Failure** - 장애가 발생한 인터페이스 수가 대체작동 조건을 충족하여 대체작동이 발생했습니다. • **Comm Failure** - 대체작동 링크가 실패하거나 피어의 작동이 중지되었습니다. • **Backplane Failure**
State	디바이스의 기본/보조 및 활성/대기 상태를 표시합니다.
This host/Other host	This host는 명령이 실행된 디바이스에 대한 정보를 나타냅니다. Other host는 대체작동 쌍의 다른 디바이스에 대한 정보를 나타냅니다.

다음은 **show failover history** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show failover history
==========================================================================
Group     From State                To State                  Reason
==========================================================================
. . .
03:42:29 UTC Apr 17 2009
    0     Sync Config               Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    1     Standby Ready             Failed
Backplane failed

03:42:29 UTC Apr 17 2009
    2     Standby Ready             Failed
Backplane failed

03:44:39 UTC Apr 17 2009
    0     Failed                    Negotiation
Backplane operational

03:44:40 UTC Apr 17 2009
    1     Failed                    Negotiation
Backplane operational

03:44:40 UTC Apr 17 2009
    2     Failed                    Negotiation
Backplane operational

==========================================================================
```

각 항목은 상태 변경이 발생한 시간 및 날짜, 시작 상태, 결과 상태 및 상태 변경 사유를 제공합니다. 최신 항목은 화면의 맨 아래에 있습니다. 이전 항목은 맨 위에 표시됩니다. 최대 60개의 항목이 표시될 수 있습니다. 최대 항목 수에 도달한 후에는 새 항목이 맨 아래에 추가되면서 가장 오래된 항목이 출력의 맨 위에서 제거됩니다.

표 7-3에는 대체작동 상태가 나와 있습니다. 안정적인 상태와 일시적인 상태의 두 가지 상태가 있습니다. 안정적인 상태는 장애와 같은 상황이 발생하여 상태가 변경될 때까지 디바이스가 그대로 유지될 수 있음을 나타냅니다. 일시적인 상태는 디바이스가 안정적인 상태에 도달하는 동안 거치는 상태입니다.

표 7-3 대체작동 상태

상태	설명
Disabled	대체작동이 비활성화되어 있습니다. 이는 안정적인 상태입니다.
Failed	디바이스가 실패한 상태입니다. 이는 안정적인 상태입니다.
Negotiation	디바이스가 피어와의 연결을 설정하고 소프트웨어 버전 호환성 및 활성/대기 역할을 확인하기 위해 피어와 협상합니다. 협상된 역할에 따라 디바이스가 대기 디바이스 상태 또는 활성 디바이스 상태로 전환되거나 실패한 상태가 됩니다. 이는 일시적인 상태입니다.
Not Detected	ASA가 피어의 상태를 감지할 수 없습니다. 이는 ASA가 대체작동이 활성화된 상태로 부팅되지만 피어가 존재하지 않거나 전원이 꺼진 경우에 발생할 수 있습니다.
대기 디바이스 상태	
Cold Standby	디바이스에서 피어가 활성 상태에 도달하기를 기다리는 중입니다. 피어 디바이스가 활성 상태에 도달하면 이 디바이스는 대기 컨피그레이션 상태로 진행됩니다. 이는 일시적인 상태입니다.
Sync Config	디바이스가 피어 디바이스에서 실행 중인 컨피그레이션을 요청합니다. 컨피그레이션 동기화 중 오류가 발생한 경우 디바이스는 초기화 상태로 돌아갑니다. 이는 일시적인 상태입니다.
Sync File System	디바이스가 피어 디바이스와 파일 시스템을 동기화합니다. 이는 일시적인 상태입니다.
Bulk Sync	디바이스가 피어에서 상태 정보를 수신합니다. 이 상태는 상태 저장 대체작동이 활성화된 경우에만 발생합니다. 이는 일시적인 상태입니다.
Standby Ready	디바이스가 활성 디바이스 장애 시 활성 디바이스의 역할을 수행할 준비가 되어 있습니다. 이는 안정적인 상태입니다.
활성 디바이스 상태	
Just Active	활성 디바이스가 되면 시작되는 디바이스의 첫 번째 상태입니다. 이 상태에 있는 동안에는 디바이스가 활성화되고 인터페이스에 대해 IP 및 MAC 주소가 설정되었음을 알리는 메시지가 피어로 전송됩니다. 이는 일시적인 상태입니다.
Active Drain	피어의 대기열 메시지가 삭제됩니다. 이는 일시적인 상태입니다.
Active Applying Config	디바이스가 시스템 컨피그레이션을 적용하는 중입니다. 이는 일시적인 상태입니다.
Active Config Applied	디바이스가 시스템 컨피그레이션 적용을 완료했습니다. 이는 일시적인 상태입니다.
Active	디바이스가 활성 상태이며 트래픽을 처리하는 중입니다. 이는 안정적인 상태입니다.

각 상태 변경에는 상태 변경 사유가 뒤따릅니다. 사유는 일반적으로 디바이스가 일시적인 상태에서 안정적인 상태로 진행될 때 동일하게 유지됩니다. 가능한 상태 변경 사유는 다음과 같습니다.

- No Error
- Set by the CI config cmd
- Failover state check
- Failover interface become OK
- HELLO not heard from mate
- Other unit has different software version
- Other unit operating mode is different
- Other unit license is different
- Other unit chassis configuration is different
- Other unit card configuration is different
- Other unit want me Active
- Other unit want me Standby
- Other unit reports that I am failed
- Other unit reports that it is failed
- Configuration mismatch
- Detected an Active mate
- No Active unit found
- Configuration synchronization done
- Recovered from communication failure
- Other unit has different set of vlans configured
- Unable to verify vlan configuration
- Incomplete configuration synchronization
- Configuration synchronization failed
- Interface check
- My communication failed
- ACK not received for failover message
- Other unit got stuck in learn state after sync
- No power detected from peer
- No failover cable
- HA state progression failed
- Detect service card failure
- Service card in other unit has failed
- My service card is as good as peer
- LAN Interface become un-configured
- Peer unit just reloaded
- Switch from Serial Cable to LAN-Based fover

- Unable to verify state of config sync
- Auto-update request
- Unknown reason

다음은 **show failover interface** 명령의 샘플 출력입니다. 이 디바이스는 대체작동 인터페이스에 IPv6 주소가 구성되어 있습니다.

```
ciscoasa(config)# sh fail int
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

관련 명령

명령	설명
show running-config failover	현재 컨피그레이션에서 **failover** 명령을 표시합니다.

show failover exec

지정된 디바이스에 대한 **failover exec** 명령 모드를 표시하려면 특권 EXEC 모드에서 **show failover exec** 명령을 사용합니다.

show failover exec {**active** | **standby** | **mate**}

구문 설명

active	활성 디바이스에 대한 **failover exec** 명령 모드를 표시합니다.
mate	피어 디바이스에 대한 **failover exec** 명령 모드를 표시합니다.
standby	대기 디바이스에 대한 **failover exec** 명령 모드를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

failover exec 명령은 지정된 디바이스로 세션을 생성합니다. 기본적으로 이 세션은 글로벌 컨피그레이션 모드로 되어 있습니다. **failover exec** 명령을 사용하여 적절한 명령(예: **interface** 명령)을 보내 이 세션의 명령 모드를 변경할 수 있습니다. 지정된 디바이스에 대한 **failover exec** 명령 모드를 변경해도 디바이스에 액세스하는 데 사용 중인 세션의 명령 모드는 변경되지 않습니다. 디바이스의 현재 세션에 대한 명령 모드 변경은 **failover exec** 명령에서 사용하는 명령 모드에 영향을 주지 않습니다.

show failover exec 명령은 **failover exec** 명령을 통해 전송된 명령이 실행되는 지정된 디바이스의 명령 모드를 표시합니다.

예

다음은 **show failover exec** 명령의 샘플 출력입니다. 이 예에서는 **failover exec** 명령을 입력할 디바이스의 명령 모드가 명령을 실행할 디바이스의 **failover exec** 명령 모드와 같지 않아도 된다는 것을 보여 줍니다.

이 예에서는 대기 디바이스에 로그인한 관리자가 활성 디바이스의 인터페이스에 이름을 추가합니다. 이 예에서 **show failover exec mate** 명령을 한 번 더 입력하면 인터페이스 컨피그레이션 모드의 피어 디바이스가 표시됩니다. **failover exec** 명령을 통해 디바이스로 전송된 명령은 이 모드에서 실행됩니다.

```
ciscoasa(config)# show failover exec mate

Active unit Failover EXEC is at config mode

! The following command changes the standby unit failover exec mode
! to interface configuration mode.
ciscoasa(config)# failover exec mate interface GigabitEthernet0/1
ciscoasa(config)# show failover exec mate

Active unit Failover EXEC is at interface sub-command mode

! Because the following command is sent to the active unit, it is replicated
! back to the standby unit.
ciscoasa(config)# failover exec mate nameif test
```

관련 명령

명령	설명
failover exec	제공된 명령을 대체작동 쌍의 지정된 디바이스에서 실행합니다.

show file

파일 시스템에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show file** 명령을 사용합니다.

show file descriptors | system | information *filename*

구문 설명

descriptors	열려 있는 모든 파일 설명자를 표시합니다.
filename	파일 이름을 지정합니다.
information	파트너 애플리케이션 패키지 파일을 포함하여 특정 파일에 대한 정보를 표시합니다.
system	디스크 파일 시스템에 대한 크기, 사용 가능한 바이트 수, 미디어 유형, 플래그 및 접두사 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.2(1)	파트너 애플리케이션 패키지 파일에 대한 정보를 볼 수 있는 기능이 추가되었습니다.

예

다음은 **show file descriptors** 명령의 샘플 출력입니다.

```
ciscoasa# show file descriptors
No open file descriptors
ciscoasa# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

다음은 **show file info** 명령의 샘플 출력입니다.

```
ciscoasa# show file info disk0:csc_embd1.0.1000.pkg
type is package (csc)
file size is 17204149 bytes version 1
```

관련 명령

명령	설명
dir	디렉토리 내용을 표시합니다.
pwd	현재 작업 디렉토리를 표시합니다.

show firewall

현재 방화벽 모드(라우팅 또는 투명 모드)를 표시하려면 특권 EXEC 모드에서 **show firewall** 명령을 사용합니다.

show firewall

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show firewall** 명령의 샘플 출력입니다.

```
ciscoasa# show firewall
Firewall mode: Router
```

관련 명령

명령	설명
firewall transparent	방화벽 모드를 설정합니다.
show mode	현재 상황 모드(단일 모드 또는 다중 모드)를 표시합니다.

show firewall module version

ASA 서비스 모듈의 소프트웨어 버전 번호를 확인하려면 특권 EXEC 모드에서 **show firewall module version** 명령을 입력합니다.

show firewall switch {**1** | **2**} **module** [*module_number*] **version**

구문 설명

module_number	(선택 사항) 모듈 번호를 지정합니다.
switch {**1** | **2**}	VSS 사용자에게만 적용됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show firewall module version** 명령의 샘플 출력입니다.

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

관련 명령

명령	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹을 생성합니다.
show module	설치된 모든 모듈을 표시합니다.

show flash

내부 플래시 메모리의 내용을 표시하려면 특권 EXEC 모드에서 **show flash:** 명령을 사용합니다.

show flash: all | controller | filesys

참고 ASA에서 **flash** 키워드는 **disk0**으로 별칭이 지정됩니다.

구문 설명

all	모든 플래시 정보를 표시합니다.
controller	파일 시스템 컨트롤러 정보를 표시합니다.
filesys	파일 시스템 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show flash:** 명령의 샘플 출력입니다.

```
ciscoasa# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
```

```
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

관련 명령

명령	설명
dir	디렉토리 내용을 표시합니다.
show disk0:	내부 플래시 메모리의 내용을 표시합니다.
show disk1:	외부 플래시 메모리 카드의 내용을 표시합니다.

show flow-export counters

NetFlow 데이터와 연계된 런타임 카운터를 표시하려면 특권 EXEC 모드에서 **show flow-export counters** 명령을 사용합니다.

show flow-export counters

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.1(1)	이 명령이 도입되었습니다.
9.0(1)	소스 포트 할당 오류에 대한 새 오류 카운터가 추가되었습니다.

사용 지침

런타임 카운터에는 통계 데이터 및 오류 데이터가 포함됩니다.

예

다음은 NetFlow 데이터와 연계된 런타임 카운터를 표시하는 **show flow-export counters** 명령의 샘플 출력입니다.

```
ciscoasa# show flow-export counters

destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                        1000
 Errors:
  block allocation failure               0
  invalid interface                      0
  template send failure                  0
  no route to collector                  0
  source port allocation                 0
```

관련 명령

명령	설명
clear flow-export counters	NetFlow의 모든 런타임 카운터를 0으로 재설정합니다.
flow-export destination	NetFlow 컬렉터의 IP 주소 또는 호스트 이름과 NetFlow 컬렉터에서 수신 대기하는 UDP 포트를 지정합니다.
flow-export template timeout-rate	템플릿 정보가 NetFlow 컬렉터로 전송되는 간격을 제어합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 후의 syslog 메시지 및 NetFlow 데이터와 연계된 syslog 메시지를 활성화합니다.

show fragment

IP 프래그먼트 리어셈블리 모듈의 운영 데이터를 표시하려면 특권 EXEC 모드에서 **show fragment** 명령을 입력합니다.

show fragment [*interface*]

구문 설명

interface	(선택 사항) ASA 인터페이스를 지정합니다.

기본값

*interface*를 지정하지 않으면 모든 인터페이스에 명령이 적용됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC 모드	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	컨피그레이션 데이터와 운영 데이터를 구분하기 위해 명령이 두 개의 명령(**show fragment** 및 **show running-config fragment**)으로 구분되었습니다.

예

이 예에서는 IP 프래그먼트 리어셈블리 모듈의 운영 데이터를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

관련 명령

명령	설명
clear configure fragment	IP 프래그먼트 리어셈블리 컨피그레이션을 지우고 기본값을 재설정합니다.
clear fragment	IP 프래그먼트 리어셈블리 모듈의 운영 데이터를 지웁니다.
fragment	패킷 조각화의 추가 관리를 제공하고 NFS와의 호환성을 개선합니다.
show running-config fragment	IP 프래그먼트 리어셈블리 컨피그레이션을 표시합니다.

show gc

가비지 수집 프로세스 통계를 표시하려면 특권 EXEC 모드에서 **show gc** 명령을 사용합니다.

show gc

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show gc** 명령의 샘플 출력입니다.

```
ciscoasa# show gc

Garbage collection process stats:
Total tcp conn delete response             :           0
Total udp conn delete response             :           0
Total number of zombie cleaned             :           0
Total number of embryonic conn cleaned     :           0
Total error response                       :           0
Total queries generated                    :           0
Total queries with conn present response   :           0
Total number of sweeps                     :         946
Total number of invalid vcid               :           0
Total number of zombie vcid                :           0
```

관련 명령

명령	설명
clear gc	가비지 수집 프로세스 통계를 제거합니다.

show h225

ASA를 통해 설정된 H.225 세션에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show h225** 명령을 사용합니다.

show h225

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show h225 명령은 ASA를 통해 설정된 H.225 세션에 대한 정보를 표시합니다. 이 명령은 **debug h323 h225 event**, **debug h323 h245 event** 및 **show local-host** 명령과 함께 H.323 검사 엔진 문제를 해결하는 데 사용됩니다.

show h225, **show h245** 또는 **show h323 ras** 명령을 사용하기 전에 **pager** 명령을 구성하는 것이 좋습니다. 많은 세션 레코드가 있는 경우 **pager** 명령을 구성하지 않으면 **show** 출력이 끝에 도달하는 데 약간의 시간이 걸릴 수 있습니다. 연결 수가 비정상적으로 많은 경우 설정한 기본 시간 제한 값에 따라 세션이 시간 초과되고 있는지 확인하십시오. 설정한 기본 시간 제한 값을 따르지 않는 경우 조사해야 하는 문제가 있는 것입니다.

예

다음은 **show h225** 명령의 샘플 출력입니다.

```
ciscoasa# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
| Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
| 1. CRV 9861
| Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
| Local: | 10.130.56.4/1050 | Foreign: 172.30.254.205/1720
```

이 출력은 현재 로컬 엔드포인트 10.130.56.3과 외부 호스트 172.30.254.203 간에 ASA를 통해 전달되는 활성 H.323 호출 하나가 있으며, 이러한 특정 엔드포인트 간에 현재 CRV(Call Reference Value)가 9861인 동시 호출 하나가 있음을 나타냅니다.

로컬 엔드 포인트 10.130.56.4와 외부 호스트 172.30.254.205의 경우 통시 호출 수는 0개입니다. 이는 H.225 세션이 여전히 존재하는 경우에도 엔드포인트 간에 활성 호출이 없음을 의미합니다. 이는 **show h225** 명령이 실행될 당시에 호출이 이미 종료되었지만 H.225 세션이 아직 삭제되지 않은 경우에 발생할 수 있습니다. 또는 두 엔드포인트가 "maintainConnection"을 TRUE로 설정하여 이를 다시 FALSE로 설정하거나 구성된 H.225 시간 제한 값에 따라 세션 시간이 초과될 때까지 세션이 열린 상태로 유지되기 때문에 두 엔드포인트의 TCP 연결이 계속 열려 있음을 의미할 수도 있습니다.

관련 명령

명령	설명
debug h323	H.323에 대한 디버그 정보 표시를 활성화합니다.
inspect h323	H.323 애플리케이션 검사를 활성화합니다.
show h245	느린 시작을 사용하여 엔드포인트에서 ASA를 통해 설정한 H.245 세션에 대한 정보를 표시합니다.
show h323 ras	ASA를 통해 설정된 H.323 RAS 세션에 대한 정보를 표시합니다.
timeout h225 | h323	H.225 신호 처리 연결 또는 H.323 제어 연결이 닫히는 유휴 시간을 구성합니다.

show h245

느린 시작을 사용하여 엔드포인트에서 ASA를 통해 설정한 H.245 세션에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show h245** 명령을 사용합니다.

show h245

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show h245 명령은 느린 시작을 사용하여 엔드포인트에서 ASA를 통해 설정한 H.245 세션에 대한 정보를 표시합니다. 느린 시작은 호출의 두 엔드포인트가 H.245에 대한 다른 TCP 제어 채널을 여는 경우를 의미합니다. 빠른 시작에서는 H.245 메시지가 H.225 제어 채널에서 H.225 메시지의 일부로 교환됩니다. 이 명령은 **debug h323 h245 event**, **debug h323 h225 event** 및 **show local-host** 명령과 함께 H.323 검사 엔진 문제를 해결하는 데 사용됩니다.

예

다음은 **show h245** 명령의 샘플 출력입니다.

```
ciscoasa# show h245
Total: 1
| LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
| MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
| Local | 10.130.56.3 RTP 49608 RTCP 49609
| MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
| Local | 10.130.56.3 RTP 49606 RTCP 49607
```

현재 ASA를 통해 활성화된 H.245 제어 세션 하나가 있습니다. 로컬 엔드포인트는 10.130.56.3이며, TPKT 값이 0이므로 이 엔드포인트의 다음 패킷에 TPKT 헤더가 있어야 합니다. TKTP 헤더는 각 H.225/H.245 메시지 앞에 있는 4바이트 헤더입니다. 이는 4바이트 헤더를 포함한 메시지 길이를 제공합니다. 외부 호스트는 172.30.254.203이며, TPKT 값이 0이므로 이 엔드포인트에 대한 다음 패킷에 TPKT 헤더가 있어야 합니다.

이러한 엔드포인트 간에 협상된 미디어의 LCN(Logical Channel Number)은 258이며, 외부 RTP IP 주소/포트 쌍은 172.30.254.203/49608, RTCP IP 주소/포트는 172.30.254.203/49609, 로컬 RTP IP 주소/포트 쌍은 10.130.56.3/49608, RTCP 포트는 49609입니다.

두 번째 LCN 259의 외부 RTP IP 주소/포트 쌍은 172.30.254.203/49606, RTCP IP 주소/포트 쌍은 172.30.254.203/49607, 로컬 RTP IP 주소/포트 쌍은 10.130.56.3/49606, RTCP 포트는 49607입니다.

관련 명령

명령	설명
debug h323	H.323에 대한 디버그 정보 표시를 활성화합니다.
inspect h323	H.323 애플리케이션 검사를 활성화합니다.
show h245	느린 시작을 사용하여 엔드포인트에서 ASA를 통해 설정한 H.245 세션에 대한 정보를 표시합니다.
show h323 ras	ASA를 통해 설정된 H.323 RAS 세션에 대한 정보를 표시합니다.
timeout h225 | h323	H.225 신호 처리 연결 또는 H.323 제어 연결이 닫히는 유휴 시간을 구성합니다.

show h323

H.323 연결에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show h323** 명령을 사용합니다.

show h323 {ras | gup}

구문 설명

ras	게이트키퍼와 해당 H.323 엔드포인트 간에 ASA를 통해 설정된 H323 RAS 세션을 표시합니다.
gup	H323 게이트웨이 업데이트 프로토콜 연결에 대한 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show h323 ras 명령은 게이트키퍼와 해당 H.323 엔드포인트 간에 ASA를 통해 설정된 H.323 RAS 세션을 표시합니다. 이 명령은 **debug h323 ras event** 및 **show local-host** 명령과 함께 H.323 검사 엔진 문제를 해결하는 데 사용됩니다.

예

다음은 **show h323 ras** 명령의 샘플 출력입니다.

```
ciscoasa# show h323 ras
Total: 1
| GK | Caller
| 172.30.254.214 10.130.56.14
ciscoasa#
```

이 출력은 게이트키퍼 172.30.254.214와 해당 클라이언트 10.130.56.14 간에 하나의 활성 등록이 있음을 보여 줍니다.

관련 명령

명령	설명
debug h323	H.323에 대한 디버그 정보 표시를 활성화합니다.
inspect h323	H.323 애플리케이션 검사를 활성화합니다.
show h245	느린 시작을 사용하여 엔드포인트에서 ASA를 통해 설정한 H.245 세션에 대한 정보를 표시합니다.
timeout h225 | h323	H.225 신호 처리 연결 또는 H.323 제어 연결이 닫히는 유휴 시간을 구성합니다.

show history

이전에 입력한 명령을 표시하려면 사용자 EXEC 모드에서 **show history** 명령을 사용합니다.

show history

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show history 명령은 이전에 입력한 명령을 표시합니다. 위쪽 및 아래쪽 화살표로 명령을 개별적으로 검사하고, **^p**를 입력하여 이전에 입력한 줄을 표시하거나, **^n**을 입력하여 다음 줄을 표시할 수 있습니다.

예

다음 예에서는 사용자 EXEC 모드에 실행한 **show history** 명령의 샘플 출력을 보여 줍니다.

```
ciscoasa> show history
    show history
    help
    show history
```

다음 예에서는 특권 EXEC 모드에 실행한 **show history** 명령의 샘플 출력을 보여 줍니다.

```
ciscoasa# show history
    show history
    help
    show history
    enable
    show history
```

다음 예에서는 글로벌 컨피그레이션 모드에 실행한 **show history** 명령의 샘플 출력을 보여 줍니다.

```
ciscoasa(config)# show history
    show history
    help
    show history
    enable
    show history
    config t
    show history
```

관련 명령

명령	설명
help	지정된 명령에 대한 도움말 정보를 표시합니다.

show icmp

ICMP 컨피그레이션을 표시하려면 특권 EXEC 모드에서 **show icmp** 명령을 사용합니다.

show icmp

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령은 이전에 없었습니다.

사용 지침

show icmp 명령은 ICMP 설정을 표시합니다.

예

다음 예에서는 ICMP 컨피그레이션을 보여 줍니다.

```
ciscoasa# show icmp
```

관련 명령

clear configure icmp	ICMP 컨피그레이션을 지웁니다.
debug icmp	ICMP에 대한 디버깅 정보 표시를 활성화합니다.
icmp	ASA 인터페이스에서 종료되는 ICMP 트래픽에 대한 액세스 규칙을 구성합니다.
inspect icmp	ICMP 검사 엔진을 활성화하거나 비활성화합니다.
timeout icmp	ICMP에 대한 유휴 시간 제한을 구성합니다.

show idb

인터페이스 설명자 블록의 상태에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show idb** 명령을 사용합니다.

show idb

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

IDB는 인터페이스 리소스를 나타내는 내부 데이터 구조입니다. 화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 **show idb** 명령의 샘플 출력입니다.

```
ciscoasa# show idb
Maximum number of Software IDBs 280. In use 23.

                    HWIDBs     SWIDBs
             Active 6          21
           Inactive 1          2
          Total IDBs 7         23
 Size each (bytes) 116         212
        Total bytes 812        4876

HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0

SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
```

```
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

표 7-4에는 각 필드에 대한 설명이 나와 있습니다.

표 7-4 show idb stats 필드

필드	설명
HWIDBs	모든 HWIDB에 대한 통계를 표시합니다. HWIDB는 시스템의 각 하드웨어 포트에 대해 생성됩니다.
SWIDBs	모든 SWIDB에 대한 통계를 표시합니다. SWIDB는 시스템의 각 기본 및 하위 인터페이스와 상황에 할당된 각 인터페이스에 대해 생성됩니다. 일부 다른 내부 소프트웨어 모듈에서도 IDB를 생성합니다.
HWIDB#	하드웨어 인터페이스 항목을 지정합니다. IDB 시퀀스 번호, 주소 및 인터페이스 이름이 각 줄에 표시됩니다.
SWIDB#	소프트웨어 인터페이스 항목을 지정합니다. IDB 시퀀스 번호, 주소, 해당 vPif ID 및 인터페이스 이름이 각 줄에 표시됩니다.
PEER IDB#	상황에 할당된 인터페이스를 지정합니다. IDB 시퀀스 번호, 주소, 해당 vPif ID, 상황 ID 및 인터페이스 이름이 각 줄에 표시됩니다.

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show igmp groups

ASA에 직접 연결되고 IGMP를 통해 학습된 수신기가 있는 멀티캐스트 그룹을 표시하려면 특권 EXEC 모드에서 **show igmp groups** 명령을 사용합니다.

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

구문 설명

detail	(선택 사항) 소스에 대한 자세한 설명을 제공합니다.
group	(선택 사항) IGMP 그룹의 주소입니다. 이 선택적 인수를 포함하면 지정된 그룹으로 표시가 제한됩니다.
if_name	(선택 사항) 지정된 인터페이스에 대한 그룹 정보를 표시합니다.
reserved	(선택 사항) 예약된 그룹에 대한 정보를 표시합니다.
summary	(선택 사항) 그룹 가입 요약 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

모든 선택적 인수 및 키워드를 생략한 경우 **show igmp groups** 명령은 직접 연결된 모든 멀티캐스트 그룹을 그룹 주소, 인터페이스 유형 및 인터페이스 번호별로 표시합니다.

예

다음은 **show igmp groups** 명령의 샘플 출력입니다.

```
ciscoasa# show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

관련 명령

명령	설명
show igmp interface	인터페이스에 대한 멀티캐스트 정보를 표시합니다.

show igmp interface

인터페이스에 대한 멀티캐스트 정보를 표시하려면 특권 EXEC 모드에서 **show igmp interface** 명령을 사용합니다.

show igmp interface [*if_name*]

구문 설명

if_name	(선택 사항) 선택한 인터페이스에 대한 IGMP 그룹 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 수정되었습니다. **detail** 키워드가 제거되었습니다.

사용 지침

선택적 *if_name* 인수를 생략한 경우 **show igmp interface** 명령은 모든 인터페이스에 대한 정보를 표시합니다.

예

다음은 **show igmp interface** 명령의 샘플 출력입니다.

```
ciscoasa# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

관련 명령

명령	설명
show igmp groups	ASA에 직접 연결되고 IGMP를 통해 학습된 수신기가 있는 멀티캐스트 그룹을 표시합니다.

show igmp traffic

IGMP 트래픽 통계를 표시하려면 특권 EXEC 모드에서 **show igmp traffic** 명령을 사용합니다.

show igmp traffic

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show igmp traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                            Received     Sent
Valid IGMP Packets             3           6
Queries                        2           6
Reports                        1           0
Leaves                         0           0
Mtrace packets                 0           0
DVMRP packets                  0           0
PIM packets                    0           0

Errors:
Malformed Packets              0
Martian source                 0
Bad Checksums                  0
```

관련 명령

명령	설명
clear igmp counters	모든 IGMP 통계 카운터를 지웁니다.
clear igmp traffic	IGMP 트래픽 카운터를 지웁니다.

show import webvpn

ASA 또는 AnyConnect Secure Mobility Client를 사용자 지정하고 지역화하는 플래시 메모리의 파일, 사용자 지정 개체, 변환 테이블 또는 플러그인을 나열하려면 특권 EXEC 모드에서 **show import webvpn** 명령을 사용합니다.

show import webvpn {**AnyConnect-customization** | **customization** | **mst-translation** | **plug-in** | **translation-table** | **url-list** | **webcontent**}[**detailed** | **xml-output**]

구문 설명

AnyConnect-customization	AnyConnect 클라이언트 GUI를 사용자 지정하는 ASA 플래시 메모리의 리소스 파일, 실행 파일 및 MS 변환을 표시합니다.
customization	클라이언트리스 VPN 포털(파일 이름이 base64로 디코딩됨)을 사용자 지정하는 ASA 플래시 메모리의 XML 사용자 지정 개체를 표시합니다.
mst-translation	AnyConnect 클라이언트 설치 프로그램을 변환하는 ASA 플래시 메모리의 MS 변환을 표시합니다.
plug-in	ASA 플래시 메모리의 플러그인 모듈(SSH, VNC, RDP 등의 타사 Java 기반 클라이언트 애플리케이션)을 표시합니다.
translation-table	클라이언트리스 포털, Secure Desktop 및 플러그인에서 표시하는 사용자 메시지의 언어를 변환하는 ASA 플래시 메모리의 변환 테이블을 표시합니다.
url-list	클라이언트리스 포털(파일 이름이 base64로 디코딩됨)에서 사용하는 ASA 플래시 메모리의 URL 목록을 표시합니다.
webcontent	클라이언트리스 포털, 클라이언트리스 애플리케이션 및 플러그인에서 온라인 도움말을 엔드 유저에게 표시하기 위해 사용하는 ASA의 플래시 메모리의 콘텐츠를 표시합니다.
detailed	플래시 메모리 내의 파일 및 해시 경로를 표시합니다.
xml-output	파일의 XML을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.2(1)	**AnyConnect-customization** 키워드가 추가되었습니다.

사용 지침

show import webvpn 명령을 사용하여 클라이언트리스 SSL VPN 사용자가 사용할 수 있는 사용자 지정 데이터 및 Java 기반 클라이언트 애플리케이션을 식별할 수 있습니다. 표시된 목록은 ASA의 플래시 메모리에 있는 요청된 모든 데이터 형식을 항목화합니다.

예

다음 예에서는 여러 **show import webvpn** 명령에서 표시하는 WebVPN 데이터를 보여 줍니다.

```
ciscoasa# show import webvpn plug
ssh
rdp
vnc
ciscoasa#

ciscoasa#show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tue, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTsPnjdBOo= Tue, 15 Sep 2009 23:23:56 GMT
rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT
ciscoasa# show import webvpn customization
Template
DfltCustomization
ciscoasa#

ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                              customization
  ua                                              customization
ciscoasa#

ciscoasa# show import webvpn url-list
Template
No bookmarks are currently defined
ciscoasa#

ciscoasa# show import webvpn webcontent
No custom webcontent is loaded
ciscoasa#
```

관련 명령

명령	설명
revert webvpn all	현재 ASA에 있는 모든 WebVPN 데이터 및 플러그인을 제거합니다.

show interface

인터페이스 통계를 보려면 특권 EXEC 모드에서 **show interface** 명령을 사용합니다.

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] [**stats** | **detail**]

구문 설명

detail	(선택 사항) 인터페이스가 추가된 순서, 구성된 상태, 실제 상태, 비대칭 라우팅 통계 등의 자세한 인터페이스 정보를 표시합니다(**asr-group** 명령에 의해 활성화된 경우). 모든 인터페이스를 표시할 경우 SSM의 내부 인터페이스에 대한 정보가 표시됩니다(ASA 5500 Series Adaptive Security Appliance에 설치된 경우). 내부 인터페이스는 사용자가 구성할 수 없으며, 정보는 디버깅용으로만 제공됩니다.
interface_name	(선택 사항) **nameif** 명령으로 설정된 인터페이스 이름을 식별합니다.
mapped_name	(선택 사항) 다중 상황 모드에서 매핑된 이름(**allocate-interface** 명령을 사용하여 할당된 경우)을 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet 0/1**)를 식별합니다. 허용되는 값은 **interface** 명령을 참조하십시오.
redundant*number*	(선택 사항) 이중 인터페이스 ID(예: **redundant1**)를 식별합니다.
stats	(기본값) 인터페이스 정보 및 통계를 표시합니다. 이 키워드는 기본값이므로 선택 사항입니다.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
vlan *number*	(선택 사항) ASA 5505 Adaptive Security Appliance와 같은 내장형 스위치가 있는 모델에 대한 VLAN 인터페이스를 지정합니다.

기본값

옵션을 지정하지 않은 경우 이 명령은 모든 인터페이스에 대한 기본 통계를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	새 인터페이스 번호 매기기 체계를 포함하고 **stats** 키워드(명료성을 위해) 및 **detail** 키워드를 추가하도록 이 명령이 수정되었습니다.
7.0(4)	이 명령에 4GE SSM 인터페이스에 대한 지원이 추가되었습니다.
7.2(1)	이 명령에 스위치 인터페이스에 대한 지원이 추가되었습니다.

릴리스	수정 사항
8.0(2)	이 명령에 이중 인터페이스에 대한 지원이 추가되었습니다. 또한 하위 인터페이스에 대한 지연이 추가되었습니다. 두 개의 새 카운터(input reset drops 및 output reset drops)가 추가되었습니다.
8.2(1)	블록 할당 실패 횟수를 표시하도록 no buffer 수가 변경되었습니다.
8.6(1)	이 명령에 소프트웨어 모듈의 제어 평면 인터페이스 및 ASA 5555-X 공유 관리 인터페이스를 통한 ASA 5512-X 지원이 추가되었습니다. 관리 인터페이스는 **show interface detail** 명령을 통해 Internal-Data0/1로 표시되고, 제어 평면 인터페이스는 Internal-Control0/0으로 표시됩니다.

사용 지침

인터페이스가 상황 간에 공유되는 경우 상황 내에서 이 명령을 입력하면 ASA에 현재 상황에 대한 통계만 표시됩니다. 물리적 인터페이스에 대한 시스템 실행 공간에서 이 명령을 입력하면 ASA에 모든 상황에 대한 통합 통계가 표시됩니다.

하위 인터페이스에 대해 표시되는 통계 수는 물리적 인터페이스에 대해 표시되는 통계 수의 하위 집합입니다.

nameif 명령은 상황 내에서만 사용할 수 있으므로 시스템 실행 공간에서는 인터페이스 이름을 사용할 수 없습니다. 마찬가지로 **allocate-interface** 명령을 사용하여 인터페이스 ID를 매핑된 이름으로 매핑한 경우 매핑된 이름만 상황에서 사용할 수 있습니다. **allocate-interface** 명령에서 **visible** 키워드를 설정한 경우 ASA의 **show interface** 명령 출력에 인터페이스 ID가 표시됩니다.

참고 전송되거나 수신된 바이트 수는 하드웨어 카운트와 트래픽 통계 카운트에서 서로 다릅니다.

하드웨어 카운트에서는 수량이 하드웨어에서 직접 수신되므로 계층 2 패킷 크기를 반영합니다. 반면, 트래픽 통계에서는 계층 3 패킷 크기를 반영합니다.

이러한 카운트 차이는 인터페이스 카드 하드웨어의 설계에 따라 달라집니다.

예를 들어 고속 이더넷 카드의 경우 이더넷 헤더를 포함하기 때문에 계층 2 카운트가 트래픽 카운트보다 14바이트 더 많습니다. 기가비트 이더넷 카드의 경우 이더넷 헤더와 CRC를 모두 포함하므로 계층 2 카운트가 트래픽 카운트보다 18바이트 더 많습니다.

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 **show interface** 명령의 샘플 출력입니다.

```
ciscoasa# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
```

```
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
```

```
        Auto-Duplex, Auto-Speed
        Active member of Redundant5
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

표 7-5에는 각 필드에 대한 설명이 나와 있습니다.

표 7-5 show interface 필드

필드	설명
Interface *ID*	인터페이스 ID입니다. **allocate-interface** 명령 **visible** 키워드를 설정하지 않은 경우 상황 내에서 ASA는 매핑된 이름(구성된 경우)을 표시합니다.
"*interface_name*"	**nameif** 명령으로 설정된 인터페이스 이름입니다. 시스템에서는 이름을 설정할 수 없으므로 시스템 실행 공간에서는 이 필드가 비어 있습니다. 이름을 구성하지 않은 경우 Hardware 줄 뒤에 다음 메시지가 표시됩니다. `Available but not configured via nameif`
is *state*	다음과 같은 관리 상태입니다. • up - 인터페이스가 종료되지 않았습니다. • administratively down - **shutdown** 명령을 통해 인터페이스가 종료되었습니다.
Line protocol is *state*	다음과 같은 회선 상태입니다. • up - 작동하는 케이블이 네트워크 인터페이스에 연결되어 있습니다. • down - 케이블이 잘못되었거나 인터페이스 커넥터에 연결되어 있지 않습니다.
VLAN identifier	하위 인터페이스에 대한 VLAN ID입니다.
Hardware	인터페이스 유형, 최대 대역폭, 지연, 이중 및 속도입니다. 링크가 중단되면 이중 및 속도에 구성된 값이 표시됩니다. 링크가 작동하면 이러한 필드에 실제 설정이 괄호 안에 포함된 구성된 값이 표시됩니다. 다음 목록은 일반적인 하드웨어 유형을 설명합니다. • i82542 - PIX 플랫폼에서 사용되는 Intel PCI 파이버 기가비트 카드 • i82543 - PIX 플랫폼에서 사용되는 Intel PCI-X 파이버 기가비트 카드 • i82546GB - ASA 플랫폼에서 사용되는 Intel PCI-X 구리 기가비트 • i82547GI - ASA 플랫폼에서 백플레인으로 사용되는 Intel CSA 구리 기가비트 • i82557 - ASA 플랫폼에서 사용되는 Intel PCI 구리 고속 이더넷 • i82559 - PIX 플랫폼에서 사용되는 Intel PCI 구리 고속 이더넷 • VCS7380 - SSM-4GE에서 사용되는 Vitesse 4포트 기가비트 스위치
Media-type	(4GE SSM 인터페이스에만 해당) 인터페이스가 RJ-45로 설정되어 있는지 또는 SFP로 설정되어 있는지 표시합니다.

표 7-5 show interface 필드(계속)

필드	설명

message area	경우에 따라 메시지가 표시될 수 있습니다. 다음 예를 참고하십시오.
	• 시스템 실행 공간에서 다음과 같은 메시지가 표시될 수 있습니다.
	`Available for allocation to a context`
	• 이름을 구성하지 않은 경우 다음과 같은 메시지가 표시됩니다.
	`Available but not configured via nameif`
	• 인터페이스가 이중 인터페이스의 멤버인 경우 다음과 같은 메시지가 표시됩니다.
	`Active member of Redundant5`

MAC address	인터페이스의 MAC 주소입니다.
MTU	이 인터페이스에서 허용되는 최대 패킷 크기(바이트)입니다. 인터페이스 이름을 설정하지 않은 경우에는 이 필드에 "MTU not set"이 표시됩니다.
IP address	**ip address** 명령을 사용하여 설정되거나 DHCP 서버에서 수신된 인터페이스 IP 주소입니다. 시스템에서는 IP 주소를 설정할 수 없으므로 시스템 실행 공간에서는 이 필드에 "IP address unassigned"가 표시됩니다.
Subnet mask	IP 주소의 서브넷 마스크입니다.
Packets input	이 인터페이스에서 수신된 패킷 수입니다.
Bytes	이 인터페이스에서 수신된 바이트 수입니다.
No buffer	블록 할당 실패 횟수입니다.
Received:	
Broadcasts	수신한 브로드캐스트 수입니다.
Input errors	아래 나열된 유형을 포함한 총 입력 오류 수입니다. 다른 입력 관련 오류로 인해 입력 오류 수가 증가할 수도 있으며, 일부 데이터그램에 둘 이상의 오류가 있을 수도 있습니다. 따라서 이 합계가 아래 유형에 대해 나열된 오류 수를 초과할 수 있습니다.
Runts	최소 패킷 크기(64바이트)보다 작기 때문에 삭제된 패킷 수입니다. Runt는 일반적으로 충돌로 인해 발생합니다. 또한 잘못된 배선 및 전기 간섭으로 인해 발생할 수도 있습니다.
Giants	최대 패킷 크기를 초과하기 때문에 삭제된 패킷 수입니다. 예를 들어 1518바이트보다 큰 이더넷 패킷은 Giant로 간주됩니다.
CRC	Cyclical Redundancy Check 오류 수입니다. 스테이션에서는 프레임을 전송할 때 프레임 끝에 CRC를 추가합니다. 이 CRC는 프레임의 데이터를 기반으로 알고리즘에서 생성됩니다. 소스와 대상 간에 프레임이 변경된 경우 ASA는 CRC가 일치하지 않는 것으로 기록합니다. 더 많은 CRC 수는 일반적으로 충돌로 인해 발생하거나 스테이션에서 잘못된 데이터를 전송했기 때문에 발생합니다.
Frame	프레임 오류 수입니다. 잘못된 프레임에는 길이 또는 프레임 체크섬이 잘못된 패킷이 포함됩니다. 이 오류는 일반적으로 충돌 또는 이더넷 디바이스의 오작동으로 인해 발생합니다.
Overrun	입력 속도가 ASA에서 데이터를 처리할 수 있는 성능을 초과하기 때문에 ASA가 수신된 데이터를 하드웨어 버퍼로 전달하지 못한 횟수입니다.
Ignored	이 필드는 사용되지 않습니다. 값은 항상 0입니다.

표 7-5 show interface 필드(계속)

필드	설명
Abort	이 필드는 사용되지 않습니다. 값은 항상 0입니다.
L2 decode drops	이름이 구성(**nameif** 명령)되지 않았거나 VLAN ID가 잘못된 프레임이 수신되어 삭제된 패킷 수입니다. 이중 인터페이스 컨피그레이션의 대기 인터페이스에는 구성된 이름(**nameif** 명령)이 없기 때문에 이 카운터가 증가할 수 있습니다.
Packets output	이 인터페이스에서 전송된 패킷 수입니다.
Bytes	이 인터페이스에서 전송된 바이트 수입니다.
Underruns	송신기가 ASA에서 처리할 수 있는 것보다 빠르게 실행된 횟수입니다.
Output Errors	구성된 최대 충돌 수를 초과했기 때문에 전송되지 않은 프레임 수입니다. 이 카운터는 네트워크 트래픽이 많은 경우에만 증가합니다.
Collisions	이더넷 충돌(단일 및 다중 충돌)로 인해 재전송된 메시지 수입니다. 일반적으로 과도하게 연장된 LAN(이더넷 또는 트렌시버 케이블이 너무 길거나, 스테이션 사이에 세 개 이상의 리피터가 있거나, 연속된 다중 포트 트렌시버가 너무 많은 경우)에서 발생합니다. 충돌하는 패킷은 출력 패킷에서 한 번만 계산됩니다.
Interface resets	인터페이스가 재설정된 횟수입니다. 인터페이스가 3초 동안 전송할 수 없는 경우 ASA는 전송을 다시 시작하도록 인터페이스를 재설정합니다. 이 간격 동안 연결 상태는 유지됩니다. 인터페이스가 루프백 또는 종료된 경우에도 인터페이스 재설정이 발생할 수 있습니다.
Babbles	사용되지 않습니다. “babble”은 송신기가 최대 프레임을 전송하는 데 걸린 시간보다 오랫동안 인터페이스에 있었음을 의미합니다.
Late collisions	정상적인 충돌 기간을 벗어나 충돌이 발생했기 때문에 전송되지 않은 프레임 수입니다. 지연 충돌은 패킷 전송에서 늦게 감지된 충돌입니다. 일반적으로 발생하지 않습니다. 두 개의 이더넷 호스트가 동시에 통신하려고 시도하는 경우 패킷 초기에 호스트가 충돌하여 둘 다 다시 꺼지거나, 두 번째 호스트가 첫 번째 호스트를 통신 중인 것으로 인식하여 대기하게 됩니다. 지연 충돌이 발생한 경우 디바이스는 ASA에서 패킷 전송을 부분적으로 완료하는 동안 이더넷에서 패킷을 전송하려고 시도합니다. ASA는 패킷의 첫 번째 부분을 유지하는 버퍼를 지웠을 수 있으므로 패킷을 다시 전송하지 않습니다. 네트워킹 프로토콜은 패킷을 다시 보내 충돌에 대처하도록 설계되므로 이 문제는 실제로 발생하지 않습니다. 그러나 지연 충돌은 네트워크에 문제가 있음을 나타냅니다. 일반적인 문제는 사양을 초과하여 실행되는 이더넷 네트워크 및 반복되는 대규모 네트워크입니다.
Deferred	링크 활동으로 인해 전송 전에 지연된 프레임 수입니다.
input reset drops	재설정이 발생한 경우 RX 링에서 삭제된 패킷 수를 계산합니다.
output reset drops	재설정이 발생한 경우 TX 링에서 삭제된 패킷 수를 계산합니다.
Rate limit drops	(4GE SSM 인터페이스에만 해당) 기가비트가 아닌 속도로 인터페이스를 구성한 후 컨피그레이션에 따라 10Mbps 또는 100Mbps보다 빠른 속도로 전송하려고 시도한 경우 삭제된 패킷 수입니다.
Lost carrier	전송 중에 반송파 신호가 손실된 횟수입니다.
No carrier	사용되지 않습니다.
Input queue (curr/max packets):	입력 대기열의 현재 및 최대 패킷 수입니다.

표 7-5 show interface 필드(계속)

필드	설명
Hardware	하드웨어 대기열의 패킷 수입니다.
Software	소프트웨어 대기열의 패킷 수입니다. 기가비트 이더넷 인터페이스에는 사용할 수 없습니다.
Output queue (curr/max packets):	출력 대기열의 현재 및 최대 패킷 수입니다.
Hardware	하드웨어 대기열의 패킷 수입니다.
Software	소프트웨어 대기열의 패킷 수입니다.
input queue (blocks free curr/low)	curr/low 항목은 인터페이스의 수신(입력) 설명자 링의 현재 슬롯 수 및 항상 사용 가능한 최소 슬롯 수입니다. 이는 기본 CPU에 의해 업데이트되므로 항상 사용 가능한 최소(인터페이스 통계가 지워지거나 디바이스가 다시 로드될 때까지) 워터마크는 그다지 정확하지 않습니다.
output queue (blocks free curr/low)	curr/low 항목은 인터페이스의 전송(출력) 설명자 링의 현재 슬롯 수 및 항상 사용 가능한 최소 슬롯 수입니다. 이는 기본 CPU에 의해 업데이트되므로 항상 사용 가능한 최소(인터페이스 통계가 지워지거나 디바이스가 다시 로드될 때까지) 워터마크는 그다지 정확하지 않습니다.
Traffic Statistics:	수신되거나 전송되거나 삭제된 패킷 수입니다.
Packets input	수신된 패킷 수와 바이트 수입니다.
Packets output	전송된 패킷 수와 바이트 수입니다.
Packets dropped	삭제된 패킷 수입니다. 일반적으로 이 카운터는 ASP(가속화된 보안 경로)에서 삭제된 패킷에 대해 증가합니다(예: 패킷이 액세스 목록 거부로 인해 삭제된 경우). 인터페이스에서 잠재적으로 삭제될 수 있는 사유는 **show asp drop** 명령을 참고하십시오.
1 minute input rate	지난 1분 동안 수신된 패킷 수(패킷/초 및 바이트/초)입니다.
1 minute output rate	지난 1분 동안 전송된 패킷 수(패킷/초 및 바이트/초)입니다.
1 minute drop rate	지난 1분 동안 삭제된 패킷 수(패킷/초)입니다.
5 minute input rate	지난 5분 동안 수신된 패킷 수(패킷/초 및 바이트/초)입니다.
5 minute output rate	지난 5분 동안 전송된 패킷 수(패킷/초 및 바이트/초)입니다.
5 minute drop rate	지난 5분 동안 삭제된 패킷 수(패킷/초)입니다.
Redundancy Information:	이중 인터페이스에 대한 멤버의 물리적 인터페이스를 표시합니다. 활성 인터페이스에는 인터페이스 ID 뒤에 “(Active)”가 표시됩니다. 멤버를 아직 지정하지 않은 경우 다음 출력이 표시됩니다. `Members unassigned`
Last switchover	이중 인터페이스에 대해 활성 인터페이스가 대기 인터페이스로 마지막으로 대체작동된 시간을 표시합니다.

다음은 ASA 5505에서 실행된 **show interface** 명령의 샘플 출력입니다(스위치 포트 포함).

```
ciscoasa# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec

    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

표 7-6에는 스위치 인터페이스(예: ASA 5505 Adaptive Security Appliance)에 대한 **show interface** 명령의 각 필드가 설명되어 있습니다. **show interface** 명령에서도 표시되는 필드는 표 7-6을 참고하십시오.

표 7-6 스위치 인터페이스에 대한 show interface 필드

필드	설명
switch ingress policy drops	이 삭제는 일반적으로 포트가 올바르게 구성되지 않은 경우 발생합니다. 기본 또는 사용자 구성 스위치 포트 설정으로 인해 스위치 포트 내에서 패킷을 성공적으로 전달할 수 없는 경우 이 수가 증가합니다. 이 삭제의 가능한 원인은 다음과 같은 컨피그레이션입니다. • **nameif** 명령이 VLAN 인터페이스에 구성되어 있지 않습니다. **참고** 동일한 VLAN 내에 있는 인터페이스의 경우 **nameif** 명령이 구성되지 않은 경우에도 VLAN 내의 스위칭이 성공하고 이 카운터가 증가하지 않습니다. • VLAN이 종료되었습니다. • 액세스 포트에서 802.1Q 태그가 지정된 패킷을 수신했습니다. • 트렁크 포트에서 허용되지 않는 태그 또는 태그가 지정되지 않은 패킷을 수신했습니다. • ASA가 이더넷 연결이 유지된 다른 Cisco 디바이스에 연결되어 있습니다. 예를 들어, Cisco IOS 소프트웨어에서 이더넷 루프백 패킷을 사용하여 인터페이스 상태를 유지하는 경우 이 패킷은 다른 디바이스에서 수신되지 않습니다. 패킷을 전송할 수 있으면 정상 상태가 유지됩니다. 이러한 유형의 패킷은 스위치 포트에서 삭제되므로 카운터가 증가합니다.
switch egress policy drops	현재 사용되지 않습니다.

다음은 **show interface detail** 명령의 샘플 출력입니다. 다음 예에서는 내부 인터페이스(플랫폼에 대해 존재하는 경우) 및 비대칭 라우팅 테이블(**asr-group** 명령을 통해 활성화된 경우)을 포함하여 모든 인터페이스에 대한 자세한 인터페이스 통계를 보여 줍니다.

```
ciscoasa# show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
```

```
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

표 7-7에는 **show interface detail** 명령의 각 필드에 대한 설명이 나와 있습니다. **show interface** 명령에서도 표시되는 필드는 표 7-7을 참고하십시오.

표 7-7 show interface detail 필드

필드	설명
Demux drops	(내부 데이터 인터페이스에만 해당) ASA가 SSM 인터페이스의 패킷을 역다중화할 수 없어 삭제된 패킷 수입니다. SSM 인터페이스는 백플레인을 통해 기본 인터페이스와 통신하며, 모든 SSM 인터페이스의 패킷은 백플레인에서 다중화됩니다.
Control Point Interface States:	
Interface number	0에서 시작하여 이 인터페이스가 생성된 순서를 나타내는 디버깅용 번호입니다.
Interface config status	다음과 같은 관리 상태입니다. • active - 인터페이스가 종료되지 않았습니다. • not active - **shutdown** 명령을 통해 인터페이스가 종료되었습니다.
Interface state	인터페이스의 실제 상태입니다. 대부분의 경우 이 상태는 위의 config status와 일치합니다. 고가용성을 구성한 경우 ASA에서 필요에 따라 인터페이스를 작동하거나 중단하기 때문에 불일치가 발생할 수 있습니다.
Asymmetrical Routing Statistics:	
Received X1 packets	이 인터페이스에서 수신된 ASR 패킷 수입니다.
Transmitted X2 packets	이 인터페이스에서 전송된 ASR 패킷 수입니다.
Dropped X3 packets	이 인터페이스에서 삭제된 ASR 패킷 수입니다. 패킷을 전달하려고 할 때 인터페이스의 작동이 중지된 경우 패킷이 삭제될 수 있습니다.

다음은 ASA 5512-X~ASA 5555-X에서 실행된 **show interface detail** 명령의 샘플 출력입니다. 이 예에서는 ASA 및 소프트웨어 모듈 둘 다에 대한 Management 0/0 인터페이스("Internal-Data0/1"로 표시)의 통합 통계를 보여 줍니다. 또한 소프트웨어 모듈과 ASA 간의 제어 트래픽에 사용되는 Internal-Control0/0 인터페이스도 출력에 표시되어 있습니다.

```
Interface Internal-Data0/1 "ipsmgmt", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "ipsmgmt":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active

Interface Internal-Control0/0 "cplane", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
```

```
     5 minute input rate 0 pkts/sec,  0 bytes/sec
     5 minute output rate 0 pkts/sec,  0 bytes/sec
     5 minute drop rate, 0 pkts/sec
Control Point Interface States:
       Interface number is 11
       Interface config status is active
       Interface state is active
```

관련 명령

명령	설명
allocate-interface	인터페이스 및 하위 인터페이스를 보안 상황에 할당합니다.
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
delay	인터페이스에 대한 지연 메트릭을 변경합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
nameif	인터페이스 이름을 설정합니다.
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.

show interface ip brief

인터페이스 IP 주소 및 상태를 보려면 특권 EXEC 모드에서 **show interface ip brief** 명령을 사용합니다.

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] **ip brief**

구문 설명

interface_name	(선택 사항) **nameif** 명령으로 설정된 인터페이스 이름을 식별합니다.
mapped_name	(선택 사항) 다중 상황 모드에서 매핑된 이름(**allocate-interface** 명령을 사용하여 할당된 경우)을 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다. 허용되는 값은 **interface** 명령을 참조하십시오.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
vlan *number*	(선택 사항) ASA 5505 Adaptive Security Appliance와 같은 내장형 스위치가 있는 모델에 대한 VLAN 인터페이스를 지정합니다.

기본값

인터페이스를 지정하지 않은 경우 ASA에서 모든 인터페이스를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드[1]	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

1. Management 0/0 인터페이스 또는 하위 인터페이스에만 사용할 수 있습니다.

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.2(1)	이 명령에 VLAN 인터페이스 및 투명 모드의 Management 0/0 인터페이스 또는 하위 인터페이스에 대한 지원이 추가되었습니다.

사용 지침

다중 상황 모드에서 **allocate-interface** 명령으로 인터페이스 ID를 매핑한 경우 하나의 상황에서만 매핑된 이름 또는 인터페이스 이름을 지정할 수 있습니다.

화면 출력에 대한 설명은 "예" 섹션을 참고하십시오.

예

다음은 **show ip brief** 명령의 샘플 출력입니다.

```
ciscoasa# show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

표 7-7에는 각 필드에 대한 설명이 나와 있습니다.

표 7-8 show interface ip brief 필드

필드	설명
Interface	인터페이스 ID 또는 다중 상황 모드의 경우 매핑된 이름(**allocate-interface** 명령을 사용하여 구성한 경우)입니다. 모든 인터페이스를 표시할 경우 AIP SSM의 내부 인터페이스에 대한 정보가 표시됩니다(ASA에 설치된 경우). 내부 인터페이스는 사용자가 구성할 수 없으며, 정보는 디버깅용으로만 제공됩니다.
IP-Address	인터페이스 IP 주소입니다.
OK?	이 열은 현재 사용되지 않으며, 항상 "Yes"로 표시됩니다.
Method	인터페이스에서 IP 주소를 수신한 방법입니다. 값은 다음과 같습니다. • unset - 구성된 IP 주소가 없습니다. • manual - 실행 중인 컨피그레이션을 구성했습니다. • CONFIG - 시작 컨피그레이션에서 로드했습니다. • DHCP - DHCP 서버에서 수신했습니다.
Status	다음과 같은 관리 상태입니다. • up - 인터페이스가 종료되지 않았습니다. • administratively down - **shutdown** 명령을 통해 인터페이스가 종료되었습니다.
Protocol	다음과 같은 회선 상태입니다. • up - 작동하는 케이블이 네트워크 인터페이스에 연결되어 있습니다. • down - 케이블이 잘못되었거나 인터페이스 커넥터에 연결되어 있지 않습니다.

관련 명령

명령	설명
allocate-interface	인터페이스 및 하위 인터페이스를 보안 상황에 할당합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
ip address	인터페이스의 IP 주소를 설정하거나 투명한 방화벽의 경우 관리 IP 주소를 설정합니다.
nameif	인터페이스 이름을 설정합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show inventory

네트워킹 디바이스에 설치되어 있으며 PID(Product Identifier: 제품 식별자), VID(Version Identifier: 버전 식별자) 및 SN(Serial Number: 일련 번호)이 할당된 모든 Cisco 제품에 대한 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show inventory** 명령을 사용합니다.

show inventory [*mod_id*]

구문 설명

mod_id	(선택 사항) 모듈 ID 또는 슬롯 번호 0~3을 지정합니다.

기본값

항목의 인벤토리를 표시할 슬롯을 지정하지 않으면 모든 모듈(전원 공급 디바이스 포함)의 인벤토리 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	—	• 예
사용자 EXEC	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	사소한 편집 내용이 변경되었습니다.
8.4(2)	SSP에 대한 출력이 추가되었습니다. 또한 이중 SSP 설치에 대한 지원이 추가되었습니다.
8.6(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X에 대한 출력(섀시, 예비 전원 공급 디바이스 및 I/O 확장 카드)이 추가되었습니다.
9.1(1)	ASA CX 모듈에 대한 출력이 추가되었습니다.

사용 지침

show inventory 명령은 각 Cisco 제품에 대한 인벤토리 정보를 검색하여 UDI 형식으로 표시합니다. 이는 PID(Product Identifier: 제품 식별자), VID(Version Identifier: 버전 식별자) 및 SN(Serial Number: 일련 번호)이라는 세 가지 개별 데이터 요소의 조합입니다.

PID는 제품을 주문할 수 있는 이름이며, 이전에는 "Product Name" 또는 "Part Number"이라고 했습니다. 이는 정확한 교체용 부품을 주문하는 데 사용하는 식별자입니다.

VID는 제품의 버전입니다. 제품이 수정된 경우 제품 변경 고지에 적용되는 Telcordia GR-209-CORE에서 파생된 엄격한 프로세스에 따라 VID가 증가합니다.

SN은 공급업체 고유의 제품 직렬화입니다. 제조된 각 제품에는 공장에서 할당된 고유한 일련 번호가 있으며, 이는 현장에서 변경할 수 없습니다. 일련 번호는 제품의 특정한 개별 인스턴스를 식별하는 방법입니다. 디바이스의 구성 요소마다 일련 번호 길이가 다를 수 있습니다.

UDI는 각 제품을 하나의 엔터티로 참조합니다. 섀시와 같은 일부 엔터티에는 슬롯과 같은 하위 엔터티가 있습니다. 각 엔티티는 Cisco 엔터티를 기준으로 계층적으로 정렬된 논리적 순서의 프레젠테이션에서 별도의 줄에 표시됩니다.

show inventory 명령은 네트워킹 디바이스에 설치된 PID가 할당된 Cisco 엔터티 목록을 표시하는 옵션 없이 사용됩니다.

Cisco 엔터티에 PID가 할당되지 않은 이 엔터티는 검색되거나 표시되지 않습니다.

참고 SSP 두 개가 동일한 섀시에 설치된 경우 모듈 번호는 섀시에서 해당 모듈의 실제 위치를 나타냅니다. 섀시 마스터는 항상 슬롯 0에 설치된 SSP입니다. SSP가 연결된 센서만 출력에 표시됩니다.

출력에서 *module*이라는 용어는 물리적 슬롯과 같습니다. SSP 자체에 대한 설명에서는 물리적 슬롯 0에 설치된 경우 module: 0, 그렇지 않은 경우 module: 1이 출력에 포함됩니다. 대상 SSP가 섀시 마스터인 경우에는 **show inventory** 명령 출력에 전원 공급 디바이스 및/또는 냉각 팬이 포함됩니다. 그렇지 않은 경우 이러한 구성 요소는 생략됩니다.

ASA 5500-X Series의 경우 하드웨어 제한으로 인해 일련 번호가 표시되지 않을 수 있습니다. 이러한 모델의 PCI-E I/O(NIC) 옵션 카드는 두 가지 유형뿐이지만 해당 UDI 표시에는 섀시 유형에 따라 6개의 출력이 표시될 수 있습니다. 이는 지정된 섀시에 따라 사용되는 PCI-E 브래킷 어셈블리가 다르기 때문입니다. 다음 예에서는 각 PCI-E I/O 카드 어셈블리에 대한 예상 출력을 보여 줍니다. 예를 들어 Silicom SFP NIC 카드가 검색된 경우 UDI 표시는 해당 카드가 설치된 디바이스에 따라 결정됩니다. VID 및 S/N 값은 전자적으로 저장되지 않으므로 N/A입니다.

ASA 5512-X 또는 5515-X에 설치된 6포트 SFP 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

ASA 5525-X에 설치된 6포트 SFP 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

ASA 5545-X 또는 5555-X에 설치된 6포트 SFP 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

ASA 5512-X 또는 5515-X에 설치된 6포트 구리 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

ASA 5525-X에 설치된 6포트 구리 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

ASA 5545-X 또는 5555-X에 설치된 6포트 구리 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

예

다음은 키워드 또는 인수 없이 실행된 **show inventory** 명령의 샘플 출력입니다. 이 출력 샘플은 ASA CX 모듈에 사용되는 저장 디바이스를 포함하여 ASA에 설치된 PID가 할당된 Cisco 엔터티 목록을 표시합니다.

```
ciscoasa> show inventory
Name: "Chassis", DESCR: "ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5555            , VID: V01     , SN: FGL170441BU

Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC         , VID: N/A     , SN: 2CS1AX

Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A                , VID: N/A     , SN: MXA174201RR
```

다음 예에서는 이중 SSP 설치의 섀시 마스터에 대해 실행된 **show inventory** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show inventory
Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-40 w 6GE,4 SFP+"
PID: ASA5585-SSP-40     , VID: V01     , SN: JAF1436ACLJ

Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585            , VID: V01     , SN: 123456789AB

Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN        , VID: V01     , SN: POG1434000G

Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC     , VID: V01     , SN: POG1434002K
```

표 7-9에는 화면에 표시되는 필드에 대한 설명이 나와 있습니다.

표 7-9 show inventory에 대한 필드 설명

필드	설명
Name	Cisco 엔터티에 할당된 물리적 이름(텍스트 문자열)입니다. 예를 들어 디바이스의 물리적 구성요소 명명 구문에 따라 콘솔, SSP 또는 “1”과 같은 간단한 구성 요소 번호(포트 또는 모듈 번호)일 수 있습니다. RFC 2737의 entPhysicalName MIB 변수와 같습니다.
DESCR	개체를 분류하는 Cisco 엔터티에 대한 물리적 설명입니다. RFC 2737의 entPhysicalDesc MIB 변수와 같습니다.
PID	엔티티 제품 식별자입니다. RFC 2737의 entPhysicalModelName MIB 변수와 같습니다.
VID	엔터티 버전 식별자입니다. RFC 2737의 entPhysicalHardwareRev MIB 변수와 같습니다.
SN	엔터티 일련 번호입니다. RFC 2737의 entPhysicalSerialNum MIB 변수와 같습니다.

관련 명령

명령	설명
show diag	네트워킹 디바이스의 컨트롤러, 인터페이스 프로세서 및 포트 어댑터에 대해 진단 정보를 표시합니다.
show tech-support	문제를 보고할 때 라우터에 대한 일반적인 정보를 표시합니다.

show ip address

인터페이스 IP 주소 또는 투명 모드의 경우 관리 IP 주소를 보려면 특권 EXEC 모드에서 **show ip address** 명령을 사용합니다.

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

구문 설명

interface_name	(선택 사항) **nameif** 명령으로 설정된 인터페이스 이름을 식별합니다.
mapped_name	(선택 사항) 다중 상황 모드에서 매핑된 이름(**allocate-interface** 명령을 사용하여 할당된 경우)을 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다. 허용되는 값은 **interface** 명령을 참조하십시오.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
vlan *number*	(선택 사항) ASA 5505 Adaptive Security Appliance와 같은 내장형 스위치가 있는 모델에 대한 VLAN 인터페이스를 지정합니다.

기본값

인터페이스를 지정하지 않은 경우 ASA에서 모든 인터페이스 IP 주소를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령에 VLAN 인터페이스에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 고가용성을 구성한 경우 현재 IP 주소와 함께 기본 IP 주소(화면에서는 “System”이라고 함)를 표시합니다. 디바이스가 활성 상태이면 시스템 IP 주소와 현재 IP 주소가 일치합니다. 디바이스가 대기 상태이면 현재 IP 주소에 대기 주소가 표시됩니다.

예

다음은 **show ip address** 명령의 샘플 출력입니다.

```
ciscoasa# show ip address
System IP Addresses:
Interface                Name          IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt          10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside        10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside       209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz           209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface                Name          IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt          10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside        10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside       209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz           209.165.200.225 255.255.255.224   manual
```

표 7-7에는 각 필드에 대한 설명이 나와 있습니다.

표 7-10 show ip 주소 필드

필드	설명
Interface	인터페이스 ID 또는 다중 상황 모드의 경우 매핑된 이름(**allocate-interface** 명령을 사용하여 구성한 경우)입니다.
Name	**nameif** 명령으로 설정된 인터페이스 이름입니다.
IP 주소	인터페이스 IP 주소입니다.
Subnet mask	IP 주소 서브넷 마스크입니다.
Method	인터페이스에서 IP 주소를 수신한 방법입니다. 값은 다음과 같습니다. • unset - 구성된 IP 주소가 없습니다. • manual - 실행 중인 컨피그레이션을 구성했습니다. • CONFIG - 시작 컨피그레이션에서 로드했습니다. • DHCP - DHCP 서버에서 수신했습니다.

관련 명령

명령	설명
allocate-interface	인터페이스 및 하위 인터페이스를 보안 상황에 할당합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
nameif	인터페이스 이름을 설정합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.

show ip address dhcp

인터페이스의 DHCP 임대 또는 서버에 대한 자세한 정보를 보려면 특권 EXEC 모드에서 **show ip address dhcp** 명령을 사용합니다.

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp** {**lease** | **server**}

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp lease** {**proxy** | **server**} {**summary**}

구문 설명

interface_name	**nameif** 명령으로 설정된 인터페이스 이름을 식별합니다.
lease	DHCP 임대에 대한 정보를 표시합니다.
mapped_name	다중 상황 모드에서 매핑된 이름(**allocate-interface** 명령을 사용하여 할당된 경우)을 식별합니다.
physical_interface	인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다. 허용되는 값은 **interface** 명령을 참조하십시오.
proxy	IPL 테이블의 프록시 항목을 표시합니다.
server	IPL 테이블의 서버 항목을 표시합니다.
subinterface	논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
summary	항목에 대한 요약을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드[1]	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

1. Management 0/0 인터페이스 또는 하위 인터페이스에만 사용할 수 있습니다.

명령 기록

릴리스	수정 사항
7.0(1)	새 서버 기능을 수용하기 위해 **lease** 및 **server** 키워드를 포함하도록 이 명령이 변경되었습니다.
7.2(1)	이 명령에 VLAN 인터페이스 및 투명 모드의 Management 0/0 인터페이스 또는 하위 인터페이스에 대한 지원이 추가되었습니다.
9.1(4)	새 서버 기능을 수용하기 위해 **proxy** 및 **summary** 키워드를 포함하도록 이 명령이 변경되었습니다.

사용 지침

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 **show ip address dhcp lease** 명령의 샘플 출력입니다.

```
ciscoasa# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

표 7-11에는 각 필드에 대한 설명이 나와 있습니다.

표 7-11 show ip address dhcp lease 필드

필드	설명
Temp IP Addr	인터페이스에 할당된 IP 주소입니다.
Temp sub net mask	인터페이스에 할당된 서브넷 마스크입니다.
DHCP Lease server	DHCP 서버 주소입니다.
state	다음과 같은 DHCP 임대 상태입니다. • Initial - ASA에서 임대를 획득하는 프로세스를 시작한 초기화 상태입니다. 임대가 끝나거나 임대 협상에 실패한 경우에도 이 상태가 표시됩니다. • Selecting - ASA가 하나 이상의 DHCP 서버에서 DHCPOFFER 메시지를 받아 하나를 선택할 수 있도록 기다리고 있습니다. • Requesting - ASA가 요청을 전송할 서버에서 다시 수신되기를 기다리고 있습니다. • Purging - 클라이언트가 IP 주소를 임대했거나 다른 오류가 발생하여 ASA에서 임대를 제거하는 중입니다. • Bound - ASA가 유효한 임대가 있으며 정상적으로 작동하고 있습니다. • Renewing - ASA가 임대를 갱신하는 중입니다. ASA는 DHCPREQUEST 메시지를 정기적으로 현재 DHCP 서버로 전송하여 응답을 기다립니다. • Rebinding - ASA가 원래 서버에서 임대를 갱신하지 못해 임의의 서버에서 응답을 받거나 임대가 끝날 때까지 DHCPREQUEST 메시지를 보냅니다. • Holddown - ASA가 임대를 제거하는 프로세스를 시작했습니다. • Releasing - ASA에서 IP 주소가 더 이상 필요하지 않음을 나타내는 해제 메시지를 서버에 보냅니다.
DHCP transaction id	클라이언트와 서버에서 요청 메시지를 연결하는 데 사용하기 위해 클라이언트에서 선택한 난수입니다.

표 7-11 show ip address dhcp lease 필드(계속)

필드	설명
Lease	인터페이스에서 이 IP 주소를 사용할 수 있는 기간으로, DHCP 서버에서 지정합니다.
Renewal	인터페이스에서 이 임대를 자동으로 갱신할 때까지의 기간입니다.
Rebind	ASA가 DHCP 서버에 다시 바인딩할 때까지의 기간입니다. 다시 바인딩은 ASA가 원래 DHCP 서버와 통신할 수 없고 임대 시간의 87.5%가 만료된 경우에 발생합니다. 그런 다음 ASA는 DHCP 요청을 브로드캐스트하여 사용 가능한 DHCP 서버에 연결하려고 시도합니다.
Temp default-gateway addr	DHCP 서버에서 제공하는 기본 게이트웨이 주소입니다.
Temp ip static route0	기본 정적 경로입니다.
Next timer fires after	내부 타이머가 트리거되는 시간(초)입니다.
Retry count	ASA에서 임대를 설정하려고 시도하면 이 필드에 ASA에서 DHCP 메시지를 보내려고 시도한 횟수가 표시됩니다. 예를 들어 ASA의 상태가 선택 중이면 ASA에서 검색 메시지를 보낸 횟수가 이 값에 표시됩니다. ASA의 상태가 요청 중이면 ASA에서 요청 메시지를 보낸 횟수가 이 값에 표시됩니다.
Client-ID	서버와의 모든 통신에 사용되는 클라이언트 ID입니다.
Proxy	이 인터페이스가 VPN 클라이언트에 대한 프록시 DHCP 클라이언트인지 여부를 참 또는 거짓으로 지정합니다.
Proxy Network	요청받은 네트워크입니다.
Hostname	클라이언트 호스트 이름입니다.

다음은 **show ip address dhcp server** 명령의 샘플 출력입니다.

```
ciscoasa# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

표 7-12에는 각 필드에 대한 설명이 나와 있습니다.

표 7-12 show ip address dhcp server 필드

필드	설명
DHCP 서버	이 인터페이스가 임대를 얻은 DHCP 서버 주소입니다. 상위 항목(“ANY”)은 기본 서버이며 항상 존재합니다.
Leases	서버에서 얻은 대여 수입니다. 예를 들어 임대 수는 일반적으로 1입니다. 서버에서 VPN용 프록시를 실행 중인 인터페이스에 대한 주소를 제공하는 경우 임대가 여러 개 있을 것입니다.
Offers	서버의 제안 수입니다.
Requests	서버로 전송된 요청 수입니다.
Acks	서버에서 받은 확인 응답 수입니다.
Naks	서버에서 받은 부정적인 확인 응답 수입니다.
Declines	서버에서 받은 거부 수입니다.
Releases	서버로 전송된 임대 수입니다.
Bad	서버에서 받은 불량 패킷 수입니다.
DNS0	DHCP 서버에서 받은 기본 DNS 서버 주소입니다.
DNS1	DHCP 서버에서 받은 보조 DNS 서버 주소입니다.
WINS0	DHCP 서버에서 받은 기본 WINS 서버 주소입니다.
WINS1	DHCP 서버에서 받은 보조 WINS 서버 주소입니다.
Subnet	DHCP 서버에서 받은 서브넷 주소입니다.
DNS Domain	DHCP 서버에서 받은 도메인입니다.

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
ip address dhcp	DHCP 서버에서 IP 주소를 받도록 인터페이스를 설정합니다.
nameif	인터페이스 이름을 설정합니다.
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.
show ip address	인터페이스의 IP 주소를 표시합니다.

show ip address pppoe

PPPoE 연결에 대한 자세한 정보를 보려면 특권 EXEC 모드에서 **show ip address pppoe** 명령을 사용합니다.

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} **pppoe**

구문 설명

interface_name	**nameif** 명령으로 설정된 인터페이스 이름을 식별합니다.
mapped_name	다중 상황 모드에서 매핑된 이름(**allocate-interface** 명령을 사용하여 할당된 경우)을 식별합니다.
physical_interface	인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다. 허용되는 값은 **interface** 명령을 참조하십시오.
subinterface	논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
vlan *number*	(선택 사항) ASA 5505 Adaptive Security Appliance와 같은 내장형 스위치가 있는 모델에 대한 VLAN 인터페이스를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드[1]	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

1. Management 0/0 인터페이스 또는 하위 인터페이스에만 사용할 수 있습니다.

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 **show ip address pppoe** 명령의 샘플 출력입니다.

```
ciscoasa# show ip address outside pppoe
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
ip address ppoe	PPPoE 서버에서 IP 주소를 받도록 인터페이스를 설정합니다.
nameif	인터페이스 이름을 설정합니다.
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.
show ip address	인터페이스의 IP 주소를 표시합니다.

show ip audit count

인터페이스에 감사 정책을 적용할 때 일치하는 서명 수를 표시하려면 특권 EXEC 모드에서 **show ip audit count** 명령을 사용하십시오.

show ip audit count [**global** | **interface** *interface_name*]

구문 설명

global	(기본 값) 모든 인터페이스에 대해 일치하는 항목 수를 표시합니다.
interface *interface_name*	(선택 사항) 특정 인터페이스에 대해 일치하는 항목 수를 표시합니다.

기본값

키워드를 지정하지 않으면 이 명령은 모든 인터페이스에 대해 일치하는 항목을 표시합니다 (**global**).

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

감사 정책을 생성하려면 **ip audit name** 명령을 사용하고, 정책을 적용하고, **ip audit interface** 명령을 사용합니다.

예

다음은 **show ip audit count** 명령의 샘플 출력입니다.

```
ciscoasa# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
```

```
2003 I ICMP Redirect              0
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

관련 명령

명령	설명
clear ip audit count	감사 정책과 일치하는 서명 수를 지웁니다.
ip audit interface	인터페이스에 감사 정책을 할당합니다.
ip audit name	패킷이 공격 서명 또는 정보 서명과 일치할 때 수행할 작업을 지정하는 명명된 감사 정책을 생성합니다.
show running-config ip audit attack	**ip audit attack** 명령에 대한 컨피그레이션을 표시합니다.

show ip verify statistics

유니캐스트 RPF 기능 때문에 끊어진 패킷 수를 표시하려면 특권 EXEC 모드에서 **show ip verify statistics** 명령을 사용하십시오. **ip verify reverse-path** 명령을 사용하여 유니캐스트 RPF를 활성화하십시오.

show ip verify statistics [interface *interface_name*]

구문 설명

interface *interface_name*	(선택 사항) 특정 인터페이스에 대한 통계를 보여줍니다.

기본값

이 명령은 모든 인터페이스에 대한 통계를 보여줍니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show ip verify statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

관련 명령

명령	설명
clear configure ip verify reverse-path	**ip verify reverse-path** 컨피그레이션을 지웁니다
clear ip verify statistics	유니캐스트 RPF 통계를 지웁니다.
ip verify reverse-path	유니캐스트 역방향 경로 전달 기능을 활성화하여 IP 스푸핑을 방지합니다.
show running-config ip verify reverse-path	**ip verify reverse-path** 컨피그레이션을 표시합니다.

show ips

AIP SSM에서 구성된 모든 IPS 가상 센서를 표시하려면 특권 EXEC 모드에서 **show ips** 명령을 사용하십시오.

show ips [**detail**]

구문 설명

detail	(선택 사항) 센서 ID 번호와 이름이 표시됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

다중 상황 모드에서, 시스템 실행 공간에서 이 명령을 입력하면 모든 가상 센서가 표시됩니다. 하지만 상황 실행 공간의 해당 상황에 할당된 가상 센서만 표시됩니다. 상황에 가상 센서를 할당하는 방법은 **allocate-ips** 명령을 참조하십시오.

가상 센서는 IPS 버전 6.0 이상에서 사용할 수 있습니다.

예

다음은 **show ips** 명령의 샘플 출력입니다.

```
ciscoasa# show ips
Sensor name
------------
ips1
ips2
```

다음은 **show ips detail** 명령의 샘플 출력입니다.

```
ciscoasa# show ips detail
Sensor name              Sensor ID
------------             ---------
ips1                     1
ips2                     2
```

관련 명령

명령	설명
allocate-ips	보안 상황에 가상 센서를 할당합니다.
ips	트래픽을 AIP SSM(으)로 우회시킵니다.

show ipsec sa

IPsec SA 목록을 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show ipsec sa** 명령을 사용합니다. 이 명령어의 대체 양식인 **show crypto ipsec sa**를 사용해도 됩니다.

show ipsec sa [**assigned-address** *hostname or IP address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

구문 설명

assigned-address	(선택 사항) 지정된 호스트 이름 또는 IP 주소에 대한 IPsec SA를 표시합니다.
detail	(선택 사항) 표시된 항목에 대한 자세한 오류 정보를 표시합니다.
entry	(선택 사항) 피어 주소별로 정렬된 IPsec SA를 표시합니다.
identity	(선택 사항) ESP를 포함하지 않고 ID별로 정렬된 IPsec SA를 표시합니다. 이는 축소된 형식입니다.
inactive	(선택 사항) 트래픽을 전달할 수 없는 IPsec SA를 표시합니다.
map *map-name*	(선택 사항) 지정된 암호화 맵에 대한 IPsec SA를 표시합니다.
peer *peer-addr*	(선택 사항) 지정된 피어 IP 주소에 대한 IPsec SA를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	OSPFv3 및 여러 상황 모드에 대한 지원이 추가되었습니다.
9.1(4)	IKEv2 이중 트래픽을 수행하면 할당된 IPv6 주소가 반영되고 GRE 전송 모드 보안 연계를 표시하도록 출력이 업데이트되었습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예는 할당된 IPv6 주소와 전송 모드 및 GRE 캡슐화 표시를 포함하여 IPsec SA를 표시합니다.

```
ciscoasa(config)# sho ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

전역 설정 모드에서 입력한 다음 예는 터널을 OSPFv3으로 식별하는 데 사용 중인 설정을 포함하여 IPsec SA를 표시합니다.

```
ciscoasa(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
```

```
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

참고 조각화 통계는 IPsec SA 정책에 IPsec 처리 전 조각화가 발생하도록 규정된 경우 사전 조각화 통계입니다. 사후 조각화 통계는 SA 정책에 IPsec 처리 후 조각화가 발생하도록 규정된 경우에 표시됩니다.

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 def라는 암호화 맵에 대한 IPsec SA를 표시합니다.

```
ciscoasa(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
```

```
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 키워드 **entry**에 대한 IPsec SA를 보여 줍니다.

```
ciscoasa(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
```

```
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 키워드 **entry detail**에 대한 IPsec SA를 보여줍니다.

```
ciscoasa(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
```

```
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

다음 예에서는 키워드 **identity**에 대한 IPsec SA를 보여 줍니다.

```
ciscoasa(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

다음 예에서는 키워드 **identity** 및 **detail**에 대한 IPsec SA를 보여 줍니다.

```
ciscoasa(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

다음 예에서는 IPv6 할당 주소를 기반으로 IPSec SA를 표시합니다.

```
ciscoasa(config)# sho ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0      #TFC
rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35

      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show ipsec sa summary

IPsec SA 요약을 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show ipsec sa summary** 명령을 사용합니다.

show ipsec sa summary

구문 설명

이 명령에는 인수 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 아래의 연결 유형별로 IPsec SA의 요약을 표시합니다.

- IPSec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN load balancing

```
ciscoasa(config)# show ipsec sa summary

Current IPsec SA's:             Peak IPsec SA's:
IPsec            :     2          Peak Concurrent SA  :    14
IPsec over UDP   :     2          Peak Concurrent L2L :     0
IPsec over NAT-T :     4          Peak Concurrent RA  :    14
IPsec over TCP   :     6
IPsec VPN LB     :     0
Total            :    14
ciscoasa(config)#
```

관련 명령

명령	설명
clear ipsec sa	IPsec SA를 모두 제거하거나 특정 파라미터를 기반으로 제거합니다.
show ipsec sa	IPsec SA 목록을 표시합니다.
show ipsec stats	IPsec 통계 목록을 표시합니다.

show ipsec stats

IPsec 통계 목록을 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show ipsec stats** 명령을 사용합니다.

show ipsec stats

구문 설명

이 명령에는 키워드 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	IPsec 하위 시스템과 함께 ESPv3 통계가 표시되며, 여러 상황 모드에 대한 지원이 추가되었습니다.

사용 지침

다음 표에는 출력 항목의 의미가 설명되어 있습니다.

출력	설명
IPsec Global Statistics	이 섹션은 ASA에서 지원하는 총 IPsec 터널 수와 관계가 있습니다.
Active tunnels	현재 연결된 IPsec 터널 수 입니다.
Previous tunnels	활성 상태인 터널을 포함하여 연결된 IPsec 터널의 수입니다.
Inbound	이 섹션은 IPsec 터널을 통해 받은 인바운드 암호화 트래픽과 관계가 있습니다.
Bytes	수신된 암호화 트래픽의 바이트 수입니다.
Decompressed bytes	해당하는 경우 압축을 해제한 후에 수신된 암호화 트래픽의 바이트 수입니다. 압축이 활성화되지 않은 경우에는 이 바이트 수가 이전 바이트 수와 항상 같아야 합니다.
Packets	수신된 암호화 IPsec 패킷의 수입니다.
Dropped packets	수신되었지만 오류 때문에 끊어진 암호화 IPsec 패킷의 수입니다.

출력(계속)	설명(계속)
Replay failures	수신된 암호화 IPsec 패킷에서 감지된 재전송 방지 실패 횟수입니다.
Authentications	수신된 암호화 IPsec 패킷에서 성공적으로 수행된 인증 횟수입니다.
Authentication failures	수신된 암호화 IPsec 패킷에서 감지된 인증 실패 횟수입니다.
Decryptions	수신된 암호화 IPsec 패킷에서 성공적으로 수행된 암호 해독 횟수입니다.
Decryption failures	수신된 암호화 IPsec 패킷에서 감지된 암호 해독 실패 횟수입니다.
Decapsulated fragments needing reassembly	다시 어셈블할 IP 조각이 포함된 암호 해독 IPsec 패킷의 수입니다.
Outbound	이 섹션은 IPsec 트래픽을 통해 전송할 아웃바운드 일반 텍스트 트래픽과 관계가 있습니다.
Bytes	암호화하여 IPsec 터널을 통해 전송할 일반 텍스트 트래픽의 바이트 수입니다.
Uncompressed bytes	암호화하여 IPsec 터널을 통해 전송할 압축되지 않은 일반 텍스트 트래픽의 바이트 수입니다. 압축이 활성화되지 않은 경우에는 이 바이트 수가 이전 바이트 수와 항상 같아야 합니다.
Packets	암호화하여 IPsec 터널을 통해 전송할 일반 패킷의 수입니다.
Dropped packets	오류 때문에 끊어였으며 암호화하여 IPsec 터널을 통해 전송할 일반 텍스트 패킷의 수입니다.
Authentications	IPsec 터널을 통해 전송할 패킷에서 수행된 인증 횟수입니다.
Authentication failures	IPsec 터널을 통해 전송할 패킷에서 감지된 인증 실패 횟수입니다.
Encryptions	IPsec 터널을 통해 전송할 패킷에서 수행된 암호화 횟수입니다.
Encryption failures	IPsec 터널을 통해 전송할 패킷에서 감지된 암호화 실패 횟수입니다.
Fragmentation successes	아웃바운드 IPsec 패킷 전송 작업의 일부로 수행된 조각화 작업 횟수입니다.
Pre-fragmentation successes	아웃바운드 IPsec 패킷 전송 작업의 일부로 수행된 사전 조각화 작업 횟수입니다. 사전 조각화는 일반 텍스트 패킷이 암호화되어 하나 이상의 IPsec패킷으로 캡슐화되기 전에 발생합니다.
Post-fragmentation successes	아웃바운드 IPsec 패킷 전송 작업의 일부로 수행된 사전 조각화 작업 횟수입니다. 사후 조각화는 일반 텍스트 패킷이 암호화되어 IPsec 패킷으로 캡슐화된 후에 발생하며, 그 결과로 여러 IP 조각이 생깁니다. 암호 해독하려면 이러한 조각을 다시 어셈블해야 합니다.
Fragmentation failures	아웃바운드 IPsec 패킷 변형 중에 발생한 조각화 실패 횟수입니다.
Pre-fragmentation failures	아웃바운드 IPsec 패킷 변형 중에 발생한 사전 조각화 실패 횟수입니다. 사전 조각화는 일반 텍스트 패킷이 암호화되어 하나 이상의 IPsec패킷으로 캡슐화되기 전에 발생합니다.

출력(계속)	설명(계속)
Post-fragmentation failure	아웃바운드 IPsec 패킷 변형 중에 발생한 사후 조각화 실패 횟수입니다. 사후 조각화는 일반 텍스트 패킷이 암호화되어 IPsec 패킷으로 캡슐화된 후에 발생하며, 그 결과로 여러 IP 조각이 생깁니다. 암호 해독하려면 이러한 조각을 다시 어셈블해야 합니다.
Fragments created	IPsec 변형의 일부로 생성된 조각의 수입니다.
PMTUs sent	IPsec 시스템에서 보낸 경로 MTU 메시지의 수입니다. IPsec에서는 너무 커서 캡슐화 후에 IPsec 터널을 통해 전송할 수 없는 패킷을 보내는 내부 호스트에 PMTU 메시지를 보냅니다. PMTU 메시지는 IPsec 터널을 통해 전송할 수 있도록 호스트에 MTU를 낮추고 더 작은 패킷을 보내라는 요청입니다.
PMTUs recvd	IPsec 시스템에서 받은 경로 MTU 메시지의 수입니다. 터널을 통해 보내는 패킷이 너무 커서 해당 네트워크 요소를 우회할 수 없는 경우 IPsec이 다운스트림 네트워크 요소로부터 경로 MTU 메시지를 수신합니다. 경로 MTU 메시지를 받으면 IPsec은 일반적으로 터널 MTU를 낮춥니다.
Protocol failures	수신된 IPsec 패킷 중 형식이 잘못된 패킷의 수입니다.
Missing SA failures	요청된 IPsec 작업 중 지정된 IPsec 보안 연계가 없는 IPsec 작업의 수입니다.
System capacity failures	IPsec 시스템 용량이 데이터 속도를 지원할 만큼 높지 않아서 완료할 수 없는 IPsec 작업의 수입니다.

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 IPsec 통계를 표시합니다.

```
ciscoasa(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
```

```
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
ciscoasa(config)#
```

관련 명령

명령	설명
clear ipsec sa	지정된 파라미터를 기반으로 IPsec SA 또는 카운터를 지웁니다.
crypto ipsec transform-set	변형 집합을 정의합니다.
show ipsec sa	지정된 파라미터를 기반으로 IPsec SA를 표시합니다.
show ipsec sa summary	IPsec SA 요약을 표시합니다.

8 장

show ipv6 access-list through show ipv6 traffic 명령

show ipv6 access-list

IPv6 액세스 목록을 표시하려면 특권 EXEC 모드에서 **show ipv6 access-list** 명령을 사용합니다. IPv6 액세스 목록에 따라 ASA를 통과할 수 있는 IPv6 트래픽이 결정됩니다.

show ipv6 access-list [*id* [*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*]]

구문 설명

any	(선택 사항) IPv6 접두사 ::/0의 약어입니다.
host *source-ipv6-address*	(선택 사항) 특정 호스트의 IPv6 주소입니다. 제공된 경우 지정된 호스트에 대한 액세스 규칙만 표시됩니다.
id	(선택 사항) 액세스 목록 이름입니다. 제공된 경우 지정된 액세스 목록만 표시됩니다.
source-ipv6-prefix /*prefix-length*	(선택 사항) IPv6 네트워크 주소 및 접두사입니다. 제공된 경우 지정된 IPv6 네트워크에 대한 액세스 규칙만 표시됩니다.

기본값

모든 IPv6 액세스 목록을 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show ipv6 access-list 명령은 IPv6에 특정하다는 점을 제외하고는 **show ip access-list** 명령과 유사한 출력을 제공합니다.

예

다음은 **show ipv6 access-list** 명령의 샘플 출력입니다. inbound, tcptraffic 및 outbound라는 IPv6 액세스 목록을 표시합니다.

```
ciscoasa# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
```

```
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

관련 명령

명령	설명
ipv6 access-list	IPv6 액세스 목록을 생성합니다.

show ipv6 dhcprelay binding

릴레이 에이전트가 생성한 릴레이 바인딩 항목을 표시하려면 특권 EXEC 모드에서 **show ipv6 dhcprelay binding** 명령을 사용합니다.

show ipv6 dhcprelay binding

구문 설명

이 명령에는 키워드 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show ipv6 dhcprelay binding 명령을 사용하면 릴레이 에이전트가 생성한 릴레이 바인딩 항목을 확인할 수 있습니다.

예

다음은 **show ipv6 dhcprelay binding** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
60 seconds.

There will be limit of 1000 bindings for each context.
```

관련 명령

명령	설명
show ipv6 dhcprelay statistics	IPv6 DHCP 릴레이 에이전트 정보를 표시합니다.

show ipv6 dhcprelay statistics

IPv6 DHCP 릴레이 에이전트 통계를 표시하려면 특권 EXEC 모드에서 **show ipv6 dhcprelay statistics** 명령을 사용합니다.

show ipv6 dhcprelay statistics

구문 설명

이 명령에는 키워드 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show ipv6 dhcprelay statistics 명령을 사용하면 IPv6 DHCP 릴레이 에이전트 정보를 볼 수 있습니다.

예

다음은 **show ipv6 dhcprelay statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                    1
  ADVERTISE                                  2
  REQUEST                                    1
  CONFIRM                                    1
  RENEW                                    496
  REBIND                                     0
  REPLY                                    498
  RELEASE                                    0
  DECLINE                                    0
  RECONFIGURE                                0
  INFORMATION-REQUEST                        0
  RELAY-FORWARD                            499
  RELAY-REPLY                              500

Relay Errors:
  Malformed message:                         0
  Block allocation/duplication failures:     0
  Hop count limit exceeded:                  0
  Forward binding creation failures:         0
```

```
  Reply binding lookup failures:                0
  No output route:                              0
  Conflict relay server route:                  0
  Failed to add server NP rule:                 0
  Unit or context is not active:                0

Total Relay Bindings Created:                 498
```

관련 명령

명령	설명
show ipv6 dhcprelay binding	릴레이 에이전트가 생성한 릴레이 바인딩 항목을 표시합니다.

show ipv6 interface

IPv6에 대해 구성된 인터페이스의 상태를 표시하려면 특권 EXEC 모드에서 **show ipv6 interface** 명령을 사용합니다.

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

구문 설명

brief	각 인터페이스의 IPv6 상태 및 컨피그레이션에 대한 간략한 요약을 표시합니다.
if_name	(선택 사항) **nameif** 명령에 의해 지정된 내부 또는 외부 인터페이스 이름입니다. 지정된 인터페이스의 상태 및 컨피그레이션이 표시됩니다.
prefix	(선택 사항) 로컬 IPv6 접두사 풀에서 생성된 접두사입니다. 접두사는 IPv6 주소의 네트워크 부분입니다.

기본값

모든 IPv6 인터페이스를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show ipv6 interface 명령은 IPv6에 특정하다는 점을 제외하고는 **show interface** 명령과 유사한 출력을 제공합니다. 인터페이스 하드웨어를 사용할 수 있는 경우 인터페이스가 *up*으로 표시됩니다. 인터페이스에서 양방향 통신을 제공할 수 있는 경우 회선 프로토콜이 *up*으로 표시됩니다.

인터페이스 이름을 지정하지 않으면 모든 IPv6 인터페이스에 대한 정보가 표시됩니다. 인터페이스 이름을 지정하면 지정된 인터페이스에 대한 정보가 표시됩니다.

예

다음은 **show ipv6 interface** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

다음은 **brief** 키워드와 함께 입력한 경우 **show ipv6 interface** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

다음은 **show ipv6 interface** 명령의 샘플 출력입니다. 주소에서 접두사를 생성한 인터페이스의 특성을 표시합니다.

```
ciscoasa# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 mld traffic

MLD(Multicast Listener Discovery) 트래픽 카운터 정보를 표시하려면 특권 EXEC 모드에서 **show ipv6 mld traffic** 명령을 사용합니다.

show ipv6 mld traffic

구문 설명

이 명령에는 키워드 또는 변수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(4)	이 명령이 도입되었습니다.

사용 지침

show ipv6 mld traffic을 사용하면 필요한 개수의 MLD 메시지가 수신 및 전송되었는지 확인할 수 있습니다.

show ipv6 mld traffic 명령에서 제공되는 정보는 다음과 같습니다.

- Elapsed time since counters cleared - 카운터가 지워진 후 경과한 시간입니다.
- Valid MLD Packets - 수신 및 전송된 유효한 MLD 패킷 수입니다.
- Queries - 수신 및 전송된 유효한 쿼리 수입니다.
- Reports - 수신 및 전송된 유효한 보고서 수입니다.
- Leaves - 수신 및 전송된 유효한 리프 수입니다.
- Mtraee packets - 수신 및 전송된 멀티캐스트 추적 패킷 수입니다.
- Errors - 발생한 오류의 유형 및 개수입니다.

예

다음은 **show ipv6 mld traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                  Received           Sent
Valid MLD Packets  1                  3
Queries            1                  0
Reports            0                  3
Leaves             0                  0
Mtrace packets     0              0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

관련 명령

명령	설명
clear ipv6 mld traffic	모든 MLD 트래픽 카운터를 재설정합니다.

show ipv6 neighbor

IPv6 네이버 검색 캐시 정보를 표시하려면 특권 EXEC 모드에서 **show ipv6 neighbor** 명령을 사용합니다.

show ipv6 neighbor [*if_name* | *address*]

구문 설명

address	(선택 사항) 제공된 IPv6 주소에 대한 네이버 검색 캐시 정보만 표시합니다.
if_name	(선택 사항) **nameif** 명령만으로 구성된 대로 제공된 인터페이스 이름에 대한 캐시 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show ipv6 neighbor 명령에서 제공되는 정보는 다음과 같습니다.

- IPv6 Address - 네이버 또는 인터페이스의 IPv6 주소입니다.
- Age - 주소가 연결할 수 있는 것으로 확인된 이후에 경과한 시간(분)입니다. 하이픈(-)은 정적 항목을 나타냅니다.
- Link-layer Addr - MAC 주소입니다. 주소를 알 수 없는 경우 하이픈(-)이 표시됩니다.
- State - 네이버 캐시 항목의 상태입니다.

참고 연결 가능성 감지는 IPv6 네이버 검색 캐시의 정적 항목에는 적용되지 않습니다 . 따라서 INCMP(불완전) 및 REACH(연결 가능) 상태의 설명이 동적 캐시 항목과 정적 항목에 대해 서로 다릅니다 .

다음은 IPv6 네이버 검색 캐시의 동적 항목에 대한 가능한 상태입니다.

- INCMP - (불완전) 항목에 대한 주소 확인을 수행하는 중입니다. 네이버 요청 메시지가 대상의 요청된 노드 멀티캐스트 주소로 전송되었지만 해당 네이버 알림 메시지가 아직 수신되지 않았습니다.
- REACH - (연결 가능) 지난 ReachableTime 밀리초 이내에 네이버의 정방향 경로가 올바르게 작동한다는 긍정적인 확인이 수신되었습니다. REACH 상태에 있는 동안 디바이스는 패킷이 전송될 때 특별한 작업을 수행하지 않습니다.
- STALE - 정방향 경로가 올바르게 작동한다는 긍정적인 확인이 마지막으로 수신된 후 ReachableTime 밀리초보다 많은 시간이 경과했습니다. STALE 상태에 있는 동안 디바이스는 패킷이 전송될 때까지 아무 작업도 수행하지 않습니다.
- DELAY - 정방향 경로가 올바르게 작동한다는 긍정적인 확인이 마지막으로 수신된 후 ReachableTime 밀리초보다 많은 시간이 경과했습니다. 패킷이 지난 DELAY_FIRST_PROBE_TIME 초 이내에 전송되었습니다. DELAY 상태로 전환된 후 DELAY_FIRST_PROBE_TIME 초 이내에 연결 가능성 확인이 수신되지 않으면 네이버 요청 메시지를 보내고 상태를 PROBE로 변경하십시오.
- PROBE - 연결 가능성 확인이 수신될 때까지 RetransTimer 밀리초마다 네이버 요청 메시지를 다시 보내 연결 가능성 확인을 적극적으로 요청합니다.
- ???? - 알 수 없는 상태입니다.

다음은 IPv6 네이버 검색 캐시의 정적 항목에 대한 가능한 상태입니다.

- INCMP - (불완전) 이 항목에 대한 인터페이스의 작동이 중지되었습니다.
- REACH - (연결 가능) 이 항목에 대한 인터페이스가 작동합니다.

- Interface

  주소에 연결할 수 있는 인터페이스입니다.

예

다음은 인터페이스와 함께 입력한 경우 **show ipv6 neighbor** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

다음은 IPv6 주소와 함께 입력한 경우 **show ipv6 neighbor** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

관련 명령

명령	설명
clear ipv6 neighbors	IPv6 네이버 검색 캐시에서 정적 항목을 제외한 모든 항목을 삭제합니다.
ipv6 neighbor	IPv6 네이버 검색 캐시에서 정적 항목을 구성합니다.

show ipv6 ospf

OSPFv3 라우팅 프로세스에 대한 일반적인 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show ipv6 ospf** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*]

구문 설명

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPFv3 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show ipv6 ospf 명령은 다음 설정을 나열합니다.

- 이벤트 로깅
- 라우터 유형
- 재배포 경로 유형
- SPF 일정 지연
- 연속된 두 SPF 사이의 보류 시간
- 연속된 두 SPF 사이의 대기 시간
- 최소 LSA 간격
- 최소 LSA 도착

예

다음은 **show ipv6 ospf** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs.
Minimum LSA arrival 1000 secs
```

관련 명령

명령	설명
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.
show ipv6 ospf database	특정 라우터의 OSPFv3 데이터베이스와 관련된 정보 목록을 표시합니다.

show ipv6 ospf border-routers

ABR(영역 경계 라우터) 및 ASBR(자동 시스템 경계 라우터)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show ipv6 ospf border-routers** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **border-routers**

구문 설명

process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPFv3 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show ipv6 ospf border-routers 명령은 다음 설정을 나열합니다.

- 영역 간 경로
- 영역 내 경로
- IPv6 주소
- 인터페이스 유형
- 영역 ID
- SPF 번호

예

다음은 **show ipv6 ospf border-routers** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf database	특정 라우터의 OSPFv3 데이터베이스와 관련된 정보 목록을 표시합니다.

show ipv6 ospf database

특정 라우터의 OSPFv3 데이터베이스와 관련된 정보 목록을 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show ipv6 ospf database** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **database** [**external | inter-area prefix | inter-area-router | network | nssa-external | router | area | as | ref-lsa |** [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] **| self-originate**] [**internal**] [**database-summary**]

구문 설명

adv-router *router-id*	(선택 사항) 알리는 라우터의 모든 LSA를 표시합니다. 라우터 ID는 RFC 2740에 문서화된 형식이어야 합니다. 즉, 콜론으로 구분된 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.
area	(선택 사항) 영역 LSA에 대한 정보만 표시합니다.
area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
as	(선택 사항) 알 수 없는 AS(자동 시스템) LSA를 필터링합니다.
database-summary	(선택 사항) 데이터베이스의 각 영역에 대해 존재하는 유형별 LSA 수와 총 LSA 수를 표시합니다.
destination-router-id	(선택 사항) 지정된 대상 라우터에 대한 정보만 표시합니다.
external	(선택 사항) 외부 LSA에 대한 정보만 표시합니다.
interface	(선택 사항) 인터페이스 상황으로 필터링된 LSA에 대한 정보를 표시합니다.
interface-name	(선택 사항) LSA 인터페이스 이름을 지정합니다.
internal	(선택 사항) 내부 LSA에 대한 정보만 표시합니다.
inter-area prefix	(선택 사항) inter-area 접두사를 기반으로 하는 LSA에 대한 정보만 표시합니다.
inter-area router	(선택 사항) 영역 내 라우터 LSA를 기반으로 하는 LSA에 대한 정보만 표시합니다.
link	(선택 사항) 링크 LSA에 대한 정보를 표시합니다. **unknown** 키워드 뒤에 사용된 경우 **link** 키워드는 링크 범위 LSA를 필터링합니다.
link-state-id	(선택 사항) LSA를 구분하는 데 사용되는 정수를 지정합니다. 네트워크 및 링크 LSA에서 링크 상태 ID는 인터페이스 인덱스와 일치합니다.
network	(선택 사항) 네트워크 LSA에 대한 정보를 표시합니다.
nssa-external	(선택 사항) NSSA(Not So Stubby Area) 외부 LSA에 대한 정보만 표시합니다.
prefix *ipv6-prefix*	(선택 사항) 네이버의 링크-로컬 IPv6 주소를 표시합니다. IPv6 접두사는 RFC 2373에 문서화된 형식이어야 합니다. 즉, 콜론으로 구분된 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.
ref-lsa	(선택 사항) 접두사 LSA 유형을 추가로 필터링합니다.
router	(선택 사항) 라우터 LSA에 대한 정보를 표시합니다.
self-originate	(선택 사항) 로컬 라우터에서 자체 시작되는 LSA만 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

다양한 형식의 명령에서 서로 다른 OSPFv3 LSA에 대한 정보를 제공합니다.

예

다음은 **show ipv6 ospf database** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3
            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf events

OSPFv3 내부 이벤트 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show ipv6 ospf events** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **events**

구문 설명

process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 OSPFv3 이벤트 정보를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf events** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,
   Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004, Age
   0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,
   Age 0, Area 10
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
```

```
11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0, Adv-Rtr
50.100.168.192
16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf flood-list

인터페이스로 플러딩되기를 기다리는 OSPFv3 LSA 목록을 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show ipv6 ospf flood-list** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **flood-list** *interface-type interface-number*

구문 설명

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
interface-number	LSA가 플러딩되는 인터페이스 번호를 지정합니다.
interface-type	LSA가 플러딩되는 인터페이스 유형을 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPFv3 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 OSPFv3 패킷 속도 정보를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf flood-list** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf graceful-restart

OSPFv3 정상 재시작에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show ipv6 ospf graceful-restart** 명령을 사용합니다.

show ipv6 ospf graceful-restart

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(1)	이 명령이 도입되었습니다.

예

다음은 **show ipv6 ospf graceful-restart** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.

show ipv6 ospf interface

OSPFv3 관련 인터페이스 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show ipv6 ospf interface** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **interface** [*type-number*] [**brief**]

구문 설명

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
brief	(선택 사항) OSPFv3 인터페이스, 상태, 주소 및 마스크, 라우터의 영역에 대한 간략한 개요 정보를 표시합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.
type-number	(선택 사항) 인터페이스 유형 및 번호를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 OSPFv3 인터페이스, 상태, 주소 및 마스크, 라우터의 영역에 대한 개요 정보를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf interface** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf interface

ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
```

```
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf neighbor

인터페이스별로 OSPFv3 네이버 정보를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show ipv6 ospf neighbor** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

구문 설명

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
detail	(선택 사항) 모든 네이버 정보를 자세히 표시합니다.
interface-type interface-number	(선택 사항) 인터페이스 유형 및 번호를 지정합니다.
neighbor-id	(선택 사항) 네이버 ID를 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 인터페이스별로 OSPFv3 네이버에 대한 자세한 정보를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf neighbor** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf neighbor

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
172.16.4.4       1    FULL/  -        00:00:31    14              POS4/0
172.16.3.3       1    FULL/BDR        00:00:30    3               FastEthernet00
172.16.5.5       1    FULL/  -        00:00:33    13              ATM3/0
```

다음은 **show ipv6 ospf neighbor detail** 명령의 샘플 출력입니다.

```
Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 00:00:33
    Neighbor is up for 00:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 00:00:38
    Neighbor is up for 00:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf request-list

라우터에서 요청된 모든 LSA 목록을 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show ipv6 ospf request-list** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

구문 설명

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
interface	(선택 사항) 이 인터페이스의 라우터가 요청한 모든 LSA 목록을 지정합니다.
interface-neighbor	(선택 사항) 이 네이버에서 이 인터페이스의 라우터가 요청한 모든 LSA 목록을 지정합니다.
neighbor	(선택 사항) 이 네이버에서 라우터가 요청한 모든 LSA 목록을 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 라우터가 요청한 모든 LSA를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf request-list** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf retransmission-list

재전송을 대기 중인 모든 LSA 목록을 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show ipv6 ospf retransmission-list** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

구문 설명

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
interface	(선택 사항) 이 인터페이스에서 재전송을 대기 중인 모든 LSA 목록을 지정합니다.
interface-neighbor	(선택 사항) 이 네이버에서 이 인터페이스에 대해 재전송을 대기 중인 모든 LSA 목록을 지정합니다.
neighbor	(선택 사항) 이 네이버에 대해 재전송을 대기 중인 모든 LSA 목록을 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 재전송을 대기 중인 모든 LSA를 나열할 수 있습니다.

예

다음은 **show ipv6 ospf retransmission-list** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf statistic

여러 OSPFv3 통계를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show ipv6 ospf statistic** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **statistic** [**detail**]

구문 설명

detail	(선택 사항) 트리거 지점을 포함하여 자세한 SPF 정보를 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 SPF가 실행된 횟수, 이유 및 기간을 나열할 수 있습니다.

예

다음은 **show ipv6 ospf statistic** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf 10 statistic detail


Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0            0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
```

```
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0            0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf summary-prefix

OSPFv3 프로세스 중에 구성된 모든 요약 주소 재배포 정보 목록을 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show ipv6 ospf summary-prefix** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **summary-prefix**

구문 설명

process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 OSPFv3 프로세스 중에 구성된 모든 요약 주소 재배포 정보 목록을 표시할 수 있습니다.

예

다음은 **show ipv6 ospf summary-prefix** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf timers

OSPFv3 타이머 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show ipv6 ospf timers** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **timers** [**lsa-group | rate-limit**]

구문 설명

lsa-group	(선택 사항) OSPFv3 LSA 그룹 정보를 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.
rate-limit	(선택 사항) OSPFv3 LSA 속도 제한 정보를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 OSPFv3 프로세스 중에 구성된 LSA 정보를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf timers lsa-group** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged
```

```
            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

다음은 **show ipv6 ospf timers rate-limit** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf timers rate-limit

List of LSAs that are in rate limit Queue
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf traffic

현재 사용 가능한 인터페이스에 대한 OSPFv3 트래픽 관련 통계를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show ipv6 ospf traffic** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **traffic** [*interface_name*]

구문 설명

interface_name	(선택 사항) 인터페이스 이름(예: interface GigabitEthernet0/0)을 지정합니다. 이 옵션을 사용하여 트래픽을 특정 인터페이스로 분리할 수 있습니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 사용 가능한 인터페이스에 대한 OSPFv3 트래픽 관련 정보를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf 10 traffic inside

Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid                  0 0
  RX Hello                 1232 53132
  RX DB des                  27 896
  RX LS req                   3 216
```

```
RX LS upd                      28 2436
RX LS ack                      14 1064
RX Total                     1304 57744

TX Failed                       0 0
TX Hello                      753 32072
TX DB des                      27 1056
TX LS req                       2 92
TX LS upd                       9 1128
TX LS ack                      15 900
TX Total                      806 35248
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf virtual-links

OSPFv3 가상 링크의 파라미터 및 현재 상태를 표시하려면 사용자 EXEC 모드 또는 특권 EXEC 모드에서 **show ipv6 ospf virtual-links** 명령을 사용합니다.

show ipv6 ospf virtual-links

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 OSPFv3 가상 링크의 파라미터 및 현재 상태를 표시할 수 있습니다.

예

다음은 **show ipv6 ospf virtual-links** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

관련 명령

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 route

IPv6 라우팅 테이블의 내용을 표시하려면 특권 EXEC 모드에서 **show ipv6 route** 명령을 사용합니다.

show ipv6 route [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]

구문 설명

cluster	(선택 사항) 클러스터의 IPv6 라우팅 테이블 시퀀스 번호, IPv6 재수렴 타이머 상태 및 IPv6 라우팅 항목 시퀀스 번호를 표시합니다.
failover	(선택 사항) IPv6 라우팅 테이블 시퀀스 번호, IPv6 재수렴 타이머 상태 및 IPv6 라우팅 항목 시퀀스 번호를 표시합니다.
interface	(선택 사항) IPv6 인터페이스 관련 경로를 표시합니다.
ospf	(선택 사항) OSPFv3 경로를 표시합니다.
summary	(선택 사항) IPv6 경로 요약을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	**failover, cluster, ospf, interface** 및 **summary** 키워드에 대한 지원이 추가되었습니다.

사용 지침

show ipv6 route 명령은 정보가 IPv6에 특정하다는 점을 제외하고는 **show route** 명령과 유사한 출력을 제공합니다.

IPv6 라우팅 테이블에 표시되는 정보는 다음과 같습니다.

- Codes - 경로를 파생한 프로토콜을 나타냅니다. 값은 다음과 같습니다.
  - C - 연결됨
  - L - 로컬
  - S - 정적
  - R - RIP 파생됨
  - B - BGP 파생됨
  - I1—ISIS L1 - 통합 IS-IS 수준 1 파생됨
  - I2—ISIS L2 - 통합 IS-IS 수준 2 파생됨
  - IA—ISIS interarea - 통합 IS-IS 영역 내 파생됨

- fe80::/10 - 원격 네트워크의 IPv6 접두사를 나타냅니다.
- [0/0] - 대괄호 안의 첫 번째 숫자는 정보 소스의 관리 영역이고, 두 번째 숫자는 경로에 대한 메트릭입니다.
- via :: - 원격 네트워크에 대한 다음 라우터의 주소를 지정합니다.
- inside - 지정된 네트워크의 다음 라우터에 연결할 수 있는 인터페이스를 지정합니다.

참고 **clustering** 및 **failover** 키워드는 이러한 기능이 ASA에 구성되지 않은 한 표시되지 않습니다.

예

다음은 **show ipv6 route** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

다음은 **show ipv6 route failover** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

다음은 마스터 디바이스에서 실행된 **show ipv6 route cluster** 명령의 샘플 출력입니다.

```
ciscoasa/LB1/master(config)# show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

다음은 역할 변경 중 슬레이브 디바이스에서 실행된 **show ipv6 route cluster** 명령의 샘플 출력입니다.

```
ciscoasa/LB2/slave(config)# cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
ciscoasa/LB2/slave(config)#
ciscoasa/LB2/master(config)#
ciscoasa/LB2/master(config)# show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

관련 명령

명령	설명
debug ipv6 route	IPv6 라우팅 테이블 업데이트 및 경로 캐시 업데이트에 대한 디버깅 메시지를 표시합니다.
ipv6 route	IPv6 라우팅 테이블에 정적 항목을 추가합니다.

show ipv6 routers

연결된 라우터에서 받은 IPv6 라우터 알림 정보를 표시하려면 특권 EXEC 모드에서 **show ipv6 routers** 명령을 사용합니다.

show ipv6 routers [*if_name*]

구문 설명

if_name	(선택 사항) 정보를 표시할 내부 또는 외부 인터페이스 이름(**nameif** 명령에 의해 지정됨)입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

인터페이스 이름을 지정하지 않으면 모든 IPv6 인터페이스에 대한 정보가 표시됩니다. 인터페이스 이름을 지정하면 지정된 인터페이스에 대한 정보가 표시됩니다.

예

다음은 인터페이스 이름 없이 입력한 경우 **show ipv6 routers** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

관련 명령

명령	설명
ipv6 route	IPv6 라우팅 테이블에 정적 항목을 추가합니다.

show ipv6 traffic

IPv6 트래픽에 대한 통계를 표시하려면 특권 EXEC 모드에서 **show ipv6 traffic** 명령을 사용합니다.

show ipv6 traffic

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

clear ipv6 traffic 명령을 사용하여 트래픽 카운터를 지울 수 있습니다.

예

다음은 **show ipv6 traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

관련 명령

명령	설명
clear ipv6 traffic	IPv6 트래픽 카운터를 지웁니다.

9 장

show isakmp ipsec-over-tcp stats through show mroute 명령

show isakmp ipsec-over-tcp stats

IPsec over TCP에 대한 런타임 통계를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show isakmp ipsec-over tcp stats** 명령을 사용합니다.

show isakmp ipsec-over-tcp stats

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
ASAv(1)	**show isakmp ipsec-over-tcp stats** 명령이 도입되었습니다.
7.2(1)	**show isakmp ipsec-over-tcp stats** 명령의 사용이 중단되었습니다. **show crypto isakmp ipsec-over-tcp stats** 명령이 이를 대체합니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

이 명령의 출력에는 다음 필드가 포함됩니다.

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets
- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures

- Checksum errors
- Internal errors

예

글로벌 컨피그레이션 모드에서 실행된 다음 예에서는 ISAKMP 통계를 표시합니다.

```
ciscoasa(config)# show isakmp ipsec-over-tcp stats
Global IPsec over TCP Statistics
--------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
crypto isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show isakmp sa

IKE 런타임 SA 데이터베이스를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show isakmp sa** 명령을 사용합니다.

show isakmp sa [**detail**]

구문 설명

detail	SA 데이터베이스에 대한 자세한 출력을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	**show isakmp sa** 명령이 도입되었습니다.
7.2(1)	이 명령의 사용이 중단되었습니다. **show crypto isakmp sa** 명령이 이를 대체합니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

이 명령의 출력에는 다음 필드가 포함됩니다.

Detail이 지정되지 않은 경우

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail이 지정된 경우

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

예

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 SA 데이터베이스에 대한 자세한 정보를 표시합니다.

```
ciscoasa(config)# show isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

ciscoasa(config)#
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show isakmp stats

런타임 통계를 표시하려면 글로벌 컨피그레이션 모드 또는 특권 EXEC 모드에서 **show isakmp stats** 명령을 사용합니다.

show isakmp stats

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
ASAv(1)	**show isakmp stats** 명령이 도입되었습니다.
7.2(1)	이 명령의 사용이 중단되었습니다. **show crypto isakmp stats** 명령이 이를 대체합니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

각 카운터는 연계된 cikePhase1GW 카운터에 매핑됩니다. 각 카운터에 대한 자세한 내용은 CISCO-IPSEC-FLOW-MONITOR-MIB.my를 참조하십시오.

- Active/Standby Tunnels - cikePhase1GWActiveTunnels
- Previous Tunnels - cikePhase1GWPreviousTunnels
- In Octets - cikePhase1GWInOctets
- In Packets - cikePhase1GWInPkts
- In Drop Packets - cikePhase1GWInDropPkts
- In Notifys - cikePhase1GWInNotifys
- In P2 Exchanges - cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids - cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects - cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests - cikePhase1GWInP2SaDelRequests
- Out Octets - cikePhase1GWOutOctets

- Out Packets - cikePhase1GWOutPkts
- Out Drop Packets - cikePhase1GWOutDropPkts
- Out Notifys - cikePhase1GWOutNotifys
- Out P2 Exchanges - cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids - cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects - cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests - cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels - cikePhase1GWInitTunnels
- Initiator Fails - cikePhase1GWInitTunnelFails
- Responder Fails - cikePhase1GWRespTunnelFails
- System Capacity Fails - cikePhase1GWSysCapFails
- Auth Fails - cikePhase1GWAuthFails
- Decrypt Fails - cikePhase1GWDecryptFails
- Hash Valid Fails - cikePhase1GWHashValidFails
- No Sa Fails - cikePhase1GWNoSaFails

이 명령의 출력에는 다음 필드가 포함됩니다.

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails

- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

예

글로벌 컨피그레이션 모드에서 실행된 다음 예에서는 ISAKMP 통계를 표시합니다.

```
ciscoasa(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show running-config isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show kernel

Linux brctl 유틸리티에서 제공하는 디버깅에 사용할 수 있는 정보를 표시하려면 특권 EXEC 모드에서 **show kernel** 명령을 사용합니다.

show kernel [process | bridge | cgroup-controller | ifconfig | module]

구문 설명

bridge	탭 브리지를 표시합니다.
cgroup-controller	cgroup-controller 통계를 표시합니다.
ifconfig	탭 및 브리지 인터페이스 통계를 표시합니다.
module	설치되고 실행되는 모듈을 표시합니다.
process	ASA에서 실행되는 활성 커널 프로세스의 현재 상태를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.4(1)	**cgroup-controller** 키워드가 추가되었습니다.
8.6(1)	**ifconfig**, **module** 및 **bridge** 키워드가 추가되었습니다.

사용 지침

이 명령은 커널에서 실행되는 여러 프로세스에 대한 통계를 표시합니다.

예

다음 예에서는 **show kernel process** 명령의 출력을 표시합니다.

```
ciscoasa# show kernel process

PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
```

```
 68    1  15  0          0        0 3725824451    S        2 kswapd0
 69    5  20 -5          0        0 3725736671    S        0 aio/0
171    1  16  0     991232       80 3725684979    S        0 init
172  171  19  0     983040      268 3725684979    S        0 rcS
201  172  21  0    1351680      344 3725712932    S        0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S      212 lina
203  202  16  0 1017602048   899932          0    S        0 lina
204  203  15  0 1017602048   899932          0    S        0 lina
205  203  15  0 1017602048   899932 3725712932    S        6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
ciscoasa#
```

표 9-1에는 각 필드에 대한 설명이 나와 있습니다.

표 9-1 show kernel process 필드

필드	설명
PID	프로세스 ID입니다.
PPID	상위 프로세스 ID입니다.
PRI	프로세스의 우선순위입니다.
NI	우선순위 계산에 사용되는 nice 값입니다. 값 범위는 19(nicest)~19(not nice to others)입니다.
VSIZE	가상 메모리 크기(바이트)입니다.
RSS	프로세스의 상주 집합 크기(킬로바이트)입니다.
WCHAN	프로세스가 대기하는 채널입니다.
STAT	프로세스의 상태입니다. • R - 실행 중 • S - 중단 가능한 상태로 대기 중 • D - 중단할 수 없는 디스크 절전 상태로 대기 중 • Z - 좀비 • T - 추적되거나 중지됨(신호에서) • P - 페이징
RUNTIME	프로세스가 사용자 모드 및 커널 모드에서 예약된 지피(Jiffy) 수입니다. 런타임은 utime과 stime의 합계입니다.
COMMAND	프로세스 이름입니다.

다음 예에서는 **show kernel module** 명령의 출력을 표시합니다.

```
ciscoasa# show kernel module

Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
tscsync                 3852  0
```

다음 예에서는 **show kernel ifconfig** 명령의 출력을 표시합니다.

```
ciscoasa# show kernel ifconfig

br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

관련 명령

명령	설명
show module	ASA에 설치된 모듈에 대한 정보를 표시합니다.

show kernel bridge

Linux 브리지, 해당 멤버 포트 및 디버깅에 사용할 수 있는 각 포트에서 학습된 MAC 주소를 표시하려면 특권 EXEC 모드에서 **show kernel bridge** 명령을 사용합니다.

show kernel bridge [**mac-address** *bridge name*]

구문 설명

bridge name	브리지 이름을 표시합니다.
mac-address	각 포트에 연결된 MAC 주소를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 Linux 브리지, 해당 멤버 포트 및 디버깅에 사용할 수 있는 각 포트에서 학습된 MAC 주소(원격 MAC 주소 포함)를 표시합니다.

예

다음 예에서는 **show kernel bridge** 명령의 출력을 표시합니다.

```
ciscoasa# show kernel bridge

bridge name    bridge id        STP enabled interfaces
br0         8000.0e3cd8a8909f    no         tap1
                                tap3
br1        8000.26d29f51a490     no         tap2
                                tap4
                                tap5hostname#
```

다음 예에서는 **show kernel bridge mac-address** 명령의 출력을 표시합니다.

```
ciscoasa# show kernel bridge mac-address br1

port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

관련 명령

명령	설명
show kernel	ASA에 설치된 모듈에 대한 정보를 표시합니다.

show lacp

트래픽 통계, 시스템 식별자 및 네이버 정보와 같은 EtherChannel LACP 정보를 표시하려면 특권 EXEC 모드에서 이 명령을 입력합니다.

show lacp {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

구문 설명

channel_group_number	(선택 사항) EtherChannel 채널 그룹 번호(1~48)를 지정하고, 이 채널 그룹에 대한 정보만 표시합니다.
counters	보내고 받은 LACPDU 및 마커 수에 대한 카운터를 표시합니다.
internal	내부 정보를 표시합니다.
neighbor	네이버 정보를 표시합니다.
sys-id	LACP 시스템 ID를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

예

다음은 **show lacp sys-id** 명령의 샘플 출력입니다.

```
ciscoasa# show lacp sys-id
32768,001c.c4e5.cfee
```

다음은 **show lacp counters** 명령의 샘플 출력입니다.

```
ciscoasa# show lacp counters

              LACPDUs         Marker      Marker Response    LACPDUs
Port        Sent   Recv     Sent   Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 1
Gi3/1       736    728      0      0        0       0         0
Gi3/2       739    730      0      0        0       0         0
Gi3/3       739    732      0      0        0       0         0
```

다음은 **show lacp internal** 명령의 샘플 출력입니다.

```
ciscoasa# show lacp internal
```

```
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d
```

다음은 **show lacp neighbor** 명령의 샘플 출력입니다.

```
ciscoasa# show lacp neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 활성 인터페이스의 최대 수를 지정합니다.
lacp port-priority	채널 그룹의 물리적 인터페이스에 대한 우선순위를 설정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel load-balance	부하 균형 알고리즘을 구성합니다.
port-channel min-bundle	포트-채널 인터페이스를 활성화하는 데 필요한 활성 인터페이스의 최소 수를 지정합니다.
show port-channel	EtherChannel 정보를 자세한 양식과 한 줄 요약 양식으로 표시합니다. 이 명령은 포트 및 포트-채널 정보도 표시합니다.
show port-channel load-balance	지정된 파라미터 집합에 대해 선택된 멤버 인터페이스 및 해시 결과와 함께 포트-채널 부하 균형 정보를 표시합니다.

show lacp cluster

cLACP 시스템 MAC 및 ID를 표시하려면 특권 EXEC 모드에서 **show lacp cluster** 명령을 사용합니다.

show lacp cluster {**system-mac** | **system-id**}

구문 설명

system-mac	시스템 ID와 해당 ID가 자동으로 생성되었는지 또는 수동으로 입력되었는지 표시합니다.
system-id	시스템 ID와 우선순위를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

clacp system-mac 명령을 사용하여 cLACP 시스템 ID 및 우선순위를 설정합니다.

예

다음은 **show lacp cluster system-mac** 명령의 샘플 출력입니다.

```
ciscoasa(cfg-cluster)# show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

다음은 **show lacp cluster system-id** 명령의 샘플 출력입니다.

```
ciscoasa(cfg-cluster)# show lacp cluster system-id
5    ,a300.010a.010a
```

관련 명령

명령	설명
clacp system-mac	cLACP 시스템 ID와 우선순위를 설정합니다.

show license

스마트 라이센싱 상태를 표시하려면 특권 EXEC 모드에서 **show license** 명령을 사용합니다.

참고 이 기능은 ASAv에서만 지원됩니다.

show license [all | entitlement | cert | pool | registration | features

구문 설명

all	스마트 라이센싱 상태, 스마트 에이전트 버전, UDI 정보, 스마트 에이전트 상태, 글로벌 규정 준수 상태, 자격 상태, 라이센싱 인증서 정보 및 스마트 에이전트 작업 일정을 표시합니다.
entitlement	사용 중인 각 자격, 해당 핸들(즉, 정수 ID), 개수, 태그, 적용 모드(예: 규준 준수, 규정 미준수 등), 버전 및 자격이 요청된 시간에 대한 자세한 정보를 표시합니다.
cert	ID 인증서 내용, 발급된 날짜 및 만료 날짜를 표시합니다.
pool	이 디바이스가 할당된 자격 풀을 표시합니다.
registration	현재 스마트 라이센스 등록 상태를 표시합니다.
features	현재 라이센스를 표시합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

show activation-key 명령은 show license features 명령과 동일한 출력을 제공합니다.

예

다음 예에서는 기본 라이센스만 있는(현재 라이센스 자격이 없음) ASAv를 표시합니다.

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

관련 명령

명령	설명
call-home	Smart Call Home을 구성합니다. 스마트 라이센싱은 Smart Call Home 인프라를 사용합니다.
clear configure license	스마트 라이센싱 컨피그레이션을 지웁니다.
feature tier	스마트 라이센싱에 대한 기능 계층을 설정합니다.
http-proxy	스마트 라이센싱 및 Smart Call Home에 대한 HTTP(S) 프록시를 설정합니다.
license smart	스마트 라이센싱에 대한 라이센스 자격을 요청할 수 있습니다.
license smart deregister	라이센스 기관에서 디바이스의 등록을 해제합니다.
license smart register	라이센스 기관에 디바이스를 등록합니다.
license smart renew	등록 또는 라이센스 자격을 갱신합니다.
service call-home	Smart Call Home을 활성화합니다.
show running-config license	스마트 라이센싱 컨피그레이션을 표시합니다.
throughput level	스마트 라이센싱에 대한 처리량을 설정합니다.

show local-host

로컬 호스트의 네트워크 상태를 표시하려면 특권 EXEC 모드에서 **show local-host** 명령을 사용합니다.

show local-host | include interface [*ip_address*] [**detail**] [**all**][**brief**] [**connection** {**tcp** *start*[-*end*] | **udp** *start*[-*end*] | **embryonic** *start*[-*end*]}] [**zone** [*zone-name*]]

구문 설명

all	(선택 사항) ASA에 연결된 로컬 호스트와 ASA에서 연결된 로컬 호스트를 포함합니다.
brief	(선택 사항) 로컬 호스트에 대한 간략한 정보를 표시합니다.
connection	(선택 사항) 연결 수 및 유형에 따라 세 가지 유형의 필터(TCP, UDP 및 embryonic)를 표시합니다. 이러한 필터를 개별적으로 사용하거나 함께 사용할 수 있습니다.
detail	(선택 사항) 활성 xlate 및 네트워크 연결에 대한 자세한 정보를 포함하여 로컬 호스트 정보의 자세한 네트워크 상태를 표시합니다.
include interface	각 인터페이스에서 사용되는 IP 주소를 지정합니다.
ip_address	(선택 사항) 로컬 호스트 IP 주소를 지정합니다.
zone [*zone_name*]	(선택 사항) 영역별 로컬 호스트를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	호스트 제한이 있는 모델의 경우 이 명령은 이제 외부 인터페이스로 간주되는 인터페이스를 표시합니다.
7.2(4)	출력이 내부 호스트에 대한 연결 수로 필터링되도록 두 가지 새로운 옵션 **connection** 및 **brief**가 **show local-host** 명령에 추가되었습니다.
9.1(2)	원격 분석 기반 알림을 위해 Cisco로 Smart Call Home 정보를 전송하는 명령이 **show local-host**에서 **show local-host	include interface**로 변경되었습니다.
9.3(2)	**zone** 키워드가 추가되었습니다.

사용 지침

show local-host 명령을 사용하여 로컬 호스트의 네트워크 상태를 표시할 수 있습니다. 로컬 호스트는 ASA로 트래픽을 전달하거나 ASA를 통해 트래픽을 전달하는 모든 호스트에 대해 생성됩니다.

이 명령을 사용하여 로컬 호스트에 대한 변환 및 연결 슬롯을 표시할 수 있습니다. 이 명령은 일반 변환 및 연결 상태를 적용할 수 없을 때 **nat 0 access-list** 명령으로 구성된 호스트에 대한 정보를 제공합니다.

또한 연결 제한 값도 표시합니다. 연결 제한이 설정되지 않은 경우에는 값이 0으로 표시되고 제한이 적용되지 않습니다.

라우팅 모드에서는 호스트 제한이 있는 모델의 경우 내부(회사 및 집 영역)에 있는 호스트는 외부(인터넷 영역)와 통신하는 경우에만 제한이 적용됩니다. 인터넷 호스트에는 제한이 적용되지 않습니다. 회사와 집 간의 트래픽을 시작하는 호스트에는 제한이 적용되지 않습니다. 기본 경로와 연결된 인터페이스는 인터넷 인터페이스로 간주됩니다. 기본 경로가 없는 경우에는 모든 인터페이스의 호스트에 제한이 적용됩니다. 투명 모드에서는 최소 개수의 호스트가 있는 인터페이스에 호스트 제한이 적용됩니다.

SYN 공격(TCP 가로채기가 구성됨) 시 **show local-host** 명령 출력에는 가로채기된 연결 수가 사용 개수에 포함됩니다. 이 필드에는 일반적으로 완전히 열려 있는 연결만 표시됩니다.

show local-host 명령 출력에서 **TCP embryonic count to host counter**는 정적 연결을 사용하는 호스트에 대해 최대 원시 제한(TCP 가로채기 워터마크)이 구성된 경우에 사용됩니다. 이 카운터는 다른 호스트에서 호스트에 연결한 총 원시 연결 수를 보여 줍니다. 이 합계가 구성된 최대 제한을 초과하면 호스트에 대한 새 연결에 TCP 가로채기가 적용됩니다.

예

다음은 **show local-host** 명령의 샘플 출력입니다.

```
ciscoasa# show local-host
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 1 active, 2 maximum active, 0 denied
```

다음은 호스트 제한이 있는 ASA에서 실행된 **show local-host** 명령의 샘플 출력입니다.

```
ciscoasa# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

다음은 호스트 제한이 있는 ASA에서 실행된 **show local-host** 명령의 샘플 출력입니다. 그러나 기본 경로가 없으므로 호스트 제한이 모든 인터페이스에 적용됩니다. 기본 경로 또는 경로에서 사용하는 인터페이스가 중단된 경우에는 기본 경로 인터페이스가 감지되지 않을 수 있습니다.

```
ciscoasa# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

다음은 호스트 제한이 없는 ASA에서 실행된 **show local-host** 명령의 샘플 출력입니다.

```
ciscoasa# show local-host
Licensed host limit: Unlimited

Interface c1in: 1 active, 1 maximum active, 0 denied
```

```
Interface c1out: 0 active, 0 maximum active, 0 denied
```

다음 예에서는 로컬 호스트의 네트워크 상태를 보여 줍니다.

```
ciscoasa# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

ciscoasa# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

ciscoasa# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
```

```
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active, 1
maximum active, 0 denied
```

다음 예에서는 최소 4개의 UDP 연결이 있고 TCP 동시 연결 수가 1~10개인 모든 호스트를 보여 줍니다.

```
ciscoasa# show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
        watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
        Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
        10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
        10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
        maximum active, 0 denied
```

다음 예에서는 **brief** 옵션을 사용하여 로컬 호스트 주소 및 연결 카운터를 보여 줍니다.

```
ciscoasa# show local-host connection udp 2
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited
        TCP embryonic count to host = 0
        TCP intercept watermark = unlimited UDP flow count/limit = 4/unlimited
Interface OUTSIDE: 3 active, 5 maximum active, 0 denied
```

다음 예에서는 **brief** 및 **connection** 옵션을 사용할 때의 출력을 보여 줍니다.

```
ciscoasa# show local-host brief
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied

ciscoasa# show local-host connection
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied
```

관련 명령

명령	설명
clear local-host	**show local-host** 명령에서 표시하는 로컬 호스트에서 네트워크 연결을 해제합니다.
nat	네트워크를 전역 IP 주소 풀에 연결합니다.

show logging

버퍼의 로그 및 기타 기록 설정을 표시하려면 특권 EXEC 모드에서 **show logging** 명령을 사용합니다.

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting**]

구문 설명

all	(선택 사항) 모든 syslog 메시지 ID를 사용 여부와 함께 표시합니다.
asdm	(선택 사항) ASDM 기록 버퍼 내용을 표시합니다.
message	(선택 사항) 기본이 아닌 수준에 있는 메시지를 표시합니다. 메시지 수준을 설정하려면 **logging message** 명령을 참고하십시오.
queue	(선택 사항) syslog 메시지 대기열을 표시합니다.
setting	(선택 사항) 기록 버퍼를 표시하지 않고 기록 설정을 표시합니다.
syslog_id	(선택 사항) 표시할 메시지 수를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.0(2)	syslog 서버가 SSL/TLS 연결을 사용하도록 구성되었는지 여부를 나타냅니다.
8.4(1)	**show logging** 명령의 출력에 감사 블록의 현재 상태에 대한 항목이 포함됩니다.

사용 지침

logging buffered 명령을 사용하는 경우 키워드 없이 **show logging** 명령을 실행하면 현재 메시지 버퍼 및 현재 설정이 표시됩니다.

show logging queue 명령을 사용하여 다음을 표시할 수 있습니다.

- 대기열의 메시지 수
- 대기열에 있는 기록된 최대 메시지 수
- 블록 메모리를 사용하여 처리할 수 없어 삭제된 메시지 수
- 트랩과 다른 syslog 메시지에 대한 별도의 대기열

참고 0 은 구성된 대기열 크기에 사용할 수 있는 숫자이며 , 허용되는 최대 대기열 크기를 나타냅니다 . 구성된 대기열 크기가 0 인 경우 **show logging queue** 명령의 출력에는 실제 대기열 크기가 표시됩니다 .

예

다음은 **show logging** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging:disabled
    Debug-trace logging: disabled
    Console logging: level informational, 3962 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 20549 messages logged
        Logging to inside 10.2.5.3 tcp/50001 connected
    Permit-hostdown state
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

참고 유효한 *state* 값은 enabled, disabled, disabled-blocking 및 disabled-not blocking입니다.

다음은 보안 syslog 서버가 구성된 경우 **show logging** 명령의 샘플 출력입니다.

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
ciscoasa(config)# show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

다음은 **show logging queue** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

다음은 **show logging message all** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
```

```
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

관련 명령

명령	설명
logging asdm	ASDM에 대한 기록을 활성화합니다.
logging buffered	버퍼에 대한 기록을 활성화합니다.
logging host	syslog 서버를 정의합니다.
logging message	메시지 수준을 설정하거나 메시지를 비활성화합니다.
logging queue	기록 대기열을 구성합니다.

show logging flow-export-syslogs

정보가 NetFlow에서도 캡처되고 **logging flow-export-syslogs enable | disable** 명령의 영향을 받는 모든 syslog 메시지를 표시하려면 특권 EXEC 모드에서 **show logging flow-export-syslogs** 명령을 사용합니다.

show logging flow-export-syslogs

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.1(1)	이 명령이 도입되었습니다.

사용 지침

logging flow-export syslogs disable 명령을 입력한 후에는 비활성화된 syslog 메시지를 알아야 합니다. 비활성화된 syslog 메시지는 다음과 같습니다.

syslog 메시지	설명
106015	첫 번째 패킷이 SYN 패킷이 아니기 때문에 TCP 흐름이 거부되었습니다.
106023	**access-group** 명령을 통해 인터페이스에 연결된 인그레스 ACL 또는 이그레스 ACL에서 거부된 흐름
106100	ACL에서 허용되거나 거부된 흐름
302013 및 302014	TCP 연결 및 삭제
302015 및 302016	UDP 연결 및 삭제
302017 및 302018	GRE 연결 및 삭제
302020 및 302021	ICMP 연결 및 삭제
313001	ASA에 대한 ICMP 패킷이 거부되었습니다.
313008	ASA에 대한 ICMPv6 패킷이 거부되었습니다.
710003	ASA에 대한 연결 시도가 거부되었습니다.

예

다음은 비활성화할 syslog 메시지를 나열하는 **show logging flow-export-syslogs** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show logging flow-export-syslogs

Syslog ID          Type                 Status
302013           Flow Created          Enabled
302015           Flow Created          Enabled
302017           Flow Created          Enabled
302020           Flow Created          Enabled
302014           Flow Deleted          Enabled
302016           Flow Deleted          Enabled
302018           Flow Deleted          Enabled
302021           Flow Deleted          Enabled
106015           Flow Denied           Enabled
106023           Flow Denied           Enabled
313001           Flow Denied           Enabled
313008           Flow Denied           Enabled
710003           Flow Denied           Enabled
106100           Flow Created/Denied   Enabled
```

관련 명령

명령	설명
flow-export destination *interface-name ipv4-address* | *hostname udp-port*	NetFlow 컬렉터의 IP 주소 또는 호스트 이름과 NetFlow 컬렉터에서 수신 대기하는 UDP 포트를 지정합니다.
flow-export template timeout-rate *minutes*	템플릿 정보가 NetFlow 컬렉터로 전송되는 간격을 제어합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 후의 syslog 메시지 및 NetFlow 데이터와 연계된 syslog 메시지를 활성화합니다.
show flow-export counters	NetFlow에 대한 런타임 카운터 집합을 표시합니다.

show logging rate-limit

허용되지 않는 syslog 메시지를 표시하려면 특권 EXEC 모드에서 **show logging rate-limit** 명령을 사용합니다.

show logging rate-limit

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

정보가 지워진 후에는 호스트에서 연결을 다시 설정할 때까지 더 이상 아무 것도 표시되지 않습니다.

예

다음 예에서는 **show logging rate-limit** 명령의 샘플 출력을 보여 줍니다.

```
ciscoasa(config)# show logging rate-limit
%ASA-7-710005: TCP request discarded from 171.69.39.0/2678 to management:10.89.130.244/443
%ASA-7-711002: Task ran for 27 msec, Process = ssm_mgmt_ifc_poll_thread, PC = 896fcac,
Traceback =
%ASA-7-711002: Task ran for 27 msec, Process = ssm_mgmt_ifc_poll_thread, PC = 896fcac,
Traceback =   0x0807C0FA
%ASA-6-106015: Deny TCP (no connection) from 171.69.39.0/2685 to 10.89.130.244/443 flags
FIN PSH ACK  on interface management
%ASA-7-710005: TCP request discarded from 171.69.39.0/2685 to management:10.89.130.244/443
%ASA-6-302013: Built inbound TCP connection 2116 for management:171.69.39.0/2689
(171.69.39.0/2689) to identity:10.89.130.244/443 (10.89.130.244/443)
%ASA-6-725001: Starting SSL handshake with client management:171.69.39.0/2689 for TLSv1
session.
%ASA-6-725003: SSL client management:171.69.39.0/2689 request to resume previous session.
%ASA-6-725002: Device completed SSL handshake with client management:171.69.39.0/2689
%ASA-6-605005: Login permitted from 171.69.39.0/2689 to management:10.89.130.244/https for
user "enable_15"
%ASA-5-111007: Begin configuration: 171.69.39.0 reading from http [POST]
```

관련 명령

명령	설명
show logging	활성화된 기록 옵션을 표시합니다.

show mac-address-table

MAC 주소 테이블을 표시하려면 특권 EXEC 모드에서 **show mac-address-table** 명령을 사용합니다.

show mac-address-table [*interface_name* | **count** | **static**]

구문 설명

count	(선택 사항) 동적 및 정적 항목의 총 개수를 나열합니다.
interface_name	(선택 사항) MAC 주소 테이블 항목을 확인할 인터페이스 이름을 식별합니다.
static	(선택 사항) 정적 항목만 나열합니다.

기본값

인터페이스를 지정하지 않으면 모든 인터페이스 MAC 주소 항목이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show mac-address-table** 명령의 샘플 출력입니다.

```
ciscoasa# show mac-address-table
interface          mac address       type      Time Left
------------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

다음은 내부 인터페이스에 대한 **show mac-address-table** 명령의 샘플 출력입니다.

```
ciscoasa# show mac-address-table inside
interface          mac address       type      Time Left
------------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

다음은 **show mac-address-table count** 명령의 샘플 출력입니다.

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

관련 명령

명령	설명
firewall transparent	방화벽을 투명 모드로 설정합니다.
mac-address-table aging-time	동적 MAC 주소 항목에 대한 시간 제한을 설정합니다.
mac-address-table static	MAC 주소 테이블에 정적 MAC 주소 항목을 추가합니다.
mac-learn	MAC 주소 학습을 비활성화합니다.

show management-access

관리 액세스용으로 구성된 내부 인터페이스의 이름을 표시하려면 특권 EXEC 모드에서 show management-access 명령을 사용합니다.

show management-access

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

management-access 명령을 사용하면 *mgmt_if*에 지정된 방화벽 인터페이스의 IP 주소를 사용하여 내부 관리 인터페이스를 정의할 수 있습니다. 인터페이스 이름은 **nameif** 명령으로 정의되며, **show interface** 명령의 출력에서 따옴표(" ") 안에 표시됩니다.

예

다음 예에서는 "inside"라는 방화벽 인터페이스를 관리 액세스 인터페이스로 구성하고 결과를 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# management-access inside
ciscoasa(config)# show management-access
management-access inside
```

관련 명령

명령	설명
clear configure management-access	ASA의 관리 액세스용 내부 인터페이스 컨피그레이션을 제거합니다.
management-access	관리 액세스용 내부 인터페이스를 구성합니다.

show mdm-proxy sessions

현재 활성 MDM 프록시 세션을 표시합니다.

show mdm-proxy sessions [checkin | enrollment]

구문 설명

checkin만 지정하면 체크 인 세션만 표시되고, **enrollment**만 지정하면 등록된 세션만 표시됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(1)	이 명령이 도입되었습니다.

관련 명령

명령	설명
mdm-proxy	config-mdm-proxy 모드를 시작하여 MDM 프록시 서비스를 구성합니다.

show mdm-proxy statistics

MDM 프록시 서비스 통계를 표시합니다.

show mdm-proxy statistics

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(1)	이 명령이 도입되었습니다.

예

```
ciscoasa (config)# show mdm-proxy statistics<cr>

MDM proxy statistics:
=====================
Total number of successful MDM enrollments: 1230
Number of active MDM enrollments: 10
Maximum number of simultaneously active MDM enrollments: 90
Minimum duration of an MDM enrollment: 4 seconds
Maximum duration of an MDM enrollment: 25 seconds
Total number of failed MDM enrollments due to authentication failure: 23
Total number of failed MDM enrollments due to SCEP enrollment failure: 28.
Total number of failed MDM enrollments: 61
Total number of successful MDM check-ins: 3167
Number of active MDM check-ins: 26
Maximum number of simultaneously active MDM check-ins: 316
Minimum duration of an MDM check-in: 3 seconds
Maximum duration of an MDM check-in: 21 seconds
Total number of failed MDM check-ins: 118
```

관련 명령

명령	설명
clear mdm-proxy statistics	MDM 프록시 카운터를 지우고 0으로 설정합니다.
mdm-proxy	config-mdm-proxy 모드를 시작하여 MDM 프록시 서비스를 구성합니다.

show memory

운영 체제에 사용 가능한 최대 실제 메모리 및 현재 사용 가능한 메모리에 대한 요약을 표시하려면 특권 EXEC 모드에서 **show memory** 명령을 사용합니다.

[**cluster exec**] **show memory** [**detail**]

구문 설명

cluster exec	(선택 사항) 클러스터링 환경에서 하나의 디바이스에서 **show memory** 명령을 실행하고 나머지 모든 디바이스에서 동시에 이 명령을 실행할 수 있도록 합니다.
detail	(선택 사항) 사용 가능한 시스템 메모리와 할당된 시스템 메모리에 대한 자세한 보기를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	**cluster exec** 옵션이 추가되었습니다.
9.2(1)	ASAv를 지원하도록 VM(가상 머신) 통계가 출력에 추가되었습니다.
9.3(2)	내부 메모리 관리자가 **show memory detail** 명령에서 표준 glibc 라이브러리로 대체되었습니다.

사용 지침

show memory 명령을 사용하여 운영 체제에 사용 가능한 최대 실제 메모리 및 현재 사용 가능한 메모리에 대한 요약을 표시할 수 있습니다. 메모리는 필요에 따라 할당됩니다.

또한 SNMP를 사용하여 **show memory** 명령에서 정보를 표시할 수 있습니다.

show memory binsize 명령과 함께 **show memory detail** 출력을 사용하여 메모리 누수를 디버그할 수 있습니다.

show memory detail 명령 출력은 세 개의 섹션(Summary, DMA Memory 및 HEAP Memory)으로 분할될 수 있습니다. 요약에는 할당된 총 메모리가 표시됩니다. DMA에 연결되거나 예약되지 않은 메모리는 HEAP으로 간주됩니다. Free Memory 값은 HEAP에서 사용되지 않은 메모리입니다. Allocated memory in use 값은 할당된 HEAP 양입니다. HEAP 할당의 분석 결과는 출력의 뒷부분에 표시됩니다. Reserved memory 및 DMA Reserved memory는 서로 다른 시스템 프로세스에서 사용되며, 주로 VPN 서비스에서 사용됩니다.

Free memory는 Free memory heap과 Free memory system의 두 부분으로 나누어집니다. Free memory heap은 glibc heap의 사용 가능한 메모리 양입니다. glibc heap이 요청에 따라 증가 및 감소할 때 free heap memory 양은 시스템에 남아 있는 총 메모리를 나타내지 않습니다. Free memory system은 ASA에 사용 가능한 여유 메모리 양을 나타냅니다.

Reserved memory(DMA)는 DMA 풀용으로 예약된 메모리 양입니다. Memory overhead는 실행 중인 여러 프로세스의 glibc 오버헤드 및 프로세스 오버헤드입니다.

allocated memory statistics total (bytes) 열에 표시된 값은 **show memory detail** 명령 출력의 실제 값(MEMPOOL_GLOBAL_SHARED POOL STATS)을 반영하지 않습니다.

출력에는 크기가 49,152인 블록이 할당된 다음 사용 가능한 풀로 반환되고 크기가 131,072인 다른 블록이 할당된 것으로 표시됩니다. 이 경우 사용 가능한 메모리가 131,072-49,152=81,920바이트 감소한 것으로 생각할 수 있지만 실제로는 100,000바이트 감소한 것입니다(Free memory 줄 참고).

```
ciscoasa# show memory detail

MEMPOOL_GLOBAL_SHARED POOL STATS:            MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =   1862270976   Non-mmapped bytes allocated =   1862270976
Number of free chunks       =           99   Number of free chunks       =          100
Number of mmapped regions   =            0   Number of mmapped regions   =            0
Mmapped bytes allocated     =            0   Mmapped bytes allocated     =            0
Max memory footprint        =   1862270976   Max memory footprint        =   1862270976
Keepcost                    =   1762019304   Keepcost                    =   1761869256
Max contiguous free mem     =   1762019304   Max contiguous free mem     =   1761869256
Allocated memory in use     =    100133944   Allocated memory in use     =    100233944
Free memory                 =   1762137032   Free memory                 =   1762037032


----- fragmented memory statistics -----     ----- fragmented memory statistics -----

 fragment size       count          total     fragment size       count          total
    (bytes)                        (bytes)       (bytes)                        (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        32768             1          33176           32768             1          33176
                                                      49152             1          50048
   1762019304             1     1762019304*     1761869256             1     1761869256*


----- allocated memory statistics -----      ----- allocated memory statistics -----

 fragment size       count          total     fragment size       count          total
    (bytes)                        (bytes)       (bytes)                        (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        49152            10         491520           49152             9         442368
        65536           125        8192000           65536           125        8192000
        98304             3         294912           98304             3         294912
       131072            18        2359296          131072            19        2490368
```

다음 출력에서는 크기가 131,072인 블록 대신 크기가 150,000인 블록이 할당되었음을 확인합니다.

```
ciscoasa# show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
pc = 0x8eda524, size = 150000   , count = 1
pc = 0x8f08054, size = 163904   , count = 1
pc = 0x846e477, size = 139264   , count = 1
pc = 0x8068691, size = 393216   , count = 3
pc = 0x8eea09b, size = 131072   , count = 1
pc = 0x88ca830, size = 141212   , count = 1
pc = 0x9589e93, size = 593580   , count = 4
pc = 0x9589bd2, size = 616004   , count = 4
pc = 0x8f2e060, size = 327808   , count = 2
```

```
pc = 0x8068284, size = 182000   , count = 1

0x8eda524 <logger_buffer_init_int+148 at syslog/main.c:403>
```

show memory detail 명령 출력에 대략적인 총 바이트 수가 표시되는 것은 설계에 따른 것입니다. 여기에는 두 가지 이유가 있습니다.

- 각 프래그먼트 크기에 대해 모든 프래그먼트의 합계를 구해야 하는 경우 단일 프래그먼트 크기에 대한 할당이 너무 많고 정확한 값을 얻으려면 수천 개의 청크를 확인해야 하기 때문에 성능이 저하될 수 있습니다.
- 각 휴지통 크기의 경우 이중 링크된 할당 목록을 확인해야 하며 많은 할당이 있을 수 있습니다. 이 경우 연장된 기간 동안 CPU를 사용할 수 없으므로 할당을 주기적으로 일시 중단해야 합니다. 할당을 다시 시작한 후에는 다른 프로세스에 메모리가 할당되거나 할당 취소되고 메모리 상태가 변경될 수 있습니다. 따라서 total bytes 열에 실제 값 대신 근사값이 제공됩니다.

예

다음은 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:        845044716 bytes (79%)
Used memory:        228697108 bytes (21%)
-------------      ----------------
Total memory:      1073741824 bytes (100%)
```

다음은 **show memory detail** 명령의 샘플 출력입니다.

```
ciscoasa# show memory detail
Free memory heap:                  2473071872 bytes (xx%)
 Free memory system:                xxxxxxxxxx bytes (xx%)
 Used memory:
      Allocated memory in use:       308939520 bytes (xx%)
      Reserved memory (DMA):         1512955904 bytes (xx%)
      Memory overhead:               xxxxxxxxx bytes (xx%)
 ----------------------------   ------------------
 Total memory:                     4294967296 bytes (100%)
-----------------------------------------------------
Total memory:                   268435456 bytes (100%)
Dynamic Shared Objects(DSO):           0 bytes
DMA memory:
  Unused memory:                 3212128 bytes (8%)
  Crypto reserved memory:        2646136 bytes (7%)
  Crypto free:                   1605536 bytes (4%)
  Crypto used:                   1040600 bytes (3%)
  Block reserved memory:        33366816 bytes (85%)
  Block free:                   31867488 bytes (81%)
  Block used:                    1499328 bytes (4%)
  Used memory:                    178440 bytes (0%)
-----------------------------------------------------
  Total memory:                 39403520 bytes (100%)
  HEAP memory:
  Free memory:                 130546920 bytes (80%)
  Used memory:                  33030808 bytes (20%)
  Init used memory by library:   4218752 bytes (3%)
  Allocated memory:            28812056 bytes (18%)
-----------------------------------------------------
  Total memory:                163577728 bytes (100%)

Least free memory: 122963528 bytes (75%)
Most used memory:   40614200 bytes (25%)

----- fragmented memory statistics -----
```

```
fragment size    count      total
(bytes)                     (bytes)
---------------- ---------- --------------
16               113        1808

<More>
```

다음은 **jumbo-frame reservation** 명령을 사용하고 **write memory** 명령 및 **reload** 명령을 실행한 후 ASA 5525에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:        3008918624 bytes (70%)
Used memory:        1286048672 bytes (30%)
-------------       ----------------------
Total memory:       4294967296 bytes (100%)
```

다음은 **jumbo-frame reservation** 명령을 사용하지 않고 ASA 5525에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:        3318156400 bytes (77%)
Used memory:         976810896 bytes (23%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

다음은 **jumbo-frame reservation** 명령을 사용한 후 ASA 5515에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:        3276619472 bytes (76%)
Used memory:        1018347824 bytes (24%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

다음은 **jumbo-frame reservation** 명령을 사용하지 않고 ASA 5515에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:        3481145472 bytes (81%)
Used memory:         813821824 bytes (19%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

다음은 **jumbo-frame reservation** 명령을 사용한 후 ASA 5585에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:        8883297824 bytes (69%)
Used memory:        4001604064 bytes (31%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

다음은 **jumbo-frame reservation** 명령을 사용하지 않고 ASA 5585에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:        9872205104 bytes (77%)
Used memory:        3012696784 bytes (23%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

다음은 **jumbo-frame** 명령을 지원하지 않는 ASA 5520에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
ree memory:         206128232 bytes (38%)
Used memory:         330742680 bytes (62%)
-------------       -----------------
Total memory:        536870912 bytes (100%)
```

다음은 **jumbo-frame** 명령을 지원하지 않는 ASA 5505에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
ciscoasa# show memory
Free memory:          48457848 bytes (18%)
Used memory:         219977608 bytes (82%)
-------------        -----------------
Total memory:        268435456 bytes (100%
```

다음은 ASAv에서 실행된 **show memory** 명령의 샘플 출력입니다.

```
Free memory:        2694133440 bytes (63%)
Used memory:        1600833856 bytes (37%)
-------------     ------------------
Total memory:       4294967296 bytes (100%)

Virtual platform memory
-----------------------
Provisioned       4096 MB
Allowed           4096 MB
Status            Compliant
```

관련 명령

명령	설명
show memory profile	ASA의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.
show memory binsize	특정 휴지통 크기에 할당된 청크에 대한 요약 정보를 표시합니다.

show memory api

시스템에 등록된 malloc 스택 API를 표시하려면 특권 EXEC 모드에서 **show memory api** 명령을 사용합니다.

show memory api

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 시스템에 등록된 malloc 스택 API를 표시합니다.

메모리 디버깅 기능(즉, delay-free-poisoner, memory tracker 또는 memory profiler)이 켜진 경우 해당 API가 **show memory api** 명령 출력에 표시됩니다.

예

다음은 **show memory api** 명령의 샘플 출력입니다.

```
ciscoasa# show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

관련 명령

명령	설명
show memory profile	ASA의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.
show memory binsize	특정 휴지통 크기에 할당된 청크에 대한 요약 정보를 표시합니다.

show memory app-cache

애플리케이션별 메모리 사용량을 확인하려면 특권 EXEC 모드에서 **show memory app-cache** 명령을 사용합니다.

show memory app-cache [**threat-detection** | **host** | **flow** | **tcb** | **http** | **access-list**] [**detail**]

구문 설명show

access-list	(선택 사항) 액세스 목록에 대한 애플리케이션 수준 메모리 캐시를 표시합니다.
detail	(선택 사항) 사용 가능한 시스템 메모리와 할당된 시스템 메모리에 대한 자세한 보기를 표시합니다.
flow	(선택 사항) 흐름에 대한 애플리케이션 수준 메모리 캐시를 표시합니다.
host	(선택 사항) 호스트에 대한 애플리케이션 수준 메모리 캐시를 표시합니다.
http	(선택 사항) HTTP에 대한 애플리케이션 수준 메모리 캐시를 표시합니다.
tcb	(선택 사항) TCB에 대한 애플리케이션 수준 메모리 캐시를 표시합니다.
threat-detection	(선택 사항) 위협 감지에 대한 애플리케이션 수준 메모리 캐시를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(1)	이 명령이 도입되었습니다.
8.1(1)	**access-list** 및 **http** 옵션이 추가되었습니다.

사용 지침

이 명령을 사용하여 애플리케이션별 메모리 사용량을 확인할 수 있습니다.

예

다음은 **show memory app-cache threat-detection** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show memory app-cache threat-detection
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

다음은 **show memory app-cache threat-detection detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show memory app-cache threat-detection detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
TD ACE stats 50 0 2 0 1936
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host stats 50 50 16120 0 116515360
TD Subnet stats 50 2 113 0 207016
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

다음은 **show memory app-cache host detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show memory app-cache host detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Core 0 1000 1000 5116 0 961808
SNP Host Core 1 1000 1000 4968 0 933984
SNP Host Core 2 1000 1000 5413 0 1017644
SNP Host Core 3 1000 1000 4573 0 859724

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 20070 0 3773160
```

다음은 **show memory app-cache flow detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show memory app-cache flow detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn Core 0 1000 1000 893 0 639388
SNP Conn Core 1 1000 948 980 0 701680
SNP Conn Core 2 1000 1000 1175 0 841300
SNP Conn Core 3 1000 1000 901 0 645116

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 3948 3949 0 2827484
```

다음은 **show memory app-cache access-list detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show memory app-cache access-list detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
NP ACL log c Core 0 1000 0 1 0 68
NP ACL log c Core 1 1000 0 6 0 408
NP ACL log c Core 2 1000 0 19 0 1292
NP ACL log c Core 3 1000 0 0 0 0
NP ACL log f Core 0 1000 0 0 0 0
NP ACL log f Core 1 1000 0 0 0 0
NP ACL log f Core 2 1000 0 0 0 0
NP ACL log f Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 26 0 1768
```

다음은 **show memory app-cache http detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show memory app-cache http detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
Inspect HTTP Core 0 1000 0 0 0 0
Inspect HTTP Core 1 1000 0 0 0 0
Inspect HTTP Core 2 1000 0 0 0 0
Inspect HTTP Core 3 1000 0 0 0 0
HTTP Result Core 0 1000 0 0 0 0
HTTP Result Core 1 1000 0 0 0 0
HTTP Result Core 2 1000 0 0 0 0
HTTP Result Core 3 1000 0 0 0 0

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 0 0 0
```

다음은 **show memory app-cache tcb detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show memory app-cache tcb detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB Core 0 1000 1000 968 0 197472
SNP TCB Core 1 1000 1000 694 0 141576
SNP TCB Core 2 1000 1000 1304 0 266016
SNP TCB Core 3 1000 1000 1034 0 210936

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 4000 0 816000
```

관련 명령

명령	설명
show memory profile	ASA의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.
show memory binsize	특정 휴지통 크기에 할당된 청크에 대한 요약 정보를 표시합니다.
show memory	운영 체제에 사용 가능한 최대 실제 메모리 및 현재 사용 가능한 메모리에 대한 요약을 표시합니다.

show memory binsize

특정 휴지통 크기에 할당된 청크에 대한 요약 정보를 표시하려면 특권 EXEC 모드에서 **show memory binsize** 명령을 사용합니다.

show memory binsize *size*

구문 설명

size	특정 휴지통 크기의 청크(메모리 블록)를 표시합니다. 휴지통 크기는 **show memory detail** 명령 출력의 "fragment size" 열에 표시됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 사용 지침이 없습니다.

예

다음 예에서는 크기가 500인 휴지통에 할당된 청크에 대한 요약 정보를 표시합니다.

```
ciscoasa# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

관련 명령

명령	설명
show memory-caller address	ASA에 구성된 주소 범위를 표시합니다.
show memory profile	ASA의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.
show memory	운영 체제에 사용 가능한 최대 실제 메모리 및 현재 사용 가능한 메모리에 대한 요약을 표시합니다.

show memory delayed-free-poisoner

memory delayed-free-poisoner 대기열 사용에 대한 요약을 표시하려면 특권 EXEC 모드에서 **show memory delayed-free-poisoner** 명령을 사용합니다.

show memory delayed-free-poisoner

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

clear memory delayed-free-poisoner 명령을 사용하여 대기열 및 통계를 지울 수 있습니다.

예

다음은 **show memory delayed-free-poisoner** 명령의 샘플 출력입니다.

```
ciscoasa# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
        3335600:  memory held in queue
           6095:  current queue count
              0:  elements dequeued
              3:  frees ignored by size
           1530:  frees ignored by locking
             27:  successful validate runs
              0:  aborted validate runs
       01:09:36:  local time of last validate
```

표 9-2에는 **show memory delayed-free-poisoner** 명령 출력의 중요한 필드에 대한 설명이 나와 있습니다.

표 9-2 show memory delayed-free-poisoner 명령 출력 설명

필드	설명
memory held in queue	delayed free-memory poisoner 툴 대기열에 있는 메모리입니다. delayed free-memory poisoner 툴을 사용하지 않는 경우 이러한 메모리는 일반적으로 **show memory** 출력에 “Free” 양으로 표시됩니다.
current queue count	대기열의 요소 수입니다.
elements dequeued	대기열에서 제거된 요소 수입니다. 이 숫자는 시스템의 사용 가능한 모든 메모리 또는 대부분의 메모리가 대기열에서 유지되는 것이 끝나면 증가하기 시작합니다.
frees ignored by size	요청이 너무 작아 필요한 추적 정보를 유지하지 못해 대기열에 배치되지 않은 사용 가능한 요청 수입니다.
frees ignored by locking	둘 이상의 애플리케이션에서 사용 중이기 때문에 대기열에 배치되지 않았으며 툴에서 가로채기된 사용 가능한 요청 수입니다. 마지막 애플리케이션이 메모리를 시스템에 다시 해제하면 해당 메모리 영역의 대기열 배치가 종료됩니다.
successful validate runs	**clear memory delayed-free-poisoner** 명령을 사용하여 모니터링을 활성화하거나 지운 이후에 대기열 내용이 확인된(자동으로 또는 **memory delayed-free-poisoner validate** 명령을 통해) 횟수입니다.
aborted validate runs	**clear memory delayed-free-poisoner** 명령을 사용하여 모니터링을 활성화하거나 지운 이후에 둘 이상의 작업(정기적 실행 또는 CLI에서의 확인 요청)에서 동시에 대기열을 사용하려고 시도하여 대기열 내용 확인 요청이 중단된 횟수입니다.
local time of last validate	마지막 확인 실행이 완료된 로컬 시스템 시간입니다.

관련 명령

명령	설명
clear memory delayed-free-poisoner	delayed free-memory poisoner 툴 대기열 및 통계를 지웁니다.
memory delayed-free-poisoner enable	delayed free-memory poisoner 툴을 활성화합니다.
memory delayed-free-poisoner validate	delayed free-memory poisoner 툴 대기열의 요소를 강제로 검증합니다.

show memory profile

ASA의 메모리 사용량(프로파일링)에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show memory profile** 명령을 사용합니다.

show memory profile [**peak**] [**detail** | **collated** | **status**]

구문 설명

collated	(선택 사항) 표시된 메모리 정보를 대조합니다.
detail	(선택 사항) 자세한 메모리 정보를 표시합니다.
peak	(선택 사항) "사용 중인" 버퍼가 아니라 피크 캡처 버퍼를 표시합니다.
status	(선택 사항) 메모리 프로파일링의 현재 상태 및 피크 캡처 버퍼를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show memory profile 명령을 사용하여 메모리 사용량 수준 및 메모리 누수 문제를 해결할 수 있습니다. 프로파일링이 중지된 경우에도 프로파일 버퍼 내용을 볼 수 있습니다. 프로파일링을 시작하면 버퍼가 자동으로 지워집니다.

참고 ASA에서는 메모리 프로파일링이 활성화된 경우 성능이 일시적으로 저하될 수 있습니다.

예

다음은 **show memory profile** 명령의 샘플 출력입니다.

```
ciscoasa# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

show memory profile detail 명령의 출력은 맨 왼쪽부터 6개의 데이터 열과 1개의 헤더 열로 나누어 집니다. 첫 번째 데이터 열에 해당하는 메모리 버킷 주소는 헤더 열에 제공됩니다(16진수 숫자). 데이터 자체는 버킷 주소에 속한 텍스트/코드에서 유지되는 바이트 수입니다. 데이터 열의 마침표(.)는 이 버킷의 텍스트에서 유지되는 메모리가 없음을 의미합니다. 행의 다른 열은 이전 열의 증분 양보다 큰 버킷 주소에 해당합니다. 예를 들어 첫 번째 행에 있는 첫 번째 데이터 열의 주소 버킷은 0x001069e0이고, 첫 번째 행에 있는 두 번째 데이터 열의 주소 버킷은 0x001069e4입니다. 일반적으로 헤더 열 주소는 다음 버킷 주소입니다. 즉, 이전 행의 마지막 데이터 열 주소에 증분값을 더한 값입니다. 사용량이 없는 모든 행은 표시되지 않습니다. 헤더 열에 3개의 마침표(...)를 표시하여 이러한 인접 행을 두 개 이상 표시하지 않을 수 있습니다.

다음은 **show memory profile detail** 명령의 샘플 출력입니다.

```
ciscoasa# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

다음은 **show memory profile collated** 명령의 샘플 출력입니다.

```
ciscoasa# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

다음은 피크 캡처 버퍼를 보여 주는 **show memory profile peak** 명령의 샘플 출력입니다.

```
ciscoasa# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

다음은 피크 캡처 버퍼 및 해당 버킷 주소에 속한 텍스트/코드에서 유지되는 바이트 수를 보여 주는 **show memory profile peak detail** 명령의 샘플 출력입니다.

```
ciscoasa# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

다음은 메모리 프로파일링의 현재 상태 및 피크 캡처 버퍼를 보여 주는 **show memory profile status** 명령의 샘플 출력입니다.

```
ciscoasa# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a 8(00000004)
```

관련 명령

명령	설명
memory profile enable	메모리 사용량 모니터링(메모리 프로파일링)을 활성화합니다.
memory profile text	프로파일링할 메모리의 프로그램 텍스트 범위를 구성합니다.
clear memory profile	메모리 프로파일링 기능에서 유지되는 메모리 버퍼를 지웁니다.

show memory top-usage

show memory detail 명령에서 할당된 상위 프래그먼트 크기를 표시하려면 특권 EXEC 모드에서 **show memory top-usage** 명령을 사용합니다.

show memory top-usage [*num*]

구문 설명

num	(선택 사항) 나열할 휴지통 크기 수를 표시합니다. 유효한 값은 1~64입니다.

기본값

*num*의 기본값은 10입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.4(6)	이 명령이 도입되었습니다.

사용 지침

show memory top-usage 명령을 사용하여 **show memory detail** 명령에서 할당된 상위 프래그먼트 크기를 표시할 수 있습니다.

이 명령은 클러스터링을 사용하지 않으므로 클러스터링이 활성화된 경우 비활성화할 필요가 없습니다.

예

다음은 **show memory top-usage** 명령의 샘플 출력입니다.

```
ciscoasa# show memory top-usage 3
MEMPOOL_DMA pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
      1572864             9       14155776
     12582912             1       12582912
      6291456             1        6291456

----- Binsize PC top usage -----

Binsize: 1572864                total (bytes): 14155776

pc = 0x805a870, size = 16422399 , count = 9
```

```
Binsize: 12582912               total (bytes): 12582912

pc = 0x805a870, size = 12960071 , count = 1

Binsize: 6291456                total (bytes): 6291456

pc = 0x9828a6c, size = 7962695  , count = 1


MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
     12582912             1       12582912
      2097152             6       12582912
        65536           181       11862016

----- Binsize PC top usage -----

Binsize: 12582912               total (bytes): 12582912

pc = 0x8249763, size = 37748736 , count = 1

Binsize: 2097152                total (bytes): 12582912

pc = 0x8a7ebfb, size = 2560064  , count = 1
pc = 0x8aa4413, size = 2240064  , count = 1
pc = 0x8a9bb13, size = 2240064  , count = 1
pc = 0x8a80542, size = 2097152  , count = 1
pc = 0x97e7172, size = 2097287  , count = 1
pc = 0x8996463, size = 2272832  , count = 1

Binsize: 65536                  total (bytes): 11862016

pc = 0x913db2b, size = 11635232 , count = 161
pc = 0x91421eb, size = 138688   , count = 2
pc = 0x97e7172, size = 339740   , count = 4
pc = 0x97e7433, size = 197229   , count = 3
pc = 0x82c3412, size = 65536    , count = 1
pc = 0x8190e09, size = 155648   , count = 2
pc = 0x8190af6, size = 77824    , count = 1
pc = 0x93016a1, size = 65536    , count = 1
pc = 0x89f1a40, size = 65536    , count = 1
pc = 0x9131140, size = 163968   , count = 2
pc = 0x8ee56c8, size = 66048    , count = 1
pc = 0x8056a01, size = 66528    , count = 1
pc = 0x80569e5, size = 66528    , count = 1
```

관련 명령

명령	설명
show memory tracking	현재 수집된 모든 정보를 표시합니다.

show memory tracking

툴에서 추적한 현재 할당된 메모리를 표시하려면 특권 EXEC 모드에서 **show memory tracking** 명령을 사용합니다.

show memory tracking [**address** | **dump** | **detail**]

구문 설명

address	(선택 사항) 주소를 통한 메모리 추적을 표시합니다.
detail	(선택 사항) 내부 메모리 추적 상태를 표시합니다.
dump	(선택 사항) 메모리 추적 주소를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

show memory tracking 명령을 사용하여 툴에서 추적한 현재 할당된 메모리를 표시할 수 있습니다.

예

다음은 **show memory tracking** 명령의 샘플 출력입니다.

```
ciscoasa# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

다음은 **show memory tracking address** 명령의 샘플 출력입니다.

```
ciscoasa# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154

memory tracking by address:
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
```

```
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2
```

다음은 **show memory tracking dump** 명령의 샘플 출력입니다.

```
ciscoasa# show memory tracking dump
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ...............
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ...............
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ...............
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

관련 명령

명령	설명
clear memory tracking	현재 수집된 모든 정보를 지웁니다.

show memory webvpn

WebVPN에 대한 메모리 사용량 통계를 생성하려면 특권 EXEC 모드에서 **show memory webvpn** 명령을 사용합니다.

show memory webvpn [**allobjects** | **blocks** | **dumpstate** [**cache** | **disk0** | **disk1** | **flash** | **ftp** | **system** | **tftp**] | **pools** | **profile** [**clear** | **dump** | **start** | **stop**] | **usedobjects** {{**begin** | **exclude** | **grep** | **include**} **line** *line*}]

구문 설명

allobjects	풀에 대한 WebVPN 메모리 소비 정보, 블록, 사용된 모든 개체 및 사용 가능한 모든 개체를 표시합니다.
begin	일치하는 줄에서 시작합니다.
blocks	메모리 블록에 대한 WebVPN 메모리 소비 정보를 표시합니다.
cache	WebVPN 메모리 캐시 상태 덤프에 대한 파일 이름을 지정합니다.
clear	WebVPN 메모리 프로파일을 지웁니다.
disk0	WebVPN 메모리 disk0 상태 덤프에 대한 파일 이름을 지정합니다.
disk1	WebVPN 메모리 disk1 상태 덤프에 대한 파일 이름을 지정합니다.
dump	WebVPN 메모리 프로파일을 파일에 저장합니다.
dumpstate	WebVPN 메모리 상태를 파일에 저장합니다.
exclude	일치하는 줄을 제외합니다.
flash	WebVPN 메모리 플래시 상태 덤프에 대한 파일 이름을 지정합니다.
ftp	WebVPN 메모리 FTP 상태 덤프에 대한 파일 이름을 지정합니다.
grep	일치하는 줄을 포함하거나 제외합니다.
include	일치하는 줄을 포함합니다.
line	일치시킬 줄을 식별합니다.
line	일치시킬 줄을 지정합니다.
pools	메모리 풀에 대한 WebVPN 메모리 소비 정보를 표시합니다.
profile	WebVPN 메모리 프로파일을 가져와 파일에 배치합니다.
system	WebVPN 메모리 시스템 상태 덤프에 대한 파일 이름을 지정합니다.
start	WebVPN 메모리 프로파일 수집을 시작합니다.
stop	WebVPN 메모리 프로파일 가져오기를 중지합니다.
tftp	WebVPN 메모리 TFTP 상태 덤프에 대한 파일 이름을 지정합니다.
usedobjects	사용된 개체에 대한 WebVPN 메모리 소비 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

예

다음은 **show memory webvpn allobjects** 명령의 샘플 출력입니다.

```
ciscoasa# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

관련 명령

명령	설명
memory-size	WebVPN 서비스에서 사용할 수 있는 ASA의 메모리 양을 설정합니다.

show memory-caller address

ASA에 구성된 주소 범위를 표시하려면 특권 EXEC 모드에서 **show memory-caller address** 명령을 사용합니다.

show memory-caller address

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

show memory-caller address 명령을 사용하여 주소 범위를 표시하려면 먼저 **memory caller-address** 명령으로 주소 범위를 구성해야 합니다.

예

다음 예에서는 **memory caller-address** 명령을 사용하여 주소 범위를 구성하는 방법 및 **show memory-caller address** 명령의 결과 출력을 보여 줍니다.

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08
ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

show memory-caller address 명령을 입력하기 전에 주소 범위를 구성하지 않은 경우에는 아무 주소도 표시되지 않습니다.

```
ciscoasa# show memory-caller address
Move down stack frame for the addresses:
```

관련 명령

명령	설명
memory caller-address	발신자 PC에 대한 메모리 블록을 구성합니다.

show mfib

전달 항목 및 인터페이스와 관련된 MFIB를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib** 명령을 사용합니다.

show mfib [*group* [*source*]] [**verbose**] [**cluster**]

구문 설명

cluster	(선택 사항) MFIB epoch 수 및 현재 타이머 값을 표시합니다.
group	(선택 사항) 멀티캐스트 그룹의 IP 주소를 표시합니다.
source	(선택 사항) 멀티캐스트 경로 소스의 IP 주소를 표시합니다. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 유니캐스트 IP 주소입니다.
verbose	(선택 사항) 항목에 대한 추가 정보를 표시합니다.

기본값

선택적 인수 없이 모든 그룹에 대한 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	**cluster** 키워드가 추가되었습니다. ASA 5580 및 5585-X에만 적용됩니다.

예

다음은 **show mfib** 명령의 샘플 출력입니다.

```
ciscoasa# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

관련 명령

명령	설명
show mfib verbose	전달 항목 및 인터페이스에 대한 자세한 정보를 표시합니다.

show mfib active

활성 멀티캐스트 소스를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib active** 명령을 사용합니다.

show mfib [*group*] **active** [*kbps*]

구문 설명

group	(선택 사항) 멀티캐스트 그룹의 IP 주소입니다.
kbps	(선택 사항) 이 값보다 크거나 같은 멀티캐스트 스트림으로 표시를 제한합니다.

이 명령에는 인수 또는 키워드가 없습니다.

기본값

*kbps*의 기본값은 4입니다. *group*을 지정하지 않으면 모든 그룹이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show mfib active 명령의 출력에는 rate PPS에 대한 양수 또는 음수가 표시됩니다. RPF 패킷이 실패하거나 라우터에서 인터페이스 출력(OIF) 목록이 있는 RPF 패킷을 발견한 경우에는 ASA에서 음수를 표시합니다. 이 활동 유형은 멀티캐스트 라우팅 문제를 나타낼 수 있습니다.

예

다음은 **show mfib active** 명령의 샘플 출력입니다.

```
ciscoasa# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

관련 명령

명령	설명
show mroute active	활성 멀티캐스트 스트림을 표시합니다.

show mfib count

MFIB 경로 및 패킷 수 데이터를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib count** 명령을 사용합니다.

show mfib [*group* [*source*]] **count**

구문 설명

group	(선택 사항) 멀티캐스트 그룹의 IP 주소입니다.
source	(선택 사항) 멀티캐스트 경로 소스의 IP 주소입니다. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 유니캐스트 IP 주소입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 패킷 삭제 통계를 표시합니다.

예

다음은 **show mfib count** 명령의 샘플 출력입니다.

```
ciscoasa# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

관련 명령

명령	설명
clear mfib counters	MFIB 라우터 패킷 카운터를 지웁니다.
show mroute count	멀티캐스트 경로 카운터를 표시합니다.

show mfib interface

MFIB 프로세스와 관련된 인터페이스에 대한 패킷 통계를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib interface** 명령을 사용합니다.

show mfib interface [*interface*]

구문 설명

interface	(선택 사항) 인터페이스 이름입니다. 지정된 인터페이스로 표시를 제한합니다.

기본값

모든 MFIB 인터페이스에 대한 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예는 **show mfib interface** 명령의 샘플 출력입니다.

```
ciscoasa# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

관련 명령

명령	설명
show mfib	전달 항목 및 인터페이스와 관련된 MFIB 정보를 표시합니다.

show mfib reserved

예약된 그룹을 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib reserved** 명령을 사용합니다.

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

구문 설명

active	(선택 사항) 활성 멀티캐스트 소스를 표시합니다.
count	(선택 사항) 패킷 및 경로 수 데이터를 표시합니다.
kpbs	(선택 사항) 이 값보다 크거나 같은 활성 멀티캐스트 소스로 표시를 제한합니다.
verbose	(선택 사항) 추가 정보를 표시합니다.

기본값

*kbps*의 기본값은 4입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 224.0.0.0~224.0.0.225 범위의 MFIB 항목을 표시합니다.

예

다음은 **show mfib reserved** 명령의 샘플 출력입니다.

```
ciscoasa# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

관련 명령

명령	설명
show mfib active	활성 멀티캐스트 스트림을 표시합니다.

show mfib status

일반적인 MFIB 컨피그레이션 및 작동 상태를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib status** 명령을 사용합니다.

show mfib status

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show mfib status** 명령의 샘플 출력입니다.

```
ciscoasa# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

관련 명령

명령	설명
show mfib	전달 항목 및 인터페이스와 관련된 MFIB 정보를 표시합니다.

show mfib summary

MFIB 항목 및 인터페이스 수에 대한 요약 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib summary** 명령을 사용합니다.

show mfib summary

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show mfib summary** 명령의 샘플 출력입니다.

```
ciscoasa# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

관련 명령

명령	설명
show mroute summary	멀티캐스트 라우팅 테이블 요약 정보를 표시합니다.

show mfib verbose

전달 항목 및 인터페이스에 대한 자세한 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mfib verbose** 명령을 사용합니다.

show mfib verbose

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show mfib verbose** 명령의 샘플 출력입니다.

```
ciscoasa# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

관련 명령

명령	설명
show mfib	전달 항목 및 인터페이스와 관련된 MFIB 정보를 표시합니다.
show mfib summary	MFIB 항목 및 인터페이스 수에 대한 요약 정보를 표시합니다.

show mgcp

MGCP 컨피그레이션 및 세션 정보를 표시하려면 특권 EXEC 모드에서 **show mgcp** 명령을 사용합니다.

show mgcp {**commands** | **sessions**} [**detail**]

구문 설명

commands	명령 대기열에 있는 MGCP 명령 수를 나열합니다.
detail	(선택 사항) 각 명령(또는 세션)에 대한 추가 정보를 출력에 나열합니다.
sessions	기존 MGCP 세션 수를 나열합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show mgcp commands 명령은 명령 대기열에 있는 MGCP 명령 수를 나열합니다. **show mgcp sessions** 명령은 기존 MGCP 세션 수를 나열합니다. **detail** 옵션은 각 명령(또는 세션)에 대한 추가 정보를 출력에 포함합니다.

예

다음은 **show mgcp** 명령 옵션의 예입니다.

```
ciscoasa# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
ciscoasa#

ciscoasa# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP | host-pc-2
        Transaction ID  2052
        Endpoint name | aaln/1
        Call ID | 9876543210abcdef
        Connection ID |
        Media IP | 192.168.5.7
        Media port | 6058
```

```
ciscoasa#

ciscoasa# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
ciscoasa#

ciscoasa# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP | host-pc-2
        Call ID | 9876543210abcdef
        Connection ID | 6789af54c9
        Endpoint name | aaln/1
        Media lcl port  6166
        Media rmt IP | 192.168.5.7
        Media rmt port  6058
ciscoasa#
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
debug mgcp	MGCP 디버그 정보를 활성화합니다.
inspect mgcp	MGCP 애플리케이션 검사를 활성화합니다.
mgcp-map	MGCP 맵을 정의하고 MGCP 맵 컨피그레이션 모드를 활성화합니다.
show conn	여러 연결 유형에 대한 연결 상태를 표시합니다.

show mmp

기존 MMP 세션에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show mmp** 명령을 사용합니다.

show mmp [*address*]

구문 설명

address	MMP 클라이언트/서버의 IP 주소를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.

예

다음 예에서는 **show mmp** 명령을 사용하여 기존 MMP 세션에 대한 정보를 표시하는 방법을 보여줍니다.

```
ciscoasa# show mmp 10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

관련 명령

명령	설명
debug mmp	MMP 검사 이벤트를 표시합니다.
inspect mmp	MMP 검사 엔진을 구성합니다.
show debug mmp	MMP 검사 모듈에 대한 현재 디버그 설정을 표시합니다.

show mode

실행 중인 소프트웨어 이미지 및 플래시 메모리의 이미지에 대한 보안 상황 모드를 표시하려면 특권 EXEC 모드에서 **show mode** 명령을 사용합니다.

show mode

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show mode** 명령의 샘플 출력입니다. 다음 예에서는 현재 모드 및 실행 중이지 않은 이미지 “image.bin”에 대한 모드를 표시합니다.

```
ciscoasa# show mode flash:/image.bin
Firewall mode: multiple
```

이 모드는 다중 모드이거나 단일 모드일 수 있습니다.

관련 명령

명령	설명
context	시스템 컨피그레이션에서 보안 상황을 만들고 상황 컨피그레이션 모드를 시작합니다.
mode	상황 모드를 단일 모드 또는 다중 모드로 설정합니다.

show module

ASA에 설치된 모듈에 대한 정보를 표시하려면 사용자 EXEC 모드에서 **show module** 명령을 사용합니다.

show module [*id* | **all**] [**details** | **recover** | **log** [**console**]

구문 설명

all	(기본값) 모든 모듈에 대한 정보를 표시합니다.
console	(선택 사항) 모듈에 대한 콘솔 로그 정보를 표시합니다.
details	(선택 사항) 모듈에 대한 원격 관리 컨피그레이션을 비롯한 추가 정보를 표시합니다.
id	모듈 ID를 지정합니다. 하드웨어 모듈의 경우 슬롯 번호(**0**(ASA의 경우) 또는 **1**(설치된 모듈의 경우))를 지정합니다. 소프트웨어 모듈의 경우 다음 이름 중 하나를 지정합니다. • **sfr** - ASA FirePOWER 모듈 • **ips** - IPS 모듈 • **cxsc** - ASA CX 모듈
log	(선택 사항) 모듈에 대한 로그 정보를 표시합니다.
recover	(선택 사항) **hw-module** 또는 **sw-module module recover** 명령에 대한 설정을 표시합니다.

기본값

기본적으로 모든 모듈에 대한 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황[1]	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

1. **show module recover** 명령은 시스템 실행 공간에서만 사용할 수 있습니다.

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.1(1)	출력에 보다 자세한 정보가 포함되도록 명령이 수정되었습니다.
8.2(1)	SSC에 대한 정보가 출력에 포함됩니다.
8.2(5)	ASA 5585-X 및 ASA 5585-X의 IPS SSP에 대한 지원 정보가 추가되었습니다.
8.4(4.1)	ASA CX 모듈에 대한 지원이 추가되었습니다.
8.6(1)	ASA 5512-X~ASA 5555-X의 경우 **log** 및 **console** 키워드가 추가되고, **ips** 디바이스 ID가 추가되었습니다.

릴리스	수정 사항
9.1(1)	**cxsc** 모듈 ID가 추가되어 ASA CX 소프트웨어 모듈에 대한 지원이 추가되었습니다.
9.2(1)	**sfr** 키워드를 포함하여 ASA FirePOWER 모듈에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 ASA에 설치된 모듈에 대한 정보를 표시합니다. ASA 자체도 화면(슬롯 0)에 모듈로 표시됩니다.

예

다음은 **show module** 명령의 샘플 출력입니다. 모듈 0이 기본 디바이스이며 모듈 1은 CSC SSM입니다.

```
ciscoasa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

다음 표에서 출력에 나열된 각 필드에 대한 설명이 나와 있습니다.

표 9-3 show module 출력 필드

필드	설명
Mod	모듈 번호(0 또는 1)입니다.
Ports	포트 수입니다.
Card Type	모듈 0에 표시된 디바이스의 유형은 플랫폼 모델입니다. 모듈 1의 SSM은 유형이 SSM입니다.
Model	이 모듈의 모델 번호입니다.
Serial No.	일련 번호입니다.
MAC Address Range	이 SSM의 인터페이스 또는 디바이스의 경우 내장형 인터페이스에 대한 MAC 주소 범위입니다.
Hw Version	하드웨어 버전입니다.
Fw Version	펌웨어 버전입니다.
Sw Version	소프트웨어 버전입니다.

표 9-3 show module 출력 필드 (계속)

필드	설명
SSM Application Name	SSM에서 실행되는 애플리케이션의 이름입니다.
SSM Application Version	SSM에서 실행되는 애플리케이션의 버전입니다.
Status	모듈 0에 있는 디바이스의 경우 상태는 Up Sys입니다. 모듈 1에 있는 SSM의 상태는 다음 중 하나일 수 있습니다. • Initializing - SSM를 검색하는 중이며, 디바이스에서 제어 통신을 초기화하는 중입니다. • Up - SSM에서 디바이스에 의한 초기화를 완료했습니다. • Unresponsive - 이 SSM와 통신하는 동안 디바이스에서 오류가 발생했습니다. • Reloading - SSM를 다시 로드하는 중입니다. • Shutting Down - SSM를 종료하는 중입니다. • Down - SSM가 종료되었습니다. • Recover - SSM에서 복구 이미지를 다운로드하는 중입니다. • No Image Present - IPS 소프트웨어가 설치되어 있지 않습니다.
Data Plane Status	데이터 평면의 현재 상태입니다.
Compatibility	나머지 디바이스에 상대적인 SSM의 호환성입니다.
Slot	물리적 슬롯 번호입니다(이중 SSP 모드에서만 사용됨).

show module details 명령의 출력은 설치된 모듈에 따라 다릅니다. 예를 들어 CSC SSM에 대한 출력에는 CSC SSM 소프트웨어 구성요소에 대한 필드가 포함됩니다.

다음은 **show module 1 details** 명령의 일반적인 샘플 출력입니다.

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

다음 표에는 출력의 추가 필드에 대한 설명이 나와 있습니다.

표 9-4 show module details 추가 출력 필드

필드	설명
DC address (표시 안 됨)	(ASA FirePOWER에만 해당). 모듈을 관리하는 FireSIGHT Management Center의 주소입니다.
Mgmt IP addr	모듈의 관리 인터페이스에 대한 IP 주소를 표시합니다.
Mgmt Network Mask (표시 안 됨)	관리 주소의 서브넷 마스크를 표시합니다.
Mgmt Gateway (표시 안 됨)	관리 주소의 게이트웨이입니다.
Mgmt web ports	모듈의 관리 인터페이스에 대해 구성된 포트를 표시합니다.
Mgmt TLS enabled	모듈의 관리 인터페이스에 대한 연결에 TLS(전송 계층 보안)가 사용되는지 여부(true 또는 false)를 표시합니다.

소프트웨어 모듈을 구성할 수 있는 모델의 경우 **show module** 명령은 가능한 모든 모듈을 나열합니다. 상태 정보는 그 중 하나가 설치되어 있는지 여부를 나타냅니다.

```
ciscoasa# show module

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt     ASA5555            FCH1714J6HP
 ips Unknown                                      N/A                FCH1714J6HP
cxsc Unknown                                      N/A                FCH1714J6HP
 sfr FirePOWER Services Software Module           ASA5555            FCH1714J6HP

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 bc16.6520.1dcd to bc16.6520.1dd6  1.0          2.1(9)8      100.8(66)11
 ips bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
cxsc bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
 sfr bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A          5.3.1-100

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc Unknown                        No Image Present Not Applicable
 sfr ASA FirePOWER                  Up               5.3.1-100

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Unresponsive       Not Applicable
 sfr Up                 Up

Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Enabled         172 days
```

다음은 **show module 1 recover** 명령의 샘플 출력입니다.

```
ciscoasa# show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

다음은 SSC가 설치된 경우 **show module 1 details** 명령의 샘플 출력입니다.

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5505 Security Services Card
Model: ASA-SSC
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc:
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

다음은 ASA 5585-X에 IPS SSP가 설치된 경우 **show module 1 details** 명령의 샘플 출력입니다.

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA-SSM-20
Hardware version: V1.0
Serial Number: 12345678
Firmware version: 1.0(7)2
Software version: 4.1(1.1)S47(0.1)
MAC Address Range: 000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status: Up
Status: Up
Mgmt IP addr: 10.89.147.13
Mgmt web ports: 443
Mgmt TLS enabled: true
```

다음은 ASA 5585-X에 CXSC SSP가 설치된 경우 **show module all** 명령의 샘플 출력입니다.

```
ciscoasa# show module all

Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi  ASA5585-SSP-10     JAF1504CBRM
  1 ASA 5585-X CXSC Security Services Processor-1 ASA5585-SSP-IPS10  JAF1510BLSE

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1d54 to 5475.d05b.1d5f  1.0          2.0(7)0      100.7(14)13
  1 5475.d05b.248c to 5475.d05b.2497  1.0          0.0(0)0      1.0
```

```
Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CXSC Security Module             Up               1.0

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

다음은 ASA 5585-X에 CXSC SSP가 설치된 경우 **show module 1 details** 명령의 샘플 출력입니다.

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA5585-S10C10-K8
Hardware version:   1.0
Serial Number:      123456789
Firmware version:   1.0(9)0
Software version:   CXSC Security Module Version 1.0
App. name:          CXSC Security Module
App. version:       Version 1.0
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Activated:          Yes
Mgmt IP addr:       100.0.1.4
Mgmt web port:      8443
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버깅 메시지를 표시합니다.
hw-module module recover	TFTP 서버에서 복구 이미지를 로드하여 모듈을 복구합니다.
hw-module module reset	모듈을 종료하고 하드웨어 재설정을 수행합니다.
hw-module module reload	모듈 소프트웨어를 다시 로드합니다.
hw-module module shutdown	컨피그레이션 데이터의 손실 없이 전원을 끄려고 준비 중인 모듈 소프트웨어를 닫습니다.
sw-module	소프트웨어 모듈을 구성합니다.

show monitor-interface

대체작동을 위해 모니터링되는 인터페이스에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show monitor-interface** 명령을 사용합니다.

show monitor-interface

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.2(2)	이 명령이 수정되었습니다. 출력에는 IPv6 주소가 포함됩니다.

사용 지침

인터페이스에 둘 이상의 IPv6 주소가 구성되어 있을 수 있으므로 링크-로컬 주소만 **show monitor-interface** 명령에 표시됩니다. 인터페이스에 IPv4 주소와 IPv6 주소가 둘 다 구성된 경우 두 주소 모두 출력에 표시됩니다. 인터페이스에 구성된 IPv4 주소가 없는 경우 IPv4 주소는 출력에 0.0.0.0으로 표시됩니다. 인터페이스에 구성된 IPv6 주소가 없는 경우 이 주소는 출력에서 생략됩니다.

모니터링되는 대체작동 인터페이스의 상태는 다음과 같습니다.

- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- Normal - 인터페이스를 트래픽을 받는 중입니다.
- Normal (Waiting) - 인터페이스가 작동하지만 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 않았습니다. 인터페이스에 대해 대기 IP 주소가 구성되어 있는지, 그리고 두 인터페이스가 연결되어 있는지 확인하십시오.
- Testing - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- Link Down - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- No Link - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- Failed - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

예

다음은 **show monitor-interface** 명령의 샘플 출력입니다.

```
ciscoasa# show monitor-interface

This host: Primary - Active
                Interface outside (10.86.94.88): Normal (Waiting)
                Interface management (192.168.1.1): Normal (Waiting)
                Interface failif (0.0.0.0/fe80::223:4ff:fe77:fed): Normal (Waiting)
        Other host: Secondary - Failed
                Interface outside (0.0.0.0): Unknown (Waiting)
                Interface management (0.0.0.0): Unknown (Waiting)
                Interface failif (0.0.0.0): Unknown (Waiting)
```

관련 명령

명령	설명
monitor-interface	특정 인터페이스에 대한 상태 모니터링을 활성화합니다.

show mrib client

MRIB 클라이언트 연결에 대한 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mrib client** 명령을 사용합니다.

show mrib client [**filter**] [**name** *client_name*]

구문 설명

filter	(선택 사항) 클라이언트 필터를 표시합니다. 각 클라이언트에서 소유한 MRIB 플래그 및 각 클라이언트와 관련된 플래그에 대한 정보를 보는 데 사용됩니다.
name *client_name*	(선택 사항) MRIB의 클라이언트로 작동하는 멀티캐스트 라우팅 프로토콜(PIM 또는 IGMP)의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

filter 옵션은 여러 MRIB 클라이언트에서 등록한 경로 및 인터페이스 수준 플래그 변경 사항을 표시하는 데 사용됩니다. 또한 이 명령 옵션은 MRIB 클라이언트가 소유한 플래그도 표시합니다.

예

다음은 **filter** 키워드를 사용한 **show mrib client** 명령의 샘플 출력입니다.

```
ciscoasa# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
```

```
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

관련 명령

명령	설명
show mrib route	MRIB 테이블 항목을 표시합니다.

show mrib route

MRIB 테이블의 항목을 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show mrib route** 명령을 사용합니다.

show mrib route [[*source* | *****] [*group*[*/prefix-length*]]]

구문 설명

*	(선택 사항) 공유 트리 항목을 표시합니다.
/prefix-length	(선택 사항) MRIB 경로의 접두사 길이입니다. 접두사(주소의 네트워크 부분)를 구성하는 상위 연속 비트 수를 나타내는 10진수 값입니다. 10진수 값 앞에 슬래시가 표시되어야 합니다.
group	(선택 사항) 그룹의 IP 주소 또는 이름입니다.
source	(선택 사항) 경로 소스의 IP 주소 또는 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

MFIB 테이블에는 MRIB에서 업데이트된 항목 및 플래그의 하위 집합이 유지됩니다. 플래그는 멀티캐스트 패킷에 대한 전달 규칙 집합에 따라 전달 및 신호 처리 동작을 결정합니다.

인터페이스 및 플래그 목록 외에 각 경로 항목에 여러 카운터가 표시됩니다. 바이트 수는 전달된 총 바이트 수입니다. 패킷 수는 이 항목에 대해 수신된 패킷 수입니다. **show mfib count** 명령은 경로에 독립적인 전역 카운터를 표시합니다.

예

다음은 **show mrib route** 명령의 샘플 출력입니다.

```
ciscoasa# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
```

```
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

관련 명령

명령	설명
show mfib count	MFIB 테이블의 경로 및 패킷 수 데이터를 표시합니다.
show mrib route summary	MRIB 테이블 항목에 대한 요약을 표시합니다.

show mroute

IPv4 멀티캐스트 라우팅 테이블을 표시하려면 특권 EXEC 모드에서 **show mroute** 명령을 사용합니다.

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

구문 설명

active *rate*	(선택 사항) 활성 멀티캐스트 소스만 표시합니다. 활성 소스는 지정된 *rate* 이상으로 전송하는 소스입니다. *rate*를 지정하지 않은 경우에는 4kbps 이상의 속도로 전송하는 소스가 활성 소스입니다.
count	(선택 사항) 패킷 수, 초당 패킷 수, 평균 패킷 크기, 초당 비트 수 등 그룹 및 소스에 대한 통계를 표시합니다.
group	(선택 사항) DNS 호스트 테이블에 정의된 멀티캐스트 그룹의 IP 주소 또는 이름입니다.
pruned	(선택 사항) 정리된 경로를 표시합니다.
reserved	(선택 사항) 예약된 그룹을 표시합니다.
source	(선택 사항) 소스 호스트 이름 또는 IP 주소입니다.
summary	(선택 사항) 멀티캐스트 라우팅 테이블의 각 항목에 대한 한 줄로 요약된 정보를 표시합니다.

기본값

지정하지 않은 경우 *rate* 인수는 기본적으로 4kbps로 설정됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show mroute 명령은 멀티캐스트 라우팅 테이블의 내용을 표시합니다. ASA는 PIM 프로토콜 메시지, IGMP 보고서 및 트래픽을 기반으로 (S,G) 및 (*,G) 항목을 생성하여 멀티캐스트 라우팅 테이블을 채웁니다. 별표(*)는 모든 소스 주소를 나타내고, "S"는 단일 소스 주소를 나타내며, "G"는 대상 멀티캐스트 그룹 주소입니다. (S, G) 항목을 생성할 때 소프트웨어는 유니캐스트 라우팅 테이블에서 발견한(RPF를 통해) 해당 대상 그룹에 대한 최상의 경로를 사용합니다.

실행 중인 컨피그레이션에서 **mroute** 명령을 보려면 **show running-config mroute** 명령을 사용합니다.

예

다음은 **show mroute** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

다음 필드가 **show mroute** 출력에 표시됩니다.

- **Flags** - 항목에 대한 정보를 제공합니다.
  - **D-Dense**. 항목이 조밀한 모드로 작동하는 중입니다.
  - **S-Sparse**. 항목이 스파스 모드로 작동하는 중입니다.
  - **B-Bidir Group**. 멀티캐스트 그룹이 양방향 모드로 작동 중임을 나타냅니다.
  - **s-SSM Group**. 멀티캐스트 그룹이 IP 주소의 SSM 범위 내에 있음을 나타냅니다. 이 플래그는 SSM 범위가 변경되면 재설정됩니다.
  - **C-Connected**. 멀티캐스트 그룹의 멤버가 직접 연결된 인터페이스에 있습니다.
  - **L-Local**. ASA 자체가 멀티캐스트 그룹의 멤버입니다. 그룹은 **igmp join-group** 명령을 통해 로컬로 조인됩니다(구성된 그룹의 경우).
  - **I-Received Source Specific Host Report**. (S, G) 항목이 (S, G) 보고서에 의해 생성되었음을 나타냅니다. 이 (S, G) 보고서는 IGMP에 의해 생성되었을 수 있습니다. 이 플래그는 DR에서만 설정됩니다.
  - **P-Pruned**. 경로가 정리되었습니다. 소프트웨어는 다운스트림 멤버가 소스에 조인할 수 있도록 이 정보를 유지합니다.
  - **R-RP-bit set**. (S, G) 항목이 RP 쪽을 가리키고 있음을 나타냅니다.
  - **F-Register flag**. 소프트웨어가 멀티캐스트 소스에 등록 중임을 나타냅니다.
  - **T-SPT-bit set**. 패킷이 최단 경로 소스 트리에 수신되었음을 나타냅니다.
  - **J-Join SPT**. (*, G) 항목의 경우 공유 트리 아래에 흐르는 트래픽 속도가 그룹에 대해 설정된 SPT-Threshold를 초과함을 나타냅니다. 기본 SPT-Threshold 설정은 0kbps입니다. J - Join shortest path tree (SPT) 플래그가 설정된 경우 공유 트리 아래에 수신된 다음 (S, G) 패킷이 소스 방향으로 (S, G) 조인을 트리거하여 ASA가 소스 트리에 조인하도록 합니다.

    (S, G) 항목의 경우 그룹에 대한 SPT-Threshold를 초과하여 항목이 생성되었음을 나타냅니다. J - Join SPT 플래그가 (S, G) 항목에 지정된 경우 ASA는 소스 트리에서 트래픽 속도를 모니터링하여 소스 트리의 트래픽 속도가 그룹에 대해 설정된 SPT-Threshold보다 1분 이상 낮게 유지되는 경우 이 소스에 대한 공유 트리로 다시 전환합니다.

참고 ASA 는 공유 트리에서 트래픽 속도를 측정하여 측정된 속도를 1 초에 한 번씩 그룹의 SPT-Threshold 와 비교합니다 . 트래픽 속도가 SPT-Threshold 를 초과하는 경우에는 다음에 트래픽 속도를 측정할 때까지 J - Join SPT 플래그가 (*, G) 항목에 설정되어 있습니다 . 다음 패킷이 공유 트리에 도착하고 새 특정 간격이 시작되면 플래그가 지워집니다 .

기본 SPT-Threshold 값인 0kbps가 그룹에 사용되는 경우에는 J - Join SPT 플래그가 항상 (*, G) 항목에 설정되고 지워지지 않습니다. 기본 SPT-Threshold 값이 사용되는 경우 ASA는 새 소스의 트래픽이 수신될 때 최단 경로 소스 트리로 즉시 전환됩니다.

- **Timers:Uptime/Expires** - Uptime은 인터페이스별로 항목이 IP 멀티캐스트 라우팅 테이블에 유지된 기간(시간, 분, 초)을 나타냅니다. Expires는 인터페이스별로 항목이 IP 멀티캐스트 라우팅 테이블에서 제거될 때까지의 기간(시간, 분, 초)을 나타냅니다.
- **Interface state** - 들어오거나 나가는 인터페이스의 상태를 나타냅니다.
  - **Interface** - 들어오거나 나가는 인터페이스 목록에 나열된 인터페이스 이름입니다.
  - **State** - 액세스 목록 또는 TTL(Time to Live) 임계값으로 인한 제한이 있는지 여부에 따라 패킷이 전달 또는 정리되거나 인터페이스에서 null로 유지됨을 나타냅니다.
- **(*, 239.1.1.40)** 및 **(* , 239.2.2.1)** - IP 멀티캐스트 라우팅 테이블의 항목입니다. 항목은 소스의 IP 주소와 그 뒤에 오는 멀티캐스트 그룹의 IP 주소로 구성됩니다. 소스 위치의 별표(*)는 모든 소스를 나타냅니다.
- **RP** - RP의 주소입니다. 스파스 모드에서 작동하는 라우터 및 액세스 서버의 경우 이 주소는 항상 224.0.0.0입니다.
- **Incoming interface** - 소스의 멀티캐스트 패킷에 필요한 인터페이스입니다. 이 인터페이스에 수신되지 않은 패킷은 삭제됩니다.
- **RPF nbr** - 소스에 대한 업스트림 라우터의 IP 주소입니다.
- **Outgoing interface list** - 전달되는 패킷이 통과하는 인터페이스입니다.

관련 명령

명령	설명
clear configure mroute	실행 중인 컨피그레이션에서 **mroute** 명령을 제거합니다.
mroute	정적 멀티캐스트 경로를 구성합니다.
show mroute	IPv4 멀티캐스트 라우팅 테이블을 표시합니다.
show running-config mroute	구성된 멀티캐스트 경로를 표시합니다.

10 장

show nac-policy through show ospf virtual-links 명령

show nac-policy

NAC 정책 사용 통계 및 NAC 정책 할당을 표시하려면 특권 EXEC 모드에서 **show nac-policy** 명령을 사용합니다.

show nac-policy [*nac-policy-name*]

구문 설명

nac-policy-name	(선택 사항) 사용 통계를 표시할 NAC 정책의 이름입니다.

기본값

이름을 지정하지 않으면 모든 NAC 정책 이름이 해당 통계와 함께 CLI에 나열합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

예

다음 예에서는 framework1 및 framework2라는 NAC 정책에 대한 데이터를 표시합니다.

```
ciscoasa(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

각 NAC 정책의 첫째 줄은 해당 이름 및 유형(nac-framework)을 나타냅니다. 정책이 그룹 정책에 할당되지 않은 경우에는 CLI에서 정책 유형 옆에 the text “is not in use”가 표시됩니다. 그렇지 않으면 해당 그룹 정책의 사용 데이터가 CLI에 표시됩니다. 표 10-1에서는 **show nac-policy** 명령의 필드를 설명합니다.

표 10-1 show nac-policy 명령 필드

필드	설명
applied session count	이 ASA에서 NAC 정책을 적용한 누적 VPN 세션 수입니다.
applied group-policy count	이 ASA에서 NAC 정책을 적용한 누적 그룹 정책 수입니다.
group-policy list	이 NAC 정책이 할당된 그룹 정책의 목록입니다. 이 경우 그룹 정책의 사용에 따라 해당 그룹 정책이 목록에 표시되는지 여부가 결정되는 것이 아닙니다. 실행 중인 컨피그레이션에서 NAC 정책이 할당된 그룹 정책이 이 목록에 표시됩니다.

관련 명령

clear nac-policy	NAC 정책 사용 통계를 재설정합니다.
show vpn-session.db	NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.
show vpn-session_summary.db	IPSec, Cisco WebVPN 및 NAC 세션 수를 표시합니다.

show nameif

nameif 명령을 사용하여 설정된 인터페이스 이름을 확인하려면 특권 EXEC 모드에서 **show nameif** 명령을 사용합니다.

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name* | **zone**]

구문 설명

mapped_name	(선택 사항) 다중 상황 모드에서 매핑된 이름(**allocate-interface** 명령을 사용하여 할당된 경우)을 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다. 허용되는 값은 **interface** 명령을 참조하십시오.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
zone	(선택 사항) 영역 이름을 표시합니다.

기본값

인터페이스를 지정하지 않은 경우 ASA에서 모든 인터페이스 이름을 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.3(2)	**zone** 키워드가 추가되었습니다.

사용 지침

다중 상황 모드에서 **allocate-interface** 명령으로 인터페이스 ID를 매핑한 경우 하나의 상황에서만 매핑된 이름을 지정할 수 있습니다. 이 명령의 출력에는 Interface 열에만 매핑된 이름이 표시됩니다.

예

다음은 **show nameif** 명령의 샘플 출력입니다.

```
ciscoasa# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

show nameif zone 명령은 다음 출력을 참고하십시오.

```
ciscoasa# show nameif zone
Interface                Name                   zone-name    Security
GigabitEthernet0/0       inside-1               inside-zone    100
GigabitEthernet0/1.21    inside                 inside-zone    100
GigabitEthernet0/1.31    4                                     0
GigabitEthernet0/2       outside                outside-zone   0
Management0/0            lan                                   0
```

관련 명령

명령	설명
allocate-interface	인터페이스 및 하위 인터페이스를 보안 상황에 할당합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
nameif	인터페이스 이름을 설정합니다.
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.

show nat

NAT 정책의 통계를 표시하려면 특권 EXEC 모드에서 **show nat** 명령을 사용합니다.

show nat [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*]
[**translated** [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*]] [**detail**]
[**divert-table** [**ipv6**] [**interface** *name*]]

구문 설명

detail	(선택 사항) 개체 필드의 자세한 정보 표시 확장을 포함합니다.
divert-table	(선택 사항) NAT 전환 테이블을 표시합니다.
interface *name*	(선택 사항) 소스 인터페이스를 지정합니다.
ip_addr mask	(선택 사항) IP 주소 및 서브넷 마스크를 지정합니다.
ipv6	(선택 사항) 전환 테이블에서 IPv6 항목을 표시합니다.
object *name*	(선택 사항) 네트워크 개체 또는 서비스 객체를 지정합니다.
object-group *name*	(선택 사항) 네트워크 개체 그룹을 지정합니다.
translated	(선택 사항) 변환된 파라미터를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.
9.0(1)	이제 이 명령은 IPv4와 IPv6 간의 변환뿐만 아니라 IPv6 트래픽을 지원합니다.

사용 지침

show nat 명령을 사용하여 NAT 정책의 런타임 표현을 표시할 수 있습니다. **detail** 선택적 키워드를 사용하여 개체를 확장하고 개체 값을 확인할 수 있습니다. 추가 선택 필드를 사용하여 **show nat** 명령 출력을 제한할 수 있습니다.

예

다음은 **show nat** 명령의 샘플 출력입니다.

```
ciscoasa# show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0

ciscoasa# show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
    1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

다음은 IPv6과 IPv4 간 **show nat detail** 명령의 샘플 출력입니다.

```
ciscoasa# show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

다음은 **show nat divert ipv6** 명령의 샘플 출력입니다.

```
ciscoasa# show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

관련 명령

명령	설명
clear nat counters	NAT 정책 카운터를 지웁니다.
nat	하나의 인터페이스에서 다른 인터페이스의 매핑된 주소로 변환된 주소를 식별합니다.

show nat divert-table

NAT 전환 테이블을 표시하려면 특권 EXEC 모드에서 **show nat divert-table** 명령을 사용합니다.

show nat divert-table [**ipv6**] [**interface** *name*]

구문 설명

divert-table	NAT 전환 테이블을 표시합니다.
ipv6	(선택 사항) 전환 테이블에서 IPv6 항목을 표시합니다.
interface *name*	(선택 사항) 소스 인터페이스를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show nat divert-table 명령을 사용하여 NAT 전환 테이블의 런타임 표현을 표시할 수 있습니다. **ipv6** 선택적 키워드를 사용하여 전환 테이블에서 IPv6 항목을 확인할 수 있습니다. **interface** 선택적 키워드를 사용하여 특정 소스 인터페이스에 대한 NAT 전환 테이블을 확인할 수 있습니다.

예

다음은 **show nat divert-table** 명령의 샘플 출력입니다.

```
ciscoasa# show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
```

```
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

관련 명령

명령	설명
clear nat counters	NAT 정책 카운터를 지웁니다.
nat	하나의 인터페이스에서 다른 인터페이스의 매핑된 주소로 변환된 주소를 식별합니다.
show nat	NAT 정책의 런타임은 표현을 표시합니다.

show nat pool

NAT 풀 사용 통계를 표시하려면 특권 EXEC 모드에서 **show nat pool** 명령을 사용합니다.

show nat pool [**cluster**]

구문 설명

cluster	(선택 사항) ASA 클러스터링이 활성화된 경우 소유자 디바이스 및 백업 디바이스에 대한 현재 PAT 주소 할당을 표시합니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.
8.4(3)	확장된 PAT의 목적지 주소를 표시하도록 출력이 수정되었습니다. 또한 **flat** 및 **include-reserve** 키워드의 사용에 따라 PAT가 수정되었습니다.
9.0(1)	이제 이 명령은 IPv6 트래픽을 지원합니다. 소유자 디바이스 및 백업 디바이스에 대한 현재 PAT 주소 할당을 표시하도록 **cluster** 키워드가 추가되었습니다.

사용 지침

NAT 풀은 매핑된 각 프로토콜/IP 주소/포트 범위에 대해 생성됩니다. 여기서 포트 범위는 기본적으로 1~511, 512~1023 및 1024~65535입니다. **nat** 명령에서 PAT 풀에 대해 **flat** 키워드를 사용하면 더 크거나 작은 범위가 표시됩니다.

각 NAT 풀은 마지막으로 사용한 후 최소 10분간 존재합니다. **clear xlate**를 사용하여 변환을 지운 경우 10분 유지 타이머가 취소됩니다.

예

다음은 **show running-config object network** 명령을 통해 표시되는 동적 PAT 규칙에 의해 생성된 NAT 풀의 샘플 출력입니다.

```
ciscoasa(config)# show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

ciscoasa# show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
```

```
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

다음은 PAT 풀 **flat** 옵션 사용을 보여 주는 **show nat pool** 명령의 샘플 출력입니다. **include-reserve** 키워드가 없으면 두 개의 범위가 표시됩니다. 둘 중 낮은 범위는 1024 미만의 소스 포트가 동일한 포트에 매핑된 경우에 사용됩니다.

```
ciscoasa# show nat pool

ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

다음은 PAT 풀 **flat include-reserve** 옵션 사용을 보여 주는 **show nat pool** 명령의 샘플 출력입니다.

```
ciscoasa# show nat pool

ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

다음은 PAT 풀 **extended flat include-reserve** 옵션 사용을 보여 주는 **show nat pool** 명령의 샘플 출력입니다. 중요한 항목은 괄호 안의 주소입니다. 이는 PAT를 확장하는 데 사용되는 목적지 주소입니다.

```
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
UDP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

관련 명령

명령	설명
nat	하나의 인터페이스에서 다른 인터페이스의 매핑된 주소로 변환된 주소를 식별합니다.
show nat	NAT 정책 통계를 표시합니다.

show ntp associations

NTP 연계 정보를 보려면 특권 EXEC 모드에서 **show ntp associations** 명령을 사용합니다.

show ntp associations [**detail**]

구문 설명

detail	(선택 사항) 각 연계에 대한 추가 세부 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 **show ntp associations** 명령의 샘플 출력입니다.

```
ciscoasa> show ntp associations
     address         ref clock      st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

표 10-2에는 각 필드에 대한 설명이 나와 있습니다.

표 10-2 show ntp associations 필드

필드	설명
(화면 표시 줄의 선행 문자)	화면 표시 줄의 첫 번째 문자는 다음 문자 중 하나일 수 있습니다. • * - 이 피어에 동기화됨 • # - 거의 이 피어에 동기화됨 • + - 동기화 가능한 피어로 선택됨 • - - 선택할 수 있는 피어 중 하나임 • ~ - 피어가 정적으로 구성되었지만 동기화되지 않음
address	NTP 피어의 주소입니다.
ref clock	피어의 참조 클럭 주소입니다.
st	피어의 계층입니다.
when	피어로부터 마지막 NTP 패킷을 받은 이후의 시간입니다.
poll	폴링 간격(초)입니다.
reach	피어 연결 가능성(8진수 비트 문자열)입니다.
delay	피어에 대한 왕복 지연 시간(밀리초)입니다.
offset	로컬 클럭에 대한 피어 클럭의 상대 시간(밀리초)입니다.
disp	분산 값입니다.

다음은 **show ntp associations detail** 명령의 샘플 출력입니다.

```
ciscoasa> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62   16000.0
```

표 10-3에는 각 필드에 대한 설명이 나와 있습니다.

표 10-3 show ntp associations detail 필드

필드	설명
IP-address configured	서버(피어) IP 주소입니다.
(status)	• our_master - ASA가 이 피어에 동기화되었습니다. • selected - 동기화 가능한 피어로 선택되었습니다. • candidate - 선택할 수 있는 피어 중 하나입니다.
(sanity)	• sane - 피어가 기본 온전성 검사에 통과했습니다. • insane - 피어가 기본 온전성 검사에 실패했습니다.
(validity)	• valid - 피어가 유효한 것으로 간주됩니다. • invalid - 피어가 유효하지 않은 것으로 간주됩니다. • leap_add - 피어에서 윤초가 더해진다는 신호를 보냅니다. • leap-sub - 피어에서 윤초가 차감된다는 신호를 보냅니다.
stratum	피어의 계층입니다.
(reference peer)	unsynced - 피어가 다른 컴퓨터에 동기화되어 있지 않습니다. ref ID - 피어가 동기화된 컴퓨터의 주소입니다.
time	피어가 해당 마스터로부터 받은 마지막 타임스탬프입니다.
our mode client	피어에 상대적인 자신의 모드로서, 항상 클라이언트입니다.
peer mode server	서버에 상대적인 피어의 모드입니다.
our poll intvl	피어에 대한 자신의 폴링 간격입니다.
peer poll intvl	피어의 폴링 간격입니다.
root delay	루트 경로를 따라 발생하는 지연 시간(최종적인 계층 1의 시간 소스)입니다.
root disp	루트 경로의 분산입니다.
reach	피어 연결 가능성(8진수 비트 문자열)입니다.
sync dist	피어 동기화 거리입니다.
delay	피어에 대한 왕복 지연 시간입니다.
offset	자신의 클럭에 상대적인 피어 클럭의 오프셋입니다.
dispersion	피어 클럭의 분산입니다.
precision	피어 클럭의 정밀도(Hz)입니다.
version	피어에서 사용 중인 NTP 버전 번호입니다.
org time	시작 타임스탬프입니다.
rcv time	수신 타임스탬프입니다.
xmt time	전송 타임스탬프입니다.
filtdelay	각 샘플의 왕복 지연 시간(밀리초)입니다.
filtoffset	각 샘플의 클럭 오프셋(밀리초)입니다.
filterror	각 샘플의 근사치 오차입니다.

관련 명령

명령	설명
ntp authenticate	NTP 인증을 활성화합니다.
ntp authentication-key	암호화된 인증 키를 NTP 서버와 동기화하도록 설정합니다.
ntp server	NTP 서버를 식별합니다.
ntp trusted-key	NTP 서버로 인증하기 위해 패킷에서 사용할 ASA의 키 ID를 제공합니다.
show ntp status	NTP 연계 상태를 표시합니다.

show ntp status

각 NTP 연계 상태를 표시하려면 사용자 EXEC 모드에서 **show ntp status** 명령을 사용합니다.

show ntp status

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

예

다음은 **show ntp status** 명령의 샘플 출력입니다.

```
ciscoasa> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

표 10-4에는 각 필드에 대한 설명이 나와 있습니다.

표 10-4 show ntp status 필드

필드	설명
Clock	• synchronized - ASA가 NTP 서버에 동기화되어 있습니다. • unsynchronized - ASA가 NTP 서버에 동기화되어 있지 않습니다.
stratum	이 시스템의 NTP 계층입니다.
reference	ASA가 동기화된 NTP 서버의 주소입니다.
nominal freq	시스템 하드웨어 클럭의 정격 주파수입니다.
actual freq	시스템 하드웨어 클럭의 측정 주파수입니다.
precision	이 시스템의 클럭 정밀도(Hz)입니다.
reference time	참조 타임스탬프입니다.
clock offset	동기화된 피어에 대한 시스템 클럭의 오프셋입니다.
root delay	루트 클럭 경로를 따라 발생하는 총 지연 시간입니다.
root dispersion	루트 경로의 분산입니다.
peer dispersion	동기화된 피어의 분산입니다.

관련 명령

명령	설명
ntp authenticate	NTP 인증을 활성화합니다.
ntp authentication-key	암호화된 인증 키를 NTP 서버와 동기화하도록 설정합니다.
ntp server	NTP 서버를 식별합니다
ntp trusted-key	NTP 서버로 인증하기 위해 패킷에서 사용할 ASA의 키 ID를 제공합니다.
show ntp associations	ASA가 연계된 NTP 서버를 표시합니다.

show object-group

개체 그룹 정보 및 관련 적중 횟수(개체 그룹이 네트워크 개체 그룹 유형인 경우)를 표시하려면 특권 EXEC 모드에서 **show object-group** 명령을 사용합니다.

show object-group [**protocol** | **service** | **icmp-type** | **id** *object-group name*]

구문 설명

icmp-type	(선택 사항) ICMP 유형 개체 그룹입니다.
id	(선택 사항) 기존 개체 그룹을 식별합니다.
object-group name	(선택 사항) 지정된 이름을 개체 그룹에 할당합니다.
protocol	(선택 사항) 프로토콜 유형 개체 그룹입니다.
service	(선택 사항) 서비스 유형 개체입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.

사용 지침

개체 그룹이 네트워크 개체 그룹 유형인 경우, 개체 그룹을 표시하려는 일상적인 시도에서 개체 적중 횟수도 표시합니다. 서비스, 프로토콜 및 ICMP 유형 개체 그룹의 적중 횟수가 표시되지 않습니다.

예

다음은 **show object-group** 명령의 샘플 출력으로, "Anet"이라는 네트워크 개체 그룹에 대한 정보를 표시합니다.

```
ciscoasa# show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

다음은 **show object-group** 명령의 샘플 출력으로, 서비스 그룹에 대한 정보를 표시합니다.

```
ciscoasa (config)# show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp

   object-group protocol C-grp-proto
   protocol-object ospf
```

다음은 **show object-group** 명령의 샘플 출력으로, 프로토콜에 대한 정보를 표시합니다.

```
ciscoasa (config)# show object-group protocol
object-group protocol C-grp-proto
   protocol-object ospf
```

관련 명령

명령	설명
clear object-group	지정된 개체 그룹에 대한 네트워크 개체 적중 횟수를 지웁니다.
show access list	모든 액세스 목록, 관련 확장 액세스 목록 항목 및 적중 횟수를 표시합니다.

show ospf

OSPF 라우팅 프로세스에 대한 일반적인 정보를 표시하려면 특권 EXEC 모드에서 **show ospf** 명령을 사용합니다.

show ospf [*pid* [*area_id*]]

구문 설명

area_id	(선택 사항) OSPF 주소 범위와 연계된 영역의 ID입니다.
pid	(선택 사항) OSPF 프로세스의 ID입니다.

기본값

*pid*를 지정하지 않으면 모든 OSPF 프로세스가 나열됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

*pid*가 포함된 경우 지정한 라우팅 프로세스에 대한 정보만 포함됩니다.

예

다음은 **show ospf** 명령의 샘플 출력으로, 특정 OSPF 라우팅 프로세스에 대한 일반적인 정보를 표시합니다.

```
ciscoasa# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

다음은 **show ospf** 명령의 샘플 출력으로, 모든 OSPF 라우팅 프로세스에 대한 일반적인 정보를 표시합니다.

```
ciscoasa# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0

 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

관련 명령

명령	설명
router ospf	OSPF 라우팅을 활성화하고 전역 OSPF 라우팅 파라미터를 구성합니다.

show ospf border-routers

ABR 및 ASBR에 대한 내부 OSPF 라우팅 테이블 항목을 표시하려면 특권 EXEC 모드에서 **show ospf border-routers** 명령을 사용합니다.

show ospf border-routers

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

예

다음은 **show ospf border-routers** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

관련 명령

명령	설명
router ospf	OSPF 라우팅을 활성화하고 전역 OSPF 라우팅 파라미터를 구성합니다.

show ospf database

ASA의 OSPF 토폴로지 데이터베이스에 포함된 정보를 표시하려면 특권 EXEC 모드에서 **show ospf database** 명령을 사용합니다.

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originate** | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

구문 설명

addr	(선택 사항) 라우터 주소입니다.
adv-router	(선택 사항) 보급된 라우터입니다.
area_id	(선택 사항) OSPF 주소 범위와 연계된 영역의 ID입니다.
asbr-summary	(선택 사항) ASBR 목록 요약을 표시합니다.
database	데이터베이스 정보를 표시합니다.
database-summary	(선택 사항) 전체 데이터베이스 요약 목록을 표시합니다.
external	(선택 사항) 지정된 자동 시스템의 외부 경로를 표시합니다.
internal	(선택 사항) 지정된 자동 시스템의 내부 경로입니다.
lsid	(선택 사항) LSA ID입니다.
network	(선택 사항) 네트워크에 대한 OSPF 데이터베이스 정보를 표시합니다.
nssa-external	(선택 사항) 외부 NSSA(Not-So-Stubby-Area) 목록을 표시합니다.
pid	(선택 사항) OSPF 프로세스의 ID입니다.
router	(선택 사항) 라우터를 표시합니다.
self-originate	(선택 사항) 지정된 자동 시스템에 대한 정보를 표시합니다.
summary	(선택 사항) 목록에 대한 요약을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

OSPF 라우팅 관련 **show** 명령은 ASA의 특권 모드에서 사용할 수 있습니다. OSPF 컨피그레이션 모드가 아니어도 OSPF 관련 **show** 명령을 사용할 수 있습니다.

예

다음은 **show ospf database** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

다음은 **show ospf database asbr-summary** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

다음은 **show ospf database router** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
```

```
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

다음은 **show ospf database network** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

다음은 **show ospf database summary** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

다음은 **show ospf database external** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

관련 명령

명령	설명
router ospf	OSPF 라우팅을 활성화하고 전역 OSPF 라우팅 파라미터를 구성합니다.

show ospf flood-list

인터페이스로 플러딩되기를 기다리는 OSPF LSA 목록을 표시하려면 특권 EXEC 모드에서 **show ospf flood-list** 명령을 사용합니다.

show ospf flood-list *interface_name*

구문 설명

interface_name	네이버 정보를 표시할 인터페이스의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

OSPF 라우팅 관련 **show** 명령은 ASA의 특권 모드에서 사용할 수 있습니다. OSPF 컨피그레이션 모드가 아니어도 OSPF 관련 **show** 명령을 사용할 수 있습니다.

예

다음은 **show ospf flood-list** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

관련 명령

명령	설명
router ospf	OSPF 라우팅을 활성화하고 전역 OSPF 라우팅 파라미터를 구성합니다.

show ospf interface

OSPF 관련 인터페이스 정보를 표시하려면 특권 EXEC 모드에서 **show ospf interface** 명령을 사용합니다.

show ospf interface [*interface_name*]

구문 설명

interface_name	(선택 사항) OSPF 관련 정보를 표시할 인터페이스의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

interface_name 인수 없이 사용하면 모든 인터페이스에 대한 OSPF 정보가 표시됩니다.

예

다음은 **show ospf interface** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

관련 명령

명령	설명
interface	인터페이스 컨피그레이션 모드를 시작합니다.

show ospf nsf

OSPFv2 관련 NSF 정보를 표시하려면 특권 EXEC 모드에서 **show ospf nsf** 명령을 사용합니다.

show ospf nsf

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(1)	이 명령이 도입되었습니다.

예

다음은 **show ospf nsf** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
    Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
    OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```

관련 명령

명령	설명
nsf cisco	NSF 지원 라우터에서 Cisco NSF를 활성화합니다.
router ospf	OSPF 라우팅을 활성화하고 전역 OSPF 라우팅 파라미터를 구성합니다.

show ospf neighbor

인터페이스별로 OSPF 네이버 정보를 표시하려면 특권 EXEC 모드에서 **show ospf neighbor** 명령을 사용합니다.

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

구문 설명

detail	(선택 사항) 지정된 라우터에 대한 세부사항을 나열합니다.
interface_name	(선택 사항) 네이버 정보를 표시할 인터페이스의 이름입니다.
nbr_router_id	(선택 사항) 네이버 라우터의 라우터 ID입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

예

다음은 **show ospf neighbor** 명령의 샘플 출력입니다. 인터페이스별로 OSPF 네이버 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

다음은 **show ospf neighbor detail** 명령의 샘플 출력입니다. 지정된 OSPF 네이버에 대한 자세한 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
    Neighbor priority is 1, State is FULL, 46 state changes
    DR is 15.1.1.62 BDR is 15.1.1.60
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
    Dead timer due in 0:00:24
    Neighbor is up for 01:42:15
    Index 5/5, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

관련 명령

명령	설명
neighbor	비브로드캐스트 네트워크에 상호 연결되는 OSPF 라우터를 구성합니다.
router ospf	OSPF 라우팅을 활성화하고 전역 OSPF 라우팅 파라미터를 구성합니다.

show ospf request-list

라우터에서 요청한 모든 LSA 목록을 표시하려면 특권 EXEC 모드에서 **show ospf request-list** 명령을 사용합니다.

show ospf request-list *nbr_router_id interface_name*

구문 설명

interface_name	네이버 정보를 표시할 인터페이스의 이름입니다. 이 인터페이스에서 라우터가 요청한 모든 LSA 목록을 표시합니다.
nbr_router_id	네이버 라우터의 라우터 ID입니다. 이 네이버에서 라우터가 요청한 모든 LSA 목록을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

예

다음은 **show ospf request-list** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

관련 명령

명령	설명
show ospf retransmission-list	재전송 대기 중인 모든 LSA 목록을 표시합니다.

show ospf retransmission-list

재전송 대기 중인 모든 LSA 목록을 표시하려면 특권 EXEC 모드에서 **show ospf retransmission-list** 명령을 사용합니다.

show ospf retransmission-list *nbr_router_id interface_name*

구문 설명

interface_name	네이버 정보를 표시할 인터페이스의 이름입니다.
nbr_router_id	네이버 라우터의 라우터 ID입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

OSPF 라우팅 관련 **show** 명령은 ASA의 특권 모드에서 사용할 수 있습니다. OSPF 컨피그레이션 모드가 아니어도 OSPF 관련 **show** 명령을 사용할 수 있습니다.

nbr_router_id 인수는 이 네이버에 대해 재전송 대기 중인 모든 LSA 목록을 표시합니다.

interface_name 인수는 이 인터페이스에 대해 재전송 대기 중인 모든 LSA 목록을 표시합니다.

예

다음은 **show ospf retransmission-list** 명령의 샘플 출력입니다. 여기서, *nbr_router_id* 인수는 192.168.1.11이고, *if_name* 인수는 outside입니다.

```
ciscoasa# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

관련 명령

명령	설명
show ospf request-list	라우터에서 요청한 모든 LSA 목록을 표시합니다.

show ospf summary-address

OSPF 프로세스 중에 구성된 모든 요약 주소 재배포 정보 목록을 표시하려면 특권 EXEC 모드에서 **show ospf summary-address** 명령을 사용합니다.

show ospf summary-address

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

예

다음은 **show ospf summary-address** 명령의 샘플 출력입니다. OSPF 프로세스에 대한 요약 주소를 구성하기 전에 ID 5를 사용하여 모든 요약 주소 재배포 정보 목록을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

관련 명령

명령	설명
summary-address	OSPF의 집계 주소를 생성합니다.

show ospf traffic

특정 OSPF 인스턴스에서 처리된(보내거나 받은) 여러 유형의 패킷 목록을 표시하려면 특권 EXEC 모드에서 **show ospf traffic** 명령을 사용합니다. 이 명령을 사용하면 디버깅을 활성화하지 않고 처리 중인 여러 유형의 OSPF 패킷에 대한 스냅샷을 가져올 수 있습니다. 두 개의 OSPF 인스턴스가 구성된 경우 show ospf traffic 명령은 각 인스턴스의 프로세스 ID를 사용하여 두 인스턴스 모두에 대한 통계를 표시합니다. **show ospf** *process_id* **traffic** 명령을 사용하여 단일 인스턴스에 대한 통계를 표시할 수도 있습니다.

show ospf traffic

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하면 디버깅을 활성화하지 않고 처리 중인 여러 유형의 OSPF 패킷에 대한 스냅샷을 가져올 수 있습니다. 두 개의 OSPF 인스턴스가 구성된 경우 **show ospf traffic** 명령은 각 인스턴스의 프로세스 ID를 사용하여 두 인스턴스 모두에 대한 통계를 표시합니다. **show ospf** *process_id* **traffic** 명령을 사용하여 단일 인스턴스에 대한 통계를 표시할 수도 있습니다.

예

다음은 **show ospf traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf traffic

OSPF statistics (Process ID 70):

       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

관련 명령

명령	설명
show ospf virtual-links	OSPF 가상 링크의 파라미터 및 현재 상태를 표시합니다.

show ospf virtual-links

OSPF 가상 링크의 파라미터 및 현재 상태를 표시하려면 특권 EXEC 모드에서 **show ospf virtual-links** 명령을 사용합니다.

show ospf virtual-links

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

예

다음은 **show ospf virtual-links** 명령의 샘플 출력입니다.

```
ciscoasa# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

관련 명령

명령	설명
area virtual-link	OSPF 가상 링크를 정의합니다.

11 장

show pager through show route 명령

show pager

인터페이스의 기본 또는 고정 경로를 표시하려면 특권 EXEC 모드에서 **show pager** 명령을 사용합니다.

show pager

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
4.0(1)	이 명령이 도입되었습니다.

예

다음은 **show pager** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show pager
pager lines 0
```

관련 명령

명령	설명
clear configure pager	실행 중인 컨피그레이션에서 "---More---" 프롬프트가 표시되기 전에 텔넷 세션에 표시되도록 설정된 줄 수를 제거합니다.
show running-config pager	실행 중인 컨피그레이션에서 "---More---" 프롬프트가 표시되기 전에 텔넷 세션에 표시되도록 설정된 줄 수를 표시합니다.
terminal pager	줄 수가 "---More---" 프롬프트가 표시되기 전에 텔넷 세션에 표시되도록 설정합니다. 이 명령은 실행 중인 컨피그레이션에 저장되지 않습니다.

show password encryption

비밀번호 암호화 컨피그레이션 설정을 표시하려면 특권 EXEC 모드에서 **show password encryption** 명령을 사용합니다.

show password encryption

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.
8.4(1)	사용자 상황에서 비밀번호 암호화를 표시할 수 있습니다.

사용 지침

write memory 명령을 사용하여 키를 저장한 경우 키 해시 옆에 “saved”가 표시됩니다. 키가 없거나 실행 중인 컨피그레이션에서 키를 제거한 경우 해시 값 대신 “Not set”이 표시됩니다.

예

다음은 **show password encryption** 명령의 샘플 출력입니다.

```
ciscoasa# show password encryption
Password Encryption: Enabled
Master key hash: 0x35859e5e 0xc607399b 0x35a3438f 0x55474935 0xbec1ee7d(not saved)
```

관련 명령

명령	설명
password encryption aes	비밀번호 암호화를 활성화합니다.
key config-key password-encrypt	암호 키를 생성하는 데 사용되는 전달 구를 설정합니다.

show perfmon

ASA의 성능에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show perfmon** 명령을 사용합니다.

show perfmon [**detail**]

구문 설명

detail	(선택 사항) 추가 통계를 표시합니다. 이러한 통계는 Cisco Unified Firewall MIB의 전역 연결 개체 및 프로토콜별 연결 개체에서 생성된 통계와 일치합니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령에 대한 지원이 ASA에서 도입되었습니다.
7.2(1)	**detail** 키워드가 추가되었습니다.

사용 지침

이 명령 출력은 텔넷 세션에 표시되지 않습니다.

perfmon 명령은 정의된 간격으로 성능 통계를 지속적으로 표시합니다. **show perfmon** 명령을 사용하면 정보를 즉시 표시할 수 있습니다.

예

다음은 **show perfmon** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
```

```
AAA Author           0/s           0/s
AAA Account          0/s           0/s
```

다음은 **show perfmon detail** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s           0/s
Connections          0/s           0/s
TCP Conns            0/s           0/s
UDP Conns            0/s           0/s
URL Access           0/s           0/s
URL Server Req       0/s           0/s
TCP Fixup            0/s           0/s
HTTP Fixup           0/s           0/s
FTP Fixup            0/s           0/s
AAA Authen           0/s           0/s
AAA Author           0/s           0/s
AAA Account          0/s           0/s
TCP Intercept        0/s           0/s

SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

관련 명령

명령	설명
perfmon	정의된 간격으로 자세한 성능 모니터링 정보를 표시합니다.

show phone-proxy

phone-proxy 관련 정보를 표시하려면 글로벌 컨피그레이션 모드에서 **show phone-proxy** 명령을 사용합니다.

show phone-proxy [media-sessions [detail] | signaling-sessions [detai] | secure-phones]

구문 설명

detail	자세한 정보를 표시합니다.
media-sessions	Phone Proxy에 의해 저장된 해당 미디어 세션을 표시합니다. 또한 미디어 세션이 설정된 인터페이스에 대해 구성된 media-termination 주소를 표시합니다.
secure-phones	데이터베이스에 저장된 보안 모드를 지원하는 전화를 표시합니다.
signaling-sessions	Phone Proxy에 의해 저장된 해당 신호 처리 세션을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.
8.2(1)	**media-sessions** 키워드를 지정하면 미디어 세션이 설정된 인터페이스에 대해 구성된 media-termination 주소도 표시되도록 명령이 업데이트되었습니다.

예

다음 예에서는 **show phone proxy** 명령을 사용하여 Phone Proxy 관련 정보를 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address     Port  MAC            Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c 0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663 0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804 0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8 0:05:00 0:00:21
```

```
outside    128.107.254.69 49875 001b.0cad.1f69 0:05:00 0:00:04
ciscoasa(config)#
```

다음 예에서는 **show phone proxy** 명령을 사용하여 데이터베이스에 저장된 보안 모드 지원 전화를 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used

Interface/IP Address      MAC               Timeout    Idle
------------------------  ----------        ---------  ------
outside:69.181.112.219    001e.7ac4.da9c    0:05:00    0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00    0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00    0:00:09
ciscoasa(config)#
```

다음 예에서는 **show phone proxy** 명령을 사용하여 미디어 세션이 설정된 인터페이스에 대해 구성된 media-termination 주소 및 성공적인 호출의 출력을 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show phone-proxy media-sessions
Media-session: 128.106.254.3/1168 refcnt 6
  <---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
  <---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

관련 명령

명령	설명
debug phone-proxy	Phone Proxy 인스턴스에 대한 디버그 메시지를 표시합니다.
phone proxy	Phone Proxy 인스턴스를 구성합니다.

show pim df

RP(랑데부 지점) 또는 인터페이스에 대한 양방향 DF "winner"를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim df** 명령을 사용합니다.

show pim df [**winner**] [*rp_address* | *if_name*]

구문 설명

rp_address	다음 중 하나일 수 있습니다. • DNS(Domain Name System) 호스트 테이블에 정의되거나 도메인 **ipv4 host** 명령으로 정의된 RP 이름 • RP의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.
if_name	물리적 또는 논리적 인터페이스 이름입니다.
winner	(선택 사항) 각 RP의 인터페이스별로 선택된 DF를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 RP 쪽 적용 메트릭도 표시합니다.

예

다음은 **show pim df** 명령의 샘플 출력입니다.

```
ciscoasa# show pim df
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

그룹-프로토콜 매핑 테이블을 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim group-map** 명령을 사용합니다.

show pim group-map [**info-source**] [*group*]

구문 설명

group	(선택 사항) 다음 중 하나일 수 있습니다. • DNS 호스트 테이블에 정의되거나 도메인 **ipv4 host** 명령으로 정의된 멀티캐스트 그룹 이름 • 멀티캐스트 그룹의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.
info-source	(선택 사항) 그룹 범위 정보 소스를 표시합니다.

기본값

모든 그룹에 대한 그룹-프로토콜 매핑을 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 RP에 대한 모든 그룹 프로토콜 주소 매핑을 표시합니다. 매핑은 다른 클라이언트를 통해 ASA에서 학습됩니다.

ASA의 PIM 구현에는 매핑 테이블에 여러 특수 항목이 있습니다. Auto-rp 그룹 범위는 특별히 sparse-mode 그룹 범위에서 거부됩니다. 또한 SSM 그룹 범위는 sparse-mode에 속하지 않습니다. Link Local 멀티캐스트 그룹(224.0.0.0/24에 의해 정의된 대로 224.0.0.0~224.0.0.225)도 sparse-mode 그룹 범위에서 거부됩니다. 마지막 항목은 지정된 RP를 사용하는 Sparse-Mode의 나머지 모든 그룹을 표시합니다.

여러 RP가 **pim rp-address** 명령으로 구성된 경우 적절한 그룹 범위가 해당 RP와 함께 표시됩니다.

예

다음은 **show pim group-map** 명령의 샘플 출력입니다.

```
ciscoasa# show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

첫 번째 및 두 번째 줄에서 Auto-RP 그룹 범위는 특별히 sparse mode 그룹 범위에서 거부됩니다.

세 번째 줄에서 link-local 멀티캐스트 그룹(224.0.0.0/24에 의해 정의된 대로 224.0.0.0~224.0.0.225)도 sparse mode 그룹 범위에서 거부됩니다.

네 번째 줄에서 PIM-SSM(PIM 소스별 멀티캐스트) 그룹 범위는 232.0.0.0/8에 매핑됩니다.

마지막 항목은 나머지 모든 그룹이 RP 10.10.3.2에 매핑된 sparse mode에 있음을 보여 줍니다.

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.
pim rp-address	PIM RP(랑데부 지점)의 주소를 구성합니다.

show pim interface

PIM에 대한 인터페이스별 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim interface** 명령을 사용합니다.

show pim interface [*if_name* | **state-off** | **state-on**]

구문 설명

if_name	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.
state-off	(선택 사항) PIM이 비활성화된 인터페이스를 표시합니다.
state-on	(선택 사항) PIM이 활성화된 인터페이스를 표시합니다.

기본값

인터페이스를 지정하지 않으면 모든 인터페이스에 대한 PIM 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

ASA의 PIM 구현에서는 ASA 자체를 PIM 네이버로 간주합니다. 따라서 이 명령 출력의 neighbor count 열에 실제 네이버 수보다 하나 많은 값이 표시됩니다.

예

다음 예에서는 내부 인터페이스에 대한 PIM 정보를 표시합니다.

```
ciscoasa# show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

show pim join-prune statistic

PIM join/prune 집계 통계를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim join-prune statistics** 명령을 사용합니다.

show pim join-prune statistics [*if_name*]

구문 설명

if_name	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.

기본값

인터페이스를 지정하지 않으면 모든 인터페이스에 대한 join/prune 통계가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

clear pim counters 명령을 사용하여 PIM join/prune 통계를 지웁니다.

예

다음은 **show pim join-prune statistic** 명령의 샘플 출력입니다.

```
ciscoasa# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

             inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

관련 명령

명령	설명
clear pim counters	PIM 트래픽 카운터를 지웁니다.

show pim neighbor

PIM 네이버 테이블의 항목을 표시하려면 사용자 EXEC 또는 특권 EXEc 모드에서 **show pim neighbor** 명령을 사용합니다.

show pim neighbor [**count** | **detail**] [*interface*]

구문 설명

interface	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.
count	(선택 사항) 총 PIM 네이버 수 및 각 인터페이스의 PIM 네이버 수를 표시합니다.
detail	(선택 사항) upstream-detection hello 옵션을 통해 학습된 네이버의 추가 주소를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 PIM hello 메시지를 통해 이 라우터에 알려진 PIM 네이버를 확인하는 데 사용됩니다. 또한 이 명령은 인터페이스가 DR(지정된 라우터)임을 나타내고, 네이버가 양방향 작업을 수행할 수 있는 경우를 알려 줍니다.

ASA의 PIM 구현에서는 ASA 자체를 PIM 네이버로 간주합니다. 따라서 ASA 인터페이스가 이 명령의 출력에 표시됩니다. ASA의 IP 주소는 주소 옆에 별표로 표시됩니다.

예

다음은 **show pim neighbor** 명령의 샘플 출력입니다.

```
ciscoasa# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

show pim range-list

PIM에 대한 범위 목록 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim range-list** 명령을 사용합니다.

show pim range-list [*rp_address*]

구문 설명

rp_address	다음 중 하나일 수 있습니다. • DNS(Domain Name System) 호스트 테이블에 정의되거나 도메인 **ipv4 host** 명령으로 정의된 RP 이름 • RP의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 그룹 매핑에 대한 멀티캐스트 전달 모드를 확인하는 데 사용됩니다. 출력에는 범위의 RP(랑데부 지점) 주소(해당되는 경우)도 표시됩니다.

예

다음은 **show pim range-list** 명령의 샘플 출력입니다.

```
ciscoasa# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

관련 명령

명령	설명
show pim group-map	그룹-PIM 모드 매핑 및 활성 RP 정보를 표시합니다.

show pim topology

PIM 토폴로지 테이블 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim topology** 명령을 사용합니다.

show pim topology [*group*] [*source*]

구문 설명

group	(선택 사항) 다음 중 하나일 수 있습니다 . • DNS 호스트 테이블에 정의되거나 도메인 **ipv4 host** 명령으로 정의된 멀티캐스트 그룹 이름 • 멀티캐스트 그룹의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.
source	(선택 사항) 다음 중 하나일 수 있습니다 . • DNS 호스트 테이블에 정의되거나 도메인 **ipv4 host** 명령으로 정의된 멀티캐스트 소스 이름 • 멀티캐스트 소스의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.

기본값

모든 그룹 및 소스에 대한 토폴로지 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

PIM 토폴로지 테이블을 사용하여 각각 자체 인터페이스 목록이 있는 지정된 그룹 (*, G), (S, G) 및 (S, G)RPT에 대한 여러 항목을 표시할 수 있습니다.

PIM은 멀티캐스트 라우팅 프로토콜(예: PIM), 로컬 멤버십 프로토콜(예: IGMP(Internet Group Management Protocol)) 및 시스템의 멀티캐스트 포워딩 엔진 간의 통신을 중개하는 MRIB를 통해 이러한 항목의 내용을 전달합니다.

MRIB는 지정된 (S, G) 항목에 대해 데이터 패킷을 허용해야 하는 인터페이스 및 데이터 패킷을 전달해야 하는 인터페이스에 표시됩니다. 또한 MFIB(Multicast Forwarding Information Base) 테이블은 전달 중 패킷별 전달 작업을 결정하는 데 사용됩니다.

참고 전달 정보에는 **show mfib route** 명령을 사용합니다.

예

다음은 **show pim topology** 명령의 샘플 출력입니다.

```
ciscoasa# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

관련 명령

명령	설명
show mrib route	MRIB 테이블을 표시합니다.
show pim topology reserved	예약된 그룹에 대한 PIM 토폴로지 테이블 정보를 표시합니다.

show pim topology reserved

예약된 그룹에 대한 PIM 토폴로지 테이블 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim topology reserved** 명령을 사용합니다.

show pim topology reserved

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show pim topology reserved** 명령의 샘플 출력입니다.

```
ciscoasa# show pim topology reserved

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside             00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside              00:00:48  off II
```

관련 명령

명령	설명
show pim topology	PIM 토폴로지 테이블을 표시합니다.

show pim topology route-count

PIM 토폴로지 테이블 항목 수를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim topology route-count** 명령을 사용합니다.

show pim topology route-count [**detail**]

구문 설명

detail	(선택 사항) 그룹별로 보다 자세한 개수 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 PIM 토폴로지 테이블의 항목 수를 표시합니다. 항목에 대한 추가 정보를 표시하려면 **show pim topology** 명령을 사용합니다.

예

다음은 **show pim topology route-count** 명령의 샘플 출력입니다.

```
ciscoasa# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

관련 명령

명령	설명
show pim topology	PIM 토폴로지 테이블을 표시합니다.

show pim traffic

PIM 트래픽 카운터를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim traffic** 명령을 사용합니다.

show pim traffic

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

clear pim counters 명령을 사용하여 PIM 트래픽 카운터를 지웁니다.

예

다음은 **show pim traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

관련 명령

명령	설명
clear pim counters	PIM 트래픽 카운터를 지웁니다.

show pim tunnel

PIM 터널 인터페이스에 대한 정보를 표시하려면 사용자 EXEC 또는 특권 EXEC 모드에서 **show pim tunnel** 명령을 사용합니다.

show pim tunnel [*if_name*]

구문 설명

if_name	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.

기본값

인터페이스를 지정하지 않으면 모든 인터페이스에 대한 PIM 터널 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC 또는 특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

PIM 등록 패킷은 가상 캡슐화 터널 인터페이스를 통해 소스의 첫 번째 DR 라우터에서 RP로 전송됩니다. RP에서는 가상 역캡슐화 터널을 사용하여 PIM 등록 패킷의 수신 인터페이스를 표시합니다. 이 명령은 두 유형의 인터페이스 모두에 대한 터널 정보를 표시합니다.

등록 터널은 공유 트리를 통해 배포되도록 소스에서 RP로 전송되는 캡슐화된(PIM 등록 메시지에서) 멀티캐스트 패킷입니다. 등록은 SM에만 적용되며, SSM 및 양방향 PIM에는 적용되지 않습니다.

예

다음은 **show pim tunnel** 명령의 샘플 출력입니다.

```
ciscoasa# show pim tunnel

Interface     RP Address Source Address

Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

관련 명령

명령	설명
show pim topology	PIM 토폴로지 테이블을 표시합니다.

show port-channel

자세한 EtherChannel 정보 및 한 줄 요약 정보를 표시하거나 포트 및 포트 채널 정보를 표시하려면 특권 EXEC 모드에서 **show port-channel** 명령을 사용합니다.

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

구문 설명

brief	(기본값) 간략한 정보를 표시합니다.
channel_group_number	(선택 사항) EtherChannel 채널 그룹 번호(1~48)를 지정하고, 이 채널 그룹에 대한 정보만 표시합니다.
detail	(선택 사항) 자세한 정보를 표시합니다.
port	(선택 사항) 각 인터페이스에 대한 정보를 표시합니다.
protocol	(선택 사항) 활성화된 경우 LACP와 같은 EtherChannel 프로토콜을 표시합니다.
summary	(선택 사항) 포트 채널에 대한 요약을 표시합니다.

명령 기본값

기본값은 **brief**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

예

다음은 **show port-channel** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

다음은 **show port-channel summary** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel summary

Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

다음은 **show port-channel detail** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel detail
       Channel-group listing:
       -----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d

Partner's information:
```

```
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                           LACP port     Admin     Oper    Port        Port
Port      Flags   State    Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x1       0x1      0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

다음은 **show port-channel port** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel port
        Channel-group listing:
        ----------------------

Group: 1
----------
        Ports in the group:
        -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                           LACP port     Admin     Oper    Port        Port
Port      Flags   State    Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1      0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d


Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1
```

```
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d


Port: Gi3/3
-----------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

다음은 **show port-channel protocol** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel protocol
       Channel-group listing:
       ----------------------

Group: 1
----------
Protocol: LACP
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 활성 인터페이스의 최대 수를 지정합니다.
lacp port-priority	채널 그룹의 물리적 인터페이스에 대한 우선순위를 설정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel load-balance	부하 균형 알고리즘을 구성합니다.
port-channel min-bundle	포트-채널 인터페이스를 활성화하는 데 필요한 활성 인터페이스의 최소 수를 지정합니다.
show lacp	트래픽 통계, 시스템 식별자 및 네이버 정보와 같은 LACP 정보를 표시합니다.
show port-channel load-balance	지정된 파라미터 집합에 대해 선택된 멤버 인터페이스 및 해시 결과와 함께 포트-채널 부하 균형 정보를 표시합니다.

show port-channel load-balance

EtherChannel에 대해 현재 포트 채널 부하 균형 알고리즘을 표시하고, 선택적으로 지정된 파라미터 집합에 대해 선택된 멤버 인터페이스를 확인하려면 특권 EXEC 모드에서 이 명령을 입력합니다.

show port-channel *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **mac** | **l4port** | **mixed** | **vlan-only** *number*} *parameters*]

구문 설명

channel_group_number	EtherChannel 채널 그룹 번호(1~48)를 지정합니다.
hash-result	(선택 사항) 현재 부하 균형 알고리즘에 대한 해싱 값을 입력한 후에 선택한 멤버 인터페이스를 표시합니다.
ip	(선택 사항) IPv4 패킷 파라미터를 지정합니다.
ipv6	(선택 사항) IPv6 패킷 파라미터를 지정합니다.
l4port	(선택 사항) 포트 패킷 파라미터를 지정합니다.
mac	(선택 사항) MAC 주소 패킷 파라미터를 지정합니다.
mixed	(선택 사항) 포트 및/또는 VLAN ID와 함께 IP 또는 IPv6 파라미터의 조합을 지정합니다.
parameters	(선택 사항) 유형에 따른 패킷 파라미터입니다. 예를 들어 **ip**의 경우 소스 IP 주소, 대상 IP 주소 및/또는 VLAN ID를 지정할 수 있습니다.
vlan-only	(선택 사항) 패킷에 대한 VLAN ID를 지정합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

사용 지침

기본적으로 ASA는 패킷의 소스 및 대상 IP 주소(**src-dst-ip**)에 따라 인터페이스에서 패킷 부하의 균형을 유지합니다. 알고리즘을 변경하려면 **port-channel load-balance** 명령을 참고하십시오.

이 명령을 사용하여 현재 부하 균형 알고리즘을 볼 수 있지만 **hash-result** 키워드를 사용하면 지정된 파라미터로 패킷에 대해 선택할 멤버 인터페이스를 테스트할 수도 있습니다. 이 명령은 현재 부하 균형 알고리즘에 대해서만 테스트합니다. 예를 들어 알고리즘이 src-dst-ip인 경우 IPv4 또는 IPv6 소스 및 대상 IP 주소를 입력합니다. 현재 알고리즘에서 사용되지 않는 다른 인수를 입력하면 해당 인수가 무시되고 알고리즘에서 실제로 사용되는 입력되지 않은 값이 기본적으로 0으로 설정됩니다. 예를 들어 알고리즘이 vlan-src-ip인 경우 다음을 입력합니다.

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

다음을 입력하면 vlan-src-ip 알고리즘이 소스 IP 주소 0.0.0.0 및 VLAN 0을 가정하고, 입력한 값을 무시합니다.

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

예

다음은 **show port-channel 1 load-balance** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

다음은 입력한 파라미터가 현재 알고리즘(src-dst-ip)과 일치하는 경우 **show port-channel 1 load-balance hash-result** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination
10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

다음은 입력한 파라미터가 현재 알고리즘(src-dst-ip)과 일치하지 않고 해시에서 0 값을 사용하는 경우 **show port-channel 1 load-balance hash-result** 명령의 샘플 출력입니다.

```
ciscoasa# show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 활성 인터페이스의 최대 수를 지정합니다.
lacp port-priority	채널 그룹의 물리적 인터페이스에 대한 우선순위를 설정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel load-balance	부하 균형 알고리즘을 구성합니다.
port-channel min-bundle	포트-채널 인터페이스를 활성화하는 데 필요한 활성 인터페이스의 최소 수를 지정합니다.
show lacp	트래픽 통계, 시스템 식별자 및 네이버 정보와 같은 LACP 정보를 표시합니다.
show port-channel	EtherChannel 정보를 자세한 양식과 한 줄 요약 양식으로 표시합니다. 이 명령은 포트 및 포트-채널 정보도 표시합니다.

show power inline

PoE 인터페이스가 있는 모델(예: ASA 5505)의 경우 인터페이스의 전원 상태를 표시하려면 사용자 EXEC 모드에서 **show power inline** 명령을 사용합니다.

show power inline

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

PoE 인터페이스를 사용하여 IP 전화기 또는 무선 액세스 포인트와 같은 전원이 필요한 디바이스에 연결할 수 있습니다.

예

다음은 **show power inline** 명령의 샘플 출력입니다.

```
ciscoasa# show power inline

  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

표 11-1에는 각 필드에 대한 설명이 나와 있습니다.

표 11-1 show power inline 필드

필드	설명
Interface	사용 가능한 PoE가 없는 인터페이스를 포함하여 ASA의 모든 인터페이스를 표시합니다.
Power	전원이 켜져 있는지 또는 꺼져 있는지 표시합니다. 디바이스에 전원이 필요하지 않거나, 해당 인터페이스에 디바이스가 없거나, 인터페이스가 종료된 경우에는 값이 Off. 인터페이스가 PoE를 지원하지 않는 경우에는 값이 n/a입니다.
Device	전원을 공급받는 디바이스의 유형(Cisco 또는 IEEE)을 표시합니다. 디바이스가 전원을 공급받지 않는 경우에는 값이 n/a입니다. 디바이스가 Cisco 전력 디바이스인 경우에는 Cisco가 표시됩니다. IEEE는 디바이스가 IEEE 802.3af- 호환 전력 디바이스임을 나타냅니다.

관련 명령

명령	설명
clear configure interface	인터페이스에 대한 모든 컨피그레이션을 지웁니다.
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show priority-queue statistics

인터페이스에 대한 우선순위 대기열 통계를 표시하려면 특권 EXEC 모드에서 **show priority-queue statistics** 명령을 사용합니다.

show priority-queue statistics [*interface-name*]

구문 설명

interface-name	(선택 사항) 최상의 결과 및 저지연 대기열 정보를 표시할 인터페이스의 이름을 지정합니다.

기본값

인터페이스 이름을 생략하면 구성된 모든 인터페이스에 대한 우선순위 대기열 통계가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

이 예에서는 test라는 인터페이스에 대한 **show priority-queue statistics** 명령 사용 및 명령 출력을 보여 줍니다. 이 출력에서 BE는 최상의 결과 대기열을 나타내고, LLQ는 저지연 대기열을 나타냅니다.

```
ciscoasa# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
ciscoasa#
```

관련 명령

명령	설명
clear configure priority-queue	명명된 인터페이스에서 우선순위 대기열 컨피그레이션을 제거합니다.
clear priority-queue statistics	하나의 인터페이스 또는 구성된 모든 인터페이스에 대한 우선순위 대기열 통계 카운터를 지웁니다.
priority-queue	인터페이스에서 우선순위 대기열을 구성합니다.
show running-config priority-queue	명명된 인터페이스의 현재 우선순위 대기열 컨피그레이션을 표시합니다.

show processes

ASA에서 실행되는 프로세스 목록을 표시하려면 특권 EXEC 모드에서 **show processes** 명령을 사용합니다.

show processes [**cpu-usage** [[**non-zero**][**sorted**]] [**cpu-hog** | **memory** | **internals**]

구문 설명

cpu-hog	CPU를 호그(즉, 100밀리초 넘게 CPU를 사용)하고 있는 프로세스 수 및 세부 정보를 표시합니다.
cpu-usage	지난 5초, 1분 및 5분 동안 각 프로세스에서 사용한 CPU의 백분율을 표시합니다.
internals	각 프로세스에 대한 내부 세부 정보를 표시합니다.
memory	각 프로세스의 메모리 할당을 표시합니다.
non-zero	(선택 사항) CPU 사용량이 0이 아닌 프로세스를 표시합니다.
sorted	(선택 사항) 프로세스에 대한 정렬된 CPU 사용량을 표시합니다.

기본값

기본적으로 이 명령은 ASA에서 실행되는 프로세스를 표시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.0(4)	1밀리초 이내의 정확도를 표시하도록 런타임 값이 향상되었습니다.
7.2(1)	CPU를 호그하는 프로세스에 대한 보다 자세한 정보를 표시하도록 출력이 향상되었습니다.
8.0(1)	**cpu-usage** 키워드가 추가되었습니다.
9.2(1)	CPU 호그(hog) 감지 정보를 표시하도록 출력이 향상되었습니다.

사용 지침

프로세스가 몇 가지 명령만 필요한 경량 스레드입니다. **show process** 명령은 ASA에서 실행 중인 프로세스 목록을 다음과 같이 표시합니다.

명령	표시되는 데이터	설명
show processes	PC	프로그램 카운터입니다.
show processes	Stack Pointer	스택 포인터입니다.
show processes	STATE	스레드 대기열의 주소입니다.

명령	표시되는 데이터	설명
show processes	Runtime	스레드가 실행된 밀리초입니다(CPU 클럭 주기 기반). 정확도는 클럭 틱(10ms 해상도) 대신 CPU 클럭 주기(<10ns 해상도)를 기반으로 프로세스 CPU 사용량을 완전하고 정확하게 계산하는 데 1밀리초 이내가 소요됩니다.
show processes	SBASE	스택 기본 주소입니다.
show processes	Stack	현재 사용 중인 바이트 수 및 스택의 총 크기입니다.
show processes	Process	스레드의 기능입니다.
show processes cpu-usage	MAXHOG	최대 CPU 호그 런타임(밀리초)입니다.
show processes cpu-usage	NUMHOG	CPU 호그 실행 횟수입니다.
show processes cpu-usage	LASTHOG	마지막 CPU 호그 런타임(밀리초)입니다.
show processes cpu-usage	PC	CPU 호깅 프로세스의 명령 포인터입니다.
show processes cpu-usage	Traceback	CPU 호깅 프로세스의 스택 추적입니다. Traceback에는 최대 14개의 주소가 있을 수 있습니다.
show processes internals	Invoked Calls	스케줄러에서 프로세스를 실행한 횟수입니다.
show processes internals	Giveups	프로세스에서 스케줄러로 CPU를 다시 양보한 횟수입니다.

show processes cpu-usage 명령을 사용하여 ASA에서 ASA의 CPU를 사용 중일 수 있는 특정 프로세스로 범위를 좁힐 수 있습니다. **sorted** 및 **non-zero** 명령을 사용하여 **show processes cpu-usage** 명령의 출력을 추가로 사용자 지정할 수 있습니다.

scheduler 및 total summary 줄에서 **show proccesses** 명령을 두 번 연속으로 실행하고 출력을 비교하여 다음을 확인할 수 있습니다.

- CPU의 100% 소비
- 각 스레드에서 사용하는 CPU 백분율 - 스레드의 런타임 델타와 총 런타임 델타를 비교하여 확인

예

다음 예에서는 ASA에서 실행 중인 프로세스 목록을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total
```

다음 예에서는 각 프로세스에서 사용하는 CPU 백분율을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show proc cpu-usage non-zero
PC         Thread     5Sec    1Min    5Min    Process
0818af8e   d482f92c   0.1%    0.1%    0.1%    Dispatch Unit
08bae136   d48180f0   0.1%    0.0%    0.2%    ssh
-------------------------------------
```

다음 예에서는 CPU를 호그 중인 프로세스 수 및 세부 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show processes cpu-hog
Granular CPU hog detection currently running, started at 15:41:16 UTC Jan 6 2014.
    Sample count: 10000 Threshold: 10ms
Granular CPU hog detection completed at 15:41:16 UTC Jan 6 2014.
    Sample count: 10000 Threshold: 10ms
```

CPU 호그 Traceback의 나머지 부분은 다음과 같습니다.

```
Process:      DATAPATH-0-2042, NUMHOG: 430, MAXHOG: 22, LASTHOG: 2
LASTHOG At:   15:42:21 UTC Jan 6 2014
PC:           0x0000000000000000 (suspend)
Call stack:   0x000000000041c98c  0x000000000041cc99  0x000000000069b0f0
              0x00000000013619af  0x000000000136cbbd  0x0000000001372203
              0x00007ffffeab2f3a
              Interrupt based hog #1
              Hog #1, traceback #1, at:   15:41:16 UTC Jan 6 2014, hog 20 ms
              PC:           0x0000000000eb616b
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000ebcf71
                            0x0000000000ebc5ab  0x0000000000ebcb0e  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af
              Hog #1, traceback #2, at:   15:41:16 UTC Jan 6 2014, hog 21 ms
              PC:           0x0000000000e8fc41
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af  0x000000000136cbbd
                            0x0000000001372203  0x00007ffffeab2f3a
              Interrupt based hog #2
              Hog #2, traceback #1, at:   15:41:36 UTC Jan 6 2014, hog 9 ms
              PC:           0x0000000000eb6167
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x0000000000ebcf71
                            0x0000000000ebc5ab  0x0000000000ebcb0e  0x0000000000e17410
                            0x0000000000e19ac4  0x0000000000e19e55  0x0000000000ca50b4
                            0x0000000001344419  0x000000000069b315  0x000000000069be9e
                            0x000000000069b0a4  0x00000000013619af
              Interrupt based hog #3
              Hog #3, traceback #1, at:   15:42:21 UTC Jan 6 2014, hog 2 ms
              PC:           0x000000000068a223
              Call stack:   0x0000000001360281  0x00007ffffeaba5f0  0x000000000069bbba
                            0x000000000069b0a4  0x00000000013619af  0x000000000136cbbd
                            0x0000000001372203  0x00007ffffeab2f3a
```

다음 예에서는 각 프로세스에 대한 메모리 할당을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show processes memory

-------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
-------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
```

다음 예에서는 각 프로세스의 내부 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show processes internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
         237          235  uauth
(other lines deleted for brevity)
```

관련 명령

명령	설명
show cpu	CPU 사용 정보를 표시합니다.

show quota management-session

현재 관리 세션에 대한 통계를 표시하려면 특권 EXEC 모드에서 **show quota management-session** 명령을 사용합니다.

show quota management-session

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.1(2)	이 명령이 도입되었습니다.

사용 지침

이 명령은 현재 관리 세션에 대한 다음 통계를 표시합니다.

- 제한
- 경고 수준
- 현재 개수
- 상위 워터마크
- 생성된 경고 수
- 생성된 오류 수

예

다음 예에서는 현재 관리 세션에 대한 통계를 보여 줍니다.

```
ciscoasa# show quota management-session
quota management-session limit 250
quota management-session warning level 225
quota management-session level 1
quota management-session high water 1
quota management-session errors 0
quota management-session warnings 0
```

관련 명령

명령	설명
show running-config quota management-session	관리 세션 할당량의 현재 값을 표시합니다.
quota management-session	디바이스에서 허용되는 동시 ASDM, SSH 및 텔넷 세션 수를 설정합니다.

show reload

ASA의 다시 로드 상태를 표시하려면 특권 EXEC 모드에서 **show reload** 명령을 사용합니다.

show reload

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 사용 지침이 없습니다.

예

다음 예에서는 4월 20일 토요일 오전 12시에 다시 로드가 예약되었음을 보여 줍니다.

```
ciscoasa# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

관련 명령

명령	설명
reload	재부팅하고 컨피그레이션을 다시 로드합니다.

show resource allocation

모든 클래스 및 클래스 멤버의 각 리소스에 대한 리소스 할당을 표시하려면 특권 EXEC 모드에서 **show resource allocation** 명령을 사용합니다.

show resource allocation [**detail**]

구문 설명

detail	추가 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.
9.0(1)	각 상황의 최대 라우팅 테이블 항목 수를 설정하기 위해 새 리소스 클래스인 routes가 생성되었습니다. 각 상황의 최대 Site-to-Site VPN 터널 수를 설정하기 위해 새 리소스 유형인 vpn other 및 vpn burst other가 생성되었습니다.

사용 지침

이 명령은 리소스 할당을 표시하지만 사용 중인 실제 리소스는 표시하지 않습니다. 실제 리소스 사용량에 대한 자세한 내용은 **show resource usage** 명령을 참고하십시오.

예

다음은 **show resource allocation** 명령의 샘플 출력입니다. 각 리소스의 총 할당이 절대값과 사용 가능한 시스템 리소스의 백분율로 표시됩니다.

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000         30.50%
 Hosts                      78842           N/A
 SSH                           35         35.00%
 Telnet                        35         35.00%
 Routes                     25000          0.00%
 Xlates                     91749           N/A
 Other VPN Sessions            20          2.66%
 Other VPN Burst               20          2.66%
 All                    unlimited
```

표 11-2에는 각 필드에 대한 설명이 나와 있습니다.

표 11-2 show resource allocation 필드

필드	설명
Resource	제한할 수 있는 리소스의 이름입니다.
Total	모든 상황에서 할당된 총 리소스 양입니다. 이는 동시 인스턴스 또는 초당 인스턴스의 절대 수입니다. 클래스 정의에서 백분율을 지정한 경우에는 ASA에서 백분율을 절대 수로 변환합니다.
% of Avail	모든 상황에서 할당된 전체 시스템 리소스의 백분율입니다(사용 가능한 경우). 리소스에 시스템 제한이 없는 경우에는 이 열에 N/A가 표시됩니다.

다음은 **show resource allocation detail** 명령의 샘플 출력입니다.

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin     Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%
```

```
Telnet            default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                             20     20.00%
Routes            default          all       C  unlimited                 N/A
                  gold               1       D  unlimited          5      N/A
                  silver             1      CA         10         10      N/A
                  bronze             0      CA          5                 N/A
                  All Contexts:      3                             20      N/A

Xlates            default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      23040      23040     N/A
                  bronze             0      CA      11520
                  All Contexts:      3                          23040     N/A

mac-addresses     default          all       C      65535
                  gold               1       D      65535      65535    100.00%
                  silver             1      CA       6553       6553      9.99%
                  bronze             0      CA       3276
                  All Contexts:      3                         137623    209.99%
```

표 11-3에는 각 필드에 대한 설명이 나와 있습니다.

표 11-3 show resource allocation detail 필드

필드	설명
Resource	제한할 수 있는 리소스의 이름입니다.
Class	기본 클래스를 비롯한 각 클래스의 이름입니다. All contexts 필드에는 모든 클래스에 걸친 전체 값이 표시됩니다.
Mmbrs	각 클래스에 할당된 상황 수입니다.
Origin	다음과 같은 리소스 제한의 출처입니다. • A - 개별 리소스 대신 **all** 옵션을 사용하여 이 제한을 설정합니다. • C - 이 제한은 멤버 클래스에서 파생됩니다. • D - 이 제한은 멤버 클래스에 정의되지 않고 기본 클래스에서 파생됩니다. 기본 클래스에 할당된 상황의 경우 이 값은 "D" 대신 "C"가 됩니다 ASA에서는 "A"를 "C" 또는 "D"와 조합할 수 있습니다.
Limit	상황별 리소스 제한(절대 수)입니다. 클래스 정의에서 백분율을 지정한 경우에는 ASA에서 백분율을 절대 수로 변환합니다.
Total	클래스의 모든 상황에서 할당된 총 리소스 양입니다. 이는 동시 인스턴스 또는 초당 인스턴스의 절대 수입니다. 리소스가 제한되지 않은 경우에는 비어 있습니다.
% of Avail	클래스의 모든 상황에서 할당된 전체 시스템 리소스의 백분율입니다(사용 가능한 경우). 리소스가 제한되지 않은 경우에는 비어 있습니다. 리소스에 시스템 제한이 없는 경우에는 이 열에 N/A가 표시됩니다.

관련 명령

명령	설명
class	리소스 클래스를 생성합니다.
context	보안 상황을 추가합니다.
limit-resource	클래스에 대한 리소스 제한을 설정합니다.
show resource types	제한을 설정할 수 있는 리소스 유형을 표시합니다.
show resource usage	ASA의 리소스 사용량을 표시합니다.

show resource types

ASA에서 사용량을 추적하는 리소스 유형을 표시하려면 특권 EXEC 모드에서 **show resource types** 명령을 사용합니다.

show resource types

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.2(1)	이 명령은 각 상황에 대해 관리할 수 있는 추가 리소스 유형을 표시합니다.
9.0(1)	각 상황의 최대 라우팅 테이블 항목 수를 설정하기 위해 새 리소스 클래스인 routes가 생성되었습니다. 각 상황의 최대 Site-to-Site VPN 터널 수를 설정하기 위해 새 리소스 유형인 vpn other 및 vpn burst other가 생성되었습니다.

예

다음 샘플 표시는 리소스 유형을 보여 줍니다.

```
ciscoasa# show resource types

Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  Routes          Routing Table Entries
  Other-vpn       Other VPN licenses
  Other-vpn-burst Allowable burst for Other VPN licenses
  All             All Resources
```

관련 명령

명령	설명
clear resource usage	리소스 사용 통계를 지웁니다.
context	보안 상황을 추가합니다.
show resource usage	ASA의 리소스 사용량을 표시합니다.

show resource usage

ASA의 리소스 사용 또는 여러 모드의 각 상황에 대한 리소스 사용을 표시하려면 특권 EXEC 모드에서 **show resource usage** 명령을 사용합니다.

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system** | **detail**] [**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

구문 설명

context *context_name*	(다중 모드에만 해당) 통계를 확인할 상황 이름을 지정합니다. 모든 상황의 경우 **all**을 지정합니다. ASA에서 각 상황에 대한 상황 사용량을 나열합니다.
count_threshold	표시되는 리소스 수의 하한을 설정합니다. 기본값은 1입니다. 리소스 사용이 설정한 숫자보다 낮으면 해당 리소스는 표시되지 않습니다. 카운터 이름에 대해 **all**을 지정한 경우 *count_threshold*는 현재 사용량에 적용됩니다. **참고** 모든 리소스를 표시하려면 *count_threshold*를 **0**으로 설정합니다.
counter *counter_name*	다음 카운터 유형의 개수를 표시합니다. • **current** - 활성 동시 인스턴스 또는 리소스의 현재 비율을 표시합니다. • **peak** - **clear resource usage** 명령 또는 디바이스 재부팅으로 인해 통계가 마지막으로 지워진 이후의 피크 동시 인스턴스 또는 리소스의 피크 비율을 표시합니다. • **denied** - Limit 열에 표시된 리소스 제한을 초과했기 때문에 거부된 인스턴스 수를 표시합니다. • **all** - (기본값) 모든 통계를 표시합니다.
detail	관리할 수 없는 리소스를 포함하여 모든 리소스의 사용량을 표시합니다. 예를 들어 TCP 가로채기 수를 볼 수 있습니다.

resource [**rate**] *resource_name*	특정 리소스의 사용량을 표시합니다. 모든 리소스의 경우 **all**(기본값)을 지정합니다. 리소스 사용률을 표시하려면 **rate**를 지정합니다. 비율로 측정되는 리소스에는 **conns**, **inspects**, **syslogs** 등이 있습니다. 이러한 리소스 유형에는 **rate** 키워드를 지정해야 합니다. conns 리소스는 동시 연결 수로도 측정되지만 초당 연결 수를 보려면 **rate** 키워드를 사용해야 합니다. 리소스 유형은 다음과 같습니다. • **asdm** - ASDM 관리 세션입니다. • **conns** - 호스트 하나와 여러 다른 호스트 간의 연결을 포함하여 두 호스트 간의 TCP 또는 UDP 연결입니다. • **inspects** - 애플리케이션 검사입니다. • **hosts** - ASA를 통해 연결할 수 있는 호스트입니다. • **mac-addresses** - 투명 방화벽 모드에서 MAC 주소 테이블에 허용되는 MAC 주소 수입니다. • **routes** - 라우팅 테이블 항목입니다. • **ssh** - SSH 세션입니다. • **syslogs** - syslog 메시지입니다. • **telnet** - 텔넷 세션입니다. • (다중 모드에만 해당) **VPN Other** - Site-to-Site VPN 세션입니다. • (다중 모드에만 해당) **VPN Burst Other** - Site-to-Site VPN 버스트 세션입니다. • **xlates** - NAT 변환입니다.
summary	(다중 모드에만 해당) 통합된 모든 상황 사용량을 표시합니다.
system	(다중 모드에만 해당) 통합된 모든 상황 사용량을 표시하되, 통합된 상황 제한 대신 리소스에 대한 시스템 제한을 표시합니다.
top *n*	(다중 모드에만 해당) 지정한 리소스의 상위 *n*명 사용자인 상황을 표시합니다. 이 옵션을 사용하는 경우 **resource all**이 아니라 단일 리소스 유형을 지정해야 합니다.

기본값

다중 상황 모드의 경우 기본 상황은 모든 상황에 대한 리소스 사용량을 표시하는 **all**입니다. 단일 모드의 경우 상황 이름이 무시되고 출력에 “context”가 “System”으로 표시됩니다.

기본 리소스 이름은 모든 리소스 유형을 표시하는 **all**입니다.

기본 카운터 이름은 모든 통계를 표시하는 **all**입니다.

기본 개수 임계값은 **1**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.2(1)	각 상황에 대한 리소스를 제한할 수 있으므로 이 명령은 거부된 리소스를 표시합니다.
9.0(1)	각 상황의 최대 라우팅 테이블 항목 수를 설정하기 위해 새 리소스 클래스인 routes가 생성되었습니다. 각 상황의 최대 Site-to-Site VPN 터널 수를 설정하기 위해 새 리소스 유형인 vpn other 및 vpn burst other가 생성되었습니다.

예

다음은 admin 상황에 대한 리소스 사용량을 표시하는 **show resource usage context** 명령의 샘플 출력입니다.

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

다음은 모든 상황 및 모든 리소스에 대한 리소스 사용량을 표시하는 **show resource usage summary** 명령의 샘플 출력입니다. 이 샘플에서는 6개의 상황에 대한 제한을 보여 줍니다.

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
Other VPN Sessions          0           10         10        740 Summary
Other VPN Burst             0           10         10        730 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

다음은 모든 상황에 대한 리소스 사용량을 표시하되, 통합된 상황 제한 대신 시스템 제한을 표시하는 **show resource usage system** 명령의 샘플 출력입니다.

```
ciscoasa# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

다음은 관리할 수 있는 리소스뿐만 아니라 모든 리소스를 표시하는 **show resource usage detail counter all 0** 명령의 샘플 출력입니다.

```
ciscoasa# show resource usage detail counter all 0

Resource              Current         Peak      Limit         Denied Context
memory                1012028      1538428  unlimited              0 admin
chunk:aaa                   0            0  unlimited              0 admin
chunk:aaa_queue             0            0  unlimited              0 admin
chunk:acct                  0            0  unlimited              0 admin
chunk:channels             25           39  unlimited              0 admin
chunk:CIFS                  0            0  unlimited              0 admin
chunk:conn                  0            0  unlimited              0 admin
chunk:crypto-conn           0            0  unlimited              0 admin
chunk:dbgtrace              1            2  unlimited              0 admin
chunk:dhcpd-radix           0            0  unlimited              0 admin
chunk:dhcp-relay-r          0            0  unlimited              0 admin
chunk:dhcp-lease-s          0            0  unlimited              0 admin
chunk:dnat                  0            0  unlimited              0 admin
chunk:ether                 0            0  unlimited              0 admin
chunk:est                   0            0  unlimited              0 admin

...

Telnet                      0            0          5              0 admin
SSH                         1            1          5              0 admin
ASDM                        0            1          5              0 admin
Syslogs [rate]              0           68  unlimited              0 admin
aaa rate                    0            0  unlimited              0 admin
url filter rate             0            0  unlimited              0 admin
Conns                       1            6  unlimited              0 admin
Xlates                      0            0  unlimited              0 admin
tcp conns                   0            0  unlimited              0 admin
Hosts                       2            3  unlimited              0 admin
Other VPN Sessions          0           10        750            740 admin
Other VPN Burst             0           10        750            730 admin
udp conns                   0            0  unlimited              0 admin
smtp-fixups                 0            0  unlimited              0 admin
Conns [rate]                0            7  unlimited              0 admin
establisheds                0            0  unlimited              0 admin
pps                         0            0  unlimited              0 admin
syslog rate                 0            0  unlimited              0 admin
bps                         0            0  unlimited              0 admin
Fixups [rate]               0            0  unlimited              0 admin
non tcp/udp conns           0            0  unlimited              0 admin
tcp-intercepts              0            0  unlimited              0 admin
globals                     0            0  unlimited              0 admin
np-statics                  0            0  unlimited              0 admin
statics                     0            0  unlimited              0 admin
nats                        0            0  unlimited              0 admin
ace-rules                   0            0        N/A              0 admin
aaa-user-aces               0            0        N/A              0 admin
filter-rules                0            0        N/A              0 admin
est-rules                   0            0        N/A              0 admin
aaa-rules                   0            0        N/A              0 admin
console-access-rul          0            0        N/A              0 admin
policy-nat-rules            0            0        N/A              0 admin
fixup-rules                 0            0        N/A              0 admin
aaa-uxlates                 0            0  unlimited              0 admin
CP-Traffic:IP               0            0  unlimited              0 admin
CP-Traffic:ARP              0            0  unlimited              0 admin
CP-Traffic:Fixup            0            0  unlimited              0 admin
CP-Traffic:NPCP             0            0  unlimited              0 admin
CP-Traffic:Unknown          0            0  unlimited              0 admin
```

관련 명령

명령	설명
class	리소스 클래스를 생성합니다.
clear resource usage	리소스 사용 통계를 지웁니다.
context	보안 상황을 추가합니다.
limit-resource	클래스에 대한 리소스 제한을 설정합니다.
show resource types	리소스 유형 목록을 표시합니다.

show rest-api agent

REST API 에이전트가 현재 활성화되어 있는지 확인하려면 특권 EXEC 모드에서 **show rest-api agent** 명령을 사용합니다.

show rest-api agent

참고 이 명령은 ASA 5506-X 및 ASA 5508-X를 제외하고 모든 버전의 ASAv, ASA 5585-X 및 모든 ASA 5500-X Series 디바이스에서 지원됩니다.

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	예	—	—

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 REST API 에이전트가 현재 활성화되어 있는지 확인할 수 있습니다.

예

다음 예에서는 REST API 에이전트가 활성화되어 있음을 나타냅니다.

```
ciscoasa(config)# show rest-api agent
REST API agent is currently enabled.
```

에이전트가 비활성화된 경우 "REST API 에이전트가 현재 비활성화되어 있습니다."라는 메시지가 표시됩니다.

관련 명령

명령	설명
rest-api	REST API 패키지를 확인하고 설치합니다. REST API 에이전트를 활성화합니다.
show version	REST API 에이전트가 활성화된 경우 해당 버전 번호가 **show version** 출력에 포함됩니다.

show rip database

RIP 토폴로지 데이터베이스에 저장된 정보를 표시하려면 특권 EXEC 모드에서 **show rip database** 명령을 사용합니다.

show rip database [*ip_addr* [*mask*]]

구문 설명

ip_addr	(선택 사항) 지정된 네트워크 주소에 대한 표시 경로를 제한합니다.
mask	(선택 사항) 선택적 네트워크 주소에 대한 네트워크 마스크를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	•	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

RIP 라우팅 관련 **show** 명령은 ASA의 특권 EXEC 모드에서 사용할 수 있습니다. RIP 컨피그레이션 모드가 아니어도 RIP 관련 **show** 명령을 사용할 수 있습니다.

RIP 데이터베이스에는 RIP를 통해 학습된 모든 경로가 포함되어 있습니다. 이 데이터베이스에 표시된 경로는 라우팅 테이블에 나타나지 않을 수도 있습니다. 라우팅 프로토콜 데이터베이스에서 라우팅 테이블이 채워지는 방법에 대한 자세한 내용은 *Cisco Security Appliance 커맨드 라인 컨피그레이션 가이드*를 참고하십시오.

예

다음은 **show rip database** 명령의 샘플 출력입니다.

```
ciscoasa# show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

다음은 네트워크 주소 및 마스크가 포함된 **show rip database** 명령의 샘플 출력입니다.

```
Router# show rip database 172.19.86.0 255.255.255.0

172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

관련 명령

명령	설명
router rip	RIP 라우팅을 활성화하고 전역 RIP 라우팅 파라미터를 구성합니다.

show route

라우팅 테이블을 표시하려면 특권 EXEC 모드에서 **show route** 명령을 사용합니다.

show route [*interface_name* [*ip_address* [*netmask* [**static**]]]] [**failover**] [**cluster**] [**zone**]

구문 설명

cluster	(선택 사항) RIB(Routing Information Base) 에포크 번호(시퀀스 번호), 현재 타이머 값 및 네트워크 설명자 블록 에포크 번호(시퀀스 번호)를 표시합니다.
failover	(선택 사항) 라우팅 테이블의 현재 시퀀스 번호 및 대체작동이 발생한 후의 라우팅 항목을 표시하며, 대기 디바이스가 활성 디바이스가 됩니다.
interface_name	(선택 사항) 지정된 인터페이스를 사용하는 경로 항목으로 표시를 제한합니다.
ip_address	(선택 사항) 지정된 대상으로의 경로로 표시를 제한합니다.
netmask	(선택 사항) 지정된 대상에 적용할 네트워크 마스크를 정의합니다.
static	(선택 사항) 고정 경로로 표시를 제한합니다.
zone	(선택 사항) 영역 인터페이스에 대한 경로를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.4(1)	**failover** 키워드가 추가되었습니다. RIB 에포크 번호(시퀀스 번호), 현재 타이머 값 및 네트워크 설명자 블록 에포크 번호(시퀀스 번호)가 출력에 표시됩니다.
9.0(1)	**cluster** 키워드가 추가되었습니다. 동적 라우팅 프로토콜(EIGRP, OSPF 및 RIP)에 적용되며, ASA 5580 및 5585-X에서만 사용할 수 있습니다.
9.2(1)	이제 이 명령에서 연결된 경로와 함께 로컬 호스트 경로를 표시합니다. 표시할 프로토콜 또는 경로 유형을 나타내기 위해 새 코드(L, I, E, su 및 +)가 도입되었습니다.
9.3(2)	**zone** 키워드가 추가되었습니다.

사용 지침

show route 명령은 정보가 IPv4에 특정하다는 점을 제외하고는 **show ipv6 route** 명령과 유사한 출력을 제공합니다.

참고 **clustering** 및 **failover** 키워드는 이러한 기능이 ASA에 구성되지 않은 한 표시되지 않습니다.

show route 명령은 새 연결에 대한 "최상의" 경로를 나열합니다. 허용된 TCP SYN을 백업 인터페이스로 전송한 경우 ASA는 동일한 인터페이스를 통해서만 응답할 수 있습니다. 해당 인터페이스의 RIB에 기본 경로가 없는 경우 ASA는 인접성이 없기 때문에 패킷을 삭제합니다. **show running-config route** 명령에 표시된 대로 구성된 모든 항목은 특정 데이터 구조로 시스템에서 유지됩니다.

show asp table routing 명령을 사용하여 백엔드 인터페이스별 라우팅 테이블을 확인할 수 있습니다. 이 설계는 프로토콜별 경로 데이터베이스가 "최상의" 경로만 표시하는 전역 라우팅 테이블과 동일하지 않다는 점에서 OSPF 또는 EIGRP와 유사합니다. 이 동작은 설계에 따른 것입니다.

참고 Cisco IOS에서 **show ip route** 명령을 사용하는 경우 **longer-prefix** 키워드를 사용할 수 있습니다. Cisco IOS에서 이 키워드를 사용하면 지정된 네트워크 및 마스크 쌍이 일치하는 경우에만 경로가 표시됩니다.

ASA에서는 **longer-prefix** 키워드가 **show route** 명령의 기본 동작입니다. 즉, CLI에 추가 키워드가 필요 없습니다. 따라서 **ip**를 입력한 경우 경로를 볼 수 없습니다. 수퍼넷 경로를 얻으려면 IP 주소와 함께 마스크 값을 전달해야 합니다.

예

다음은 **show route** 명령의 샘플 출력입니다.

```
ciscoasa# show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

다음은 admin 상황에서 ASA 5555에 대해 실행된 **show route** 명령의 샘플 출력입니다. VPN 하드웨어 클라이언트가 개별 사용자 인증에 사용하는 내부 루프백 주소가 출력에 표시됩니다.

```
ciscoasa/admin(config)# show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route
```

```
Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

다음은 대체작동 후 OSPF 및 EIGRP 경로와 대기 디바이스의 동기화를 보여 주는 **show route failover** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show route failover

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                        [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

다음은 **show route cluster** 명령의 샘플 출력입니다.

```
ciscoasa(cfg-cluster)# show route cluster

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route


Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

show route zone 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

show route bgp

라우팅 테이블을 표시하려면 특권 EXEC 모드에서 **show route bgp** 명령을 사용합니다.

show route [bgp [*as_number*]**]**

구문 설명

bgp	(선택 사항) BGP 경로에 대한 RIB(Routing Information Base) 에포크 번호(시퀀스 번호), 현재 타이머 값 및 네트워크 설명자 블록 에포크 번호(시퀀스 번호)를 표시합니다.
as_number	(선택 사항) 지정된 AS 번호를 사용하는 경로 항목으로 표시를 제한합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

show route bgp 명령은 정보가 BGP에 특정하다는 점을 제외하고는 **show route** 명령과 유사한 출력을 제공합니다.

show route bgp 명령은 새 BGP 연결에 대한 "최상의" 경로를 나열합니다.

다음은 **show route bgp** 명령의 샘플 출력입니다.

```
ciscoasa# show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

show route eigrp

라우팅 테이블을 표시하려면 특권 EXEC 모드에서 **show route eigrp** 명령을 사용합니다.

show route [eigrp [*process-id*]**]**

구문 설명

eigrp	(선택 사항) EIGRP 경로에 대한 RIB(Routing Information Base) 에포크 번호(시퀀스 번호), 현재 타이머 값 및 네트워크 설명자 블록 에포크 번호(시퀀스 번호)를 표시합니다.
process-id	(선택 사항) 지정된 프로세스 ID를 사용하는 경로 항목으로 표시를 제한합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

show route eigrp 명령은 정보가 EIGRP에 특정하다는 점을 제외하고는 **show route** 명령과 유사한 출력을 제공합니다.

show route eigrp 명령은 새 BGP 연결에 대한 "최상의" 경로를 나열합니다.

다음은 **show route eigrp** 명령의 샘플 출력입니다.

```
ciscoasa# show route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

show route summary

라우팅 테이블의 현재 상태를 표시하려면 특권 EXEC 모드에서 **show route summary** 명령을 사용합니다.

show route summary

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

show route summary 명령은 라우팅 테이블의 현재 상태를 표시합니다.

다음은 **show route summary** 명령의 샘플 출력입니다.

```
ciscoasa# show route summary

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

12 장

show running-config through show switch vlan 명령

show running-config

현재 ASA에서 실행 중인 컨피그레이션을 표시하려면 특권 EXEC 모드에서 **show running-config** 명령을 사용합니다.

show running-config [**all**] [*command*]

구문 설명

all	기본 컨피그레이션을 비롯하여 작동 중인 전체 컨피그레이션을 표시합니다.
command	특정 명령과 관련된 컨피그레이션을 표시합니다. 사용 가능한 명령은 **show running-config ?**를 사용하여 CLI 도움말을 참고하십시오.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.3(1)	명령 출력에 암호화된 비밀번호가 표시됩니다.

사용 지침

show running-config 명령은 ASA 메모리의 활성 컨피그레이션(저장된 컨피그레이션 변경 사항 포함)을 표시합니다.

ASA의 플래시 메모리에 저장된 컨피그레이션을 표시하려면 **show configuration** 명령을 사용합니다.

show running-config 명령 출력에는 비밀번호 암호화가 활성화되거나 비활성화된 경우 암호화된 비밀번호, 마스킹된 비밀번호 또는 일반 텍스트 비밀번호가 표시됩니다.

참고 ASDM 명령은 해당 명령을 사용하여 ASA에 연결하거나 ASA를 구성한 후 컨피그레이션에 표시됩니다.

예

다음은 **show running-config** 명령의 샘플 출력입니다.

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.0(1)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.1.1.2 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.3 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname example1
domain-name example.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.1.1.2
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
```

```
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map abc_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy abc_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

다음은 **show running-config access-group** 명령의 샘플 출력입니다.

```
ciscoasa# show running-config access-group
access-group 100 in interface outside
```

다음은 **show running-config arp** 명령의 샘플 출력입니다.

```
ciscoasa# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

관련 명령

명령	설명
clear configure	실행 중인 컨피그레이션을 지웁니다.
show configuration	시작 컨피그레이션을 표시합니다.

show scansafe server

Cloud Web Security 프록시 서버의 상태를 표시하려면 특권 EXEC 모드에서 **show scansafe server** 명령을 사용합니다.

show scansafe server

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 서버가 현재 활성 서버인지, 백업 서버인지 또는 연결할 수 없는지와 같은 서버의 상태를 표시합니다.

예

다음은 **show scansafe server** 명령의 샘플 출력입니다.

```
ciscoasa# show scansafe server
ciscoasa# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
ciscoasa# Backup: proxy137.scansafe.net (80.254.152.99)
```

관련 명령

명령	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](파라미터)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스의 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	사용자 또는 그룹이 허용 목록과 일치하는지 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	ASA에서 Cloud Web Security 프록시 서버를 폴링하여 해당 가용성을 확인하기 전에 대기할 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 상황 모드에서 상황별로 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe statistics	총 HTTP 연결 수와 현재 HTTP 연결 수를 표시합니다.
user-identity monitor	AD 에이전트에서 지정된 사용자 또는 그룹 정보를 다운로드합니다.
whitelist	트래픽의 클래스에 대해 허용 목록 작업을 수행합니다.

show scansafe statistics

Cloud Web Security 활동에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show scansafe statistics** 명령을 사용합니다.

show scansafe statistics

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

show scansafe statistics 명령은 프록시 서버로 리디렉션된 연결 수, 현재 리디렉션 중인 연결 수 및 허용 목록에 포함된 연결 수와 같은 Cloud Web Security 활동에 대한 정보를 표시합니다.

예

다음은 **show scansafe statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

관련 명령

명령	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](파라미터)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스의 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	사용자 또는 그룹이 허용 목록과 일치하는지 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	ASA에서 Cloud Web Security 프록시 서버를 폴링하여 해당 가용성을 확인하기 전에 대기할 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 상황 모드에서 상황별로 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe server	현재 활성 서버인지, 백업 서버인지 또는 연결할 수 없는지와 같은 서버의 상태를 표시합니다.
user-identity monitor	AD 에이전트에서 지정된 사용자 또는 그룹 정보를 다운로드합니다.
whitelist	트래픽의 클래스에 대해 허용 목록 작업을 수행합니다.

show service-policy

서버 정책 통계를 표시하려면 특권 EXEC 모드에서 **show service-policy** 명령을 사용합니다.

show service-policy [**global** | **interface** *intf*] [**csc** | **cxsc** | **inspect** *inspection* [*arguments*] | **ips** | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]

show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

구문 설명

csc	(선택 사항) **csc** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
cxsc	(선택 사항) **cxsc** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
dest_ip dest_mask	**flow** 키워드를 사용할 경우 트래픽 흐름의 대상 IP 주소 및 넷마스크입니다.
details	(선택 사항) **set connection** 키워드를 사용할 경우 클라이언트별 연결 제한이 활성화된 경우 클라이언트별 연결 정보를 표시합니다.
eq *dest_port*	(선택 사항) **flow** 키워드를 사용할 경우 흐름의 대상 포트와 같습니다.
eq *src_port*	(선택 사항) **flow** 키워드를 사용할 경우 흐름의 소스 포트와 같습니다.
flow *protocol*	(선택 사항) 5튜블(프로토콜, 소스 IP 주소, 소스 포트, 대상 IP 주소, 대상 포트)로 식별되는 특정 흐름과 일치하는 정책을 표시합니다. 이 명령을 사용하여 서비스 정책 컨피그레이션이 특정 연결에 대한 원하는 서비스를 제공하는지 확인할 수 있습니다. 흐름은 5튜플로 설명되기 때문에 일부 정책은 지원되지 않습니다. 다음 지원되는 정책 일치를 참고하십시오. • **match access-list** • **match port** • **match rtp** • **match default-inspection-traffic**
global	(선택 사항) 전역 정책으로 출력을 제한합니다.
host *dest_host*	**flow** 키워드를 사용할 경우 트래픽 흐름의 호스트 대상 IP 주소입니다.
host *src_host*	**flow** 키워드를 사용할 경우 트래픽 흐름의 호스트 소스 IP 주소입니다.
icmp_control_message	(선택 사항) **flow** 키워드를 사용할 때 ICMP를 프로토콜로 지정할 경우 트래픽 흐름의 ICMP 제어 메시지를 지정합니다.
icmp_number	(선택 사항) **flow** 키워드를 사용할 때 ICMP를 프로토콜로 지정할 경우 트래픽 흐름의 ICMP 프로토콜 수를 지정합니다.
inspect *inspection* [*arguments*]	(선택 사항) **inspect** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다. 일부 **inspect** 명령은 세부 출력이 지원되지 않습니다. 모든 검사를 확인하려면 인수 없이 **show service-policy** 명령을 사용합니다. 검사마다 사용할 수 있는 인수가 다릅니다. 자세한 내용은 CLI 도움말을 참고하십시오.
interface *intf*	(선택 사항) *intf* 인수로 지정된 인터페이스에 적용되는 정책을 표시합니다. 여기서 *intf*는 **nameif** 명령에 지정된 인터페이스 이름입니다.
ips	(선택 사항) **ips** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
police	(선택 사항) **police** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
priority	(선택 사항) **priority** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.

set connection	(선택 사항) **set connection** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
sfr	(선택 사항) **sfr** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
shape	(선택 사항) **shape** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
src_ip src_mask	**flow** 키워드를 사용할 경우 트래픽 흐름의 소스 IP 주소 및 넷마스크입니다.
user-statistics	(선택 사항) **user-statistics** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다. 이 명령은 선택한 사용자에 대한 보낸 패킷 수, 보낸 삭제 수, 받은 패킷 수, 받은 삭제 수 등 ID 방화벽에 대한 사용자 통계를 표시합니다.

기본값

인수를 지정하지 않으면 모든 전역 및 인터페이스 정책이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.1(1)	**csc** 키워드가 추가되었습니다.
7.2(4)/8.0(4)	**shape** 키워드가 추가되었습니다.
8.4(2)	ID 방화벽에 대한 **user-statistics** 키워드 지원이 추가되었습니다.
8.4(4.1)	ASA CX 모듈에 대한 **cxsc** 키워드 지원이 추가되었습니다.
9.2(1)	ASA FirePOWER 모듈에 대한 **sfr** 키워드 지원이 추가되었습니다.

사용 지침

show service-policy 명령 출력에 표시되는 원시 연결 수는 **class-map** 명령에 정의된 것과 일치하는 트래픽에 대해 인터페이스에 현재 연결된 원시 연결 수를 나타냅니다. “embryonic-conn-max” 필드는 MPF(Modular Policy Framework)를 사용하여 트래픽 클래스에 대해 구성된 최대 원시 제한을 표시합니다. 표시된 현재 원시 연결 수가 최대값과 같거나 최대값을 초과하는 경우 **class-map** 명령에 정의된 트래픽 유형과 일치하는 새 TCP 연결에 TCP 가로채기가 적용됩니다.

서비스 정책 변경 사항을 컨피그레이션에 적용하면 모든 *새* 연결에서 새로운 서비스 정책을 사용합니다. 기존 연결에서는 연결 설정 당시에 구성된 정책을 계속 사용합니다. **show** 명령 출력에는 이전 연결에 대한 데이터가 포함되지 않습니다. 예를 들어 인터페이스에서 QoS 서비스 정책을 제거한 다음 수정된 버전을 다시 추가한 경우 **show service-policy** 명령은 새 서비스 정책과 일치하는 새 연결과 연계된 QoS 카운터만 표시합니다. 이전 정책에 대한 기존 연결은 더 이상 명령 출력에 표시되지 않습니다. 모든 연결에서 새 정책을 사용하려면 새 정책을 사용하여 다시 연결할 수 있도록 현재 연결을 해제해야 합니다. 자세한 내용은 **clear conn** 또는 **clear local-host** 명령을 참고하십시오.

참고 **inspect icmp** 및 **inspect icmp error** 정책의 경우에는 패킷 수에 에코 요청 및 응답 패킷만 포함됩니다.

예

다음은 **show service-policy global** 명령의 샘플 출력입니다.

```
ciscoasa# show service-policy global

Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
```

다음은 **show service-policy priority** 명령의 샘플 출력입니다.

```
ciscoasa# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap
```

다음은 **show service-policy flow** 명령의 샘플 출력입니다.

```
ciscoasa# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

다음은 **show service-policy inspect http** 명령의 샘플 출력입니다. 이 예에서는 match-any 클래스 맵의 각 match 명령에 대한 통계를 표시합니다.

```
ciscoasa# show service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
```

```
        Match: request method connect, 0 packets
        log, packet 648
```

다음은 **show service-policy inspect waas** 명령의 샘플 출력입니다. 이 예에서는 waas 통계를 표시합니다.

```
ciscoasa# show service-policy inspect waas

Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
        SYN with WAAS option 4
        SYN-ACK with WAAS option 4
        Confirmed WAAS connections 4
        Invalid ACKs seen on WAAS connections 0
        Data exceeding window size on WAAS connections 0
```

다음은 **show gtp requests** 명령의 샘플 출력입니다.

```
ciscoasa# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

다음 예에서와 같이 세로 막대(|)를 사용하여 디스플레이를 필터링하 수 있습니다.

```
ciscoasa# show service-policy gtp statistics | grep gsn
```

이 예에서는 gsn이라는 단어가 포함된 GTP 통계를 출력에 표시합니다.

다음 명령에서는 GTP 검사 통계를 보여 줍니다.

```
ciscoasa# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

표 12-1에는 **show service-policy inspect gtp statistics** 명령 출력의 각 열에 대한 설명이 나와 있습니다.

표 12-1 GPRS GTP 통계

열 머리글	설명
version_not_support	지원되지 않는 GTP 버전 필드가 있는 패킷을 표시합니다.
msg_too_short	길이가 8바이트 미만인 패킷을 표시합니다.
unknown_msg	알 수 없는 유형의 메시지를 표시합니다.
unexpected_data_msg	예상치 못한 데이터 메시지를 표시합니다.
mandatory_ie_missing	필수 IE(정보 요소)가 없는 메시지를 표시합니다.

표 12-1 GPRS GTP 통계(계속)

열 머리글	설명
mandatory_ie_incorrect	필수 IE(정보 요소)의 형식이 잘못된 메시지를 표시합니다.
optional_ie_incorrect	선택적 IE(정보 요소)의 형식이 잘못된 메시지를 표시합니다.
ie_unknown	알 수 없는 IE(정보 요소)가 있는 메시지를 표시합니다.
ie_out_of_order	시퀀스가 잘못된 IE(정보 요소)가 있는 메시지를 표시합니다.
ie_unexpected	예상치 못한 IE(정보 요소)가 있는 메시지를 표시합니다.
total_forwarded	전달된 총 메시지 수를 표시합니다.
total_dropped	삭제된 총 메시지 수를 표시합니다.
signalling_msg_dropped	삭제된 신호 처리 메시지 수를 표시합니다.
data_msg_dropped	삭제된 데이터 메시지 수를 표시합니다.
signalling_msg_forwarded	전달된 신호 처리 메시지 수를 표시합니다.
data_msg_forwarded	전달된 데이터 메시지 수를 표시합니다.
total created_pdp	생성된 총 PDP(Packet Data Protocol) 상황 수를 표시합니다.
total deleted_pdp	삭제된 총 PDP(Packet Data Protocol) 상황 수를 표시합니다.
total created_pdpmcb	생성된 총 PDPMCB 세션 수를 표시합니다.
total deleted_pdpmcb	삭제된 총 PDPMCB 세션 수를 표시합니다.
pdp_non_existent	존재하지 않는 PDP 상황에 대해 수신된 메시지를 표시합니다.

다음 명령은 PDP 상황에 대한 정보를 표시합니다.

```
ciscoasa# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

표 12-2에는 **show service-policy inspect gtp pdp-context** 명령 출력의 각 열에 대한 설명이 나와 있습니다.

표 12-2 PDP 상황

열 머리글	설명
Version	GTP 버전을 표시합니다.
TID	터널 식별자를 표시합니다.
MS Addr	모바일 스테이션 주소를 표시합니다.
SGSN Addr	서빙 게이트웨이 서비스 노드를 표시합니다.
Idle	PDP 상황이 사용되지 않은 시간을 표시합니다.
APN	액세스 포인트 이름을 표시합니다.

관련 명령

명령	설명
clear configure service-policy	서비스 정책 컨피그레이션을 지웁니다.
clear service-policy	모든 서비스 정책 컨피그레이션을 지웁니다.
service-policy	서비스 정책을 구성합니다.
show running-config service-policy	실행 중인 컨피그레이션에 구성된 서비스 정책을 표시합니다.

show shared license

공유 라이센스 통계를 표시하려면 특권 EXEC 모드에서 **show shared license** 명령을 사용합니다. 선택적 키워드는 라이센싱 서버에만 사용할 수 있습니다.

show shared license [**detail** | **client** [*hostname*] | **backup**]

구문 설명

backup	(선택 사항) 백업 서버에 대한 정보를 표시합니다.
client	(선택 사항) 참가자로 표시를 제한합니다.
detail	(선택 사항) 참가자별 통계를 포함하여 모든 통계를 표시합니다.
hostname	(선택 사항) 특정 참가자로 표시를 제한합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

통계를 지우려면 **clear shared license** 명령을 입력합니다.

예

다음은 라이센스 참가자에 대한 **show shared license** 명령의 샘플 출력입니다.

```
ciscoasa# show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
```

```
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client ID           Usage   Hostname
  ASA0926K04D         0       5510-B
```

표 12-3에는 **show shared license** 명령의 출력에 대한 설명이 나와 있습니다.

표 12-3 show shared license 설명

필드	설명
Primary License Server	기본 서버의 IP 주소입니다.
Version	공유 라이센스 버전입니다.
Status	백업 서버에서 명령이 실행된 경우 “Active”는 이 디바이스가 기본 공유 라이센싱 서버 역할을 맡았음을 의미합니다. “Inactive”는 디바이스가 대기 모드에 있으며, 기본 서버와 통신하고 있음을 나타냅니다. 기본 라이센싱 서버에 대체작동이 구성된 경우 대체작동 중 잠시 동안 백업 서버가 “Active” 상태가 될 수 있지만 통신이 다시 동기화되면 “Inactive” 상태로 돌아갑니다.
Shared license utilization	
SSLVPN	
Total for network	사용 가능한 총 공유 세션 수를 표시합니다.
Available	사용 가능한 남은 공유 세션 수를 표시합니다.
Utilized	활성 라이센스 서버용으로 가져온 공유 세션 수를 표시합니다.
This device	
Platform limit	설치된 라이센스에 따른 이 디바이스의 총 SSL VPN 세션 수를 표시합니다.
Current usage	공유 풀에서 이 디바이스가 현재 소유한 공유 SSL VPN 세션 수를 표시합니다.
High usage	이 디바이스가 지금까지 소유한 최대 공유 SSL VPN 세션 수를 표시합니다.
Messages Tx/Rx/Error	
Registration Get 릴리스 Transfer	각 연결 유형에 대한 전송, 수신 및 오류 패킷 수를 표시합니다.
Client ID	고유한 클라이언트 ID입니다.
Usage	사용 중인 세션 수를 표시합니다.
Hostname	이 디바이스의 호스트 이름을 표시합니다.

다음은 라이센스 서버에 대한 **show shared license detail** 명령의 샘플 출력입니다.

```
ciscoasa# show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0

Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

관련 명령

명령	설명
activation-key	라이센스 액티베이션 키를 입력합니다.
clear configure license-server	공유 라이센싱 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자에 대한 공유 라이센싱 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup address	참가자에 대한 공유 라이센싱 백업 서버를 식별합니다.
license-server backup backup-id	기본 공유 라이센싱 서버에 대한 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server backup enable	디바이스를 공유 라이센싱 백업 서버로 사용합니다.
license-server enable	디바이스를 공유 라이센싱 서버로 사용합니다.

명령	설명
license-server port	서버가 참가자의 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server refresh-interval	서버와 통신해야 하는 빈도를 설정하기 위해 참가자에게 제공되는 새로 고침 간격을 설정합니다.
license-server secret	공유 라이센싱 서버의 공유 암호를 설정합니다.
show activation-key	현재 설치된 라이센스 수를 표시합니다.
show running-config license-server	공유 라이센싱 서버 컨피그레이션을 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보를 표시합니다.

show shun

shun 정보를 표시하려면 특권 EXEC 모드에서 **show shun** 명령을 사용합니다.

show shun [*src_ip* | *statistics*]

구문 설명

src_ip	(선택 사항) 해당 주소에 대한 정보를 표시합니다.
statistics	(선택 사항) 인터페이스 카운터만 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.2(2)	위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

예

다음은 **show shun** 명령의 샘플 출력입니다.

```
ciscoasa# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

관련 명령

명령	설명
clear shun	현재 활성화된 모든 shun을 비활성화하고 shun 통계를 지웁니다.
shun	새 연결을 방지하고 모든 기존 연결의 패킷을 거부하여 공격 호스트에 대한 동적 응답을 활성화합니다.

show sip

SIP 세션을 표시하려면 특권 EXEC 모드에서 **show sip** 명령을 사용합니다.

show sip

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show sip 명령은 SIP 검사 엔진 문제 해결을 도와주며, **inspect protocol sip udp 5060** 명령을 통해 설명됩니다. **show timeout sip** 명령은 지정된 프로토콜의 시간 제한 값을 표시합니다.

show sip 명령은 ASA에 설정된 SIP 세션의 정보를 표시합니다. 이 명령은 **debug sip** 및 **show local-host** 명령과 함께 SIP 검사 엔진 문제를 해결하는 데 사용됩니다.

참고 **show sip** 명령을 사용하기 전에 **pager** 명령을 구성하는 것이 좋습니다. 많은 세션 레코드가 있는 경우 **pager** 명령을 구성하지 않으면 **show sip** 출력이 끝에 도달하는 데 약간의 시간이 걸립니다.

예

다음은 **show sip** 명령의 샘플 출력입니다.

```
ciscoasa# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
|state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
|state Active, idle 0:00:06
```

이 샘플에서는 ASA의 활성 SIP 세션 두 개를 보여 줍니다(`Total` 필드에 표시). 각 `call-id`는 통화를 나타냅니다.

`call-id`가 `c3943000-960ca-2e43-228f@10.130.56.44`인 첫 번째 세션은 상태가 `Call Init`입니다. 이는 세션이 여전히 통화 설정 상태임을 의미합니다. 통화 설정은 ACK가 표시된 경우에만 완료됩니다. 이 세션은 1 초 동안 유휴 상태였습니다.

두 번째 세션은 통화 설정이 완료되고 엔드포인트에서 미디어를 교환 중인 Active 상태에 있습니다. 이 세션은 6초 동안 유휴 상태였습니다.

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
debug sip	SIP에 대한 디버그 정보를 활성화합니다.
inspect sip	SIP 애플리케이션 검사를 활성화합니다.
show conn	여러 연결 유형에 대한 연결 상태를 표시합니다.
timeout	여러 프로토콜 및 세션 유형에 대한 최대 유휴 시간을 설정합니다.

show skinny

SCCP(Skinny) 검사 엔진 문제를 해결하려면 특권 EXEC 모드에서 **show skinny** 명령을 사용합니다.

show skinny

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show skinny 명령은 SCCP(Skinny) 검사 엔진 문제 해결을 도와줍니다.

예

다음은 아래 조건에 따른 **show skinny** 명령의 샘플 출력입니다. 두 개의 활성 Skinny 세션이 ASA에 설정되어 있습니다. 첫 번째 세션은 내부 Cisco IP Phone(로컬 주소 10.0.0.11)과 외부 Cisco CallManager(172.18.1.33) 간에 설정되었습니다. TCP 포트 2000이 CallManager입니다. 두 번째 세션은 다른 내부 Cisco IP Phone(로컬 주소 10.0.0.22)과 동일한 Cisco CallManager 간에 설정되었습니다.

```
ciscoasa# show skinny

        LOCAL                   FOREIGN                 STATE

-----------------------------------------------------------------

1       10.0.0.11/52238         172.18.1.33/2000                1

  MEDIA 10.0.0.11/22948         172.18.1.22/20798

2       10.0.0.22/52232         172.18.1.33/2000                1

  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

이 출력은 두 개의 내부 Cisco IP Phone 모두 간에 통화가 설정되었음을 나타냅니다. 첫 번째 전화와 두 번째 전화의 RTP 수신 대기 포트는 각각 UDP 22948 및 20798입니다.

다음은 이러한 Skinny 연결에 대한 xlate 정보입니다.

```
ciscoasa# show xlate debug
2 in use, 2 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
debug skinny	SCCP 디버그 정보를 활성화합니다.
inspect skinny	SCCP 애플리케이션 검사를 활성화합니다.
show conn	여러 연결 유형에 대한 연결 상태를 표시합니다.
timeout	여러 프로토콜 및 세션 유형에 대한 최대 유휴 시간을 설정합니다.

show sla monitor configuration

기본값을 포함하여 SLA 작업에 대한 컨피그레이션 값을 표시하려면 사용자 EXEC 모드에서 **show sla monitor configuration** 명령을 사용합니다.

show sla monitor configuration [*sla-id*]

구문 설명

sla-id	(선택 사항) SLA 작업의 ID 번호입니다. 유효한 값은 1~2147483647입니다.

기본값

*sla-id*를 지정하지 않으면 모든 SLA 작업에 대한 컨피그레이션 값이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

show running config sla monitor 명령을 사용하여 실행 중인 컨피그레이션의 SLA 작업 명령을 확인할 수 있습니다.

예

다음은 **show sla monitor** 명령의 샘플 출력입니다. SLA 작업 123에 대한 컨피그레이션 값을 표시합니다. **show sla monitor** 명령의 출력 뒤에는 동일한 SLA 작업에 대한 **show running-config sla monitor** 명령의 출력이 나와 있습니다.

```
ciscoasa> show sla monitor 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
```

```
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ciscoasa# show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

관련 명령

명령	설명
show running-config sla monitor	실행 중인 컨피그레이션의 SLA 작업 컨피그레이션 명령을 표시합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.

show sla monitor operational-state

SLA 작업의 작동 상태를 표시하려면 사용자 EXEC 모드에서 **show sla monitor operational-state** 명령을 사용합니다.

show sla monitor operational-state [*sla-id*]

구문 설명

sla-id	(선택 사항) SLA 작업의 ID 번호입니다. 유효한 값은 1~2147483647입니다.

기본값

*sla-id*를 지정하지 않으면 모든 SLA 작업에 대한 통계가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

show running-config sla monitor 명령을 사용하여 실행 중인 컨피그레이션의 SLA 작업 명령을 표시할 수 있습니다.

예

다음은 **show sla monitor operational-state** 명령의 샘플 출력입니다.

```
ciscoasa> show sla monitor operationl-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

관련 명령

명령	설명
show running-config sla monitor	실행 중인 컨피그레이션의 SLA 작업 컨피그레이션 명령을 표시합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.

show snmp-server engineid

ASA에 구성된 SNMP 엔진의 식별 정보를 표시하려면 특권 EXEC 모드에서 **show snmp-server engineid** 명령을 사용합니다.

show snmp-server engineid

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

예

다음은 **show snmp-server engineid** 명령의 샘플 출력입니다.

```
ciscoasa# show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

사용 지침

SNMP 엔진은 로컬 디바이스에 상주할 수 있는 SNMP의 사본입니다. 엔진 ID는 각 ASA 상황의 각 SNMP 에이전트에 할당되는 고유한 값입니다. 엔진 ID는 ASA에서 구성할 수 없습니다. 엔진 ID는 25바이트이며 암호화된 비밀번호를 생성하는 데 사용됩니다. 그런 다음 암호화된 비밀번호는 플래시 메모리에 저장됩니다. 엔진 ID를 캐시할 수 있습니다. 대체작동 쌍에서는 엔진 ID가 피어와 동기화됩니다.

관련 명령

명령	설명
clear configure snmp-server	SNMP 서버 컨피그레이션을 지웁니다.
show running-config snmp-server	SNMP 서버 컨피그레이션을 표시합니다.
snmp-server	SNMP 서버를 구성합니다.

show snmp-server group

구성된 SNMP 그룹의 이름, 사용 중인 보안 모델, 다양한 보기의 상태 및 각 그룹의 저장소 유형을 표시하려면 특권 EXEC 모드에서 **show snmp-server group** 명령을 사용합니다.

show snmp-server group

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

예

다음은 **show snmp-server group** 명령의 샘플 출력입니다.

```
ciscoasa# show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                     security model:v3 priv
readview : def_read_view                 writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

사용 지침

SNMP 사용자 및 그룹은 SNMP에 대한 VACM(보기 기반 액세스 제어 모델)에 따라 사용됩니다. SNMP 그룹에 따라 사용할 보안 모델이 결정됩니다. SNMP 사용자는 SNMP 그룹의 보안 모델과 일치해야 합니다. 각 SNMP 그룹 이름과 보안 수준 쌍은 고유해야 합니다.

관련 명령

명령	설명
clear configure snmp-server	SNMP 서버 컨피그레이션을 지웁니다.
show running-config snmp-server	SNMP 서버 컨피그레이션을 표시합니다.
snmp-server	SNMP 서버를 구성합니다.

show snmp-server statistics

SNMP 서버 통계를 표시하려면 특권 EXEC 모드에서 **show snmp-server statistics** 명령을 사용합니다.

show snmp-server statistics

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음은 **show snmp-server statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

관련 명령

명령	설명
clear configure snmp-server	SNMP 서버 컨피그레이션을 지웁니다.
clear snmp-server statistics	SNMP 패킷 입력 및 출력 카운터를 지웁니다.
show running-config snmp-server	SNMP 서버 컨피그레이션을 표시합니다.
snmp-server	SNMP 서버를 구성합니다.

show snmp-server user

SNMP 사용자의 구성된 특성에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show snmp-server user** 명령을 사용합니다.

show snmp-server user [*username*]

구문 설명

username	(선택 사항) SNMP 정보를 표시할 특정 사용자를 식별합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

예

다음은 **show snmp-server user** 명령의 샘플 출력입니다.

```
ciscoasa# show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

이 출력은 다음 정보를 제공합니다.

- SNMP 사용자의 이름을 식별하는 문자열인 사용자 이름
- ASA에서 SNMP 사본을 식별하는 문자열인 엔진 ID
- 설정이 ASA의 휘발성 또는 임시 메모리에 설정되었는지, 아니면 비휘발성 또는 영구 메모리에 설정(ASA가 꺼졌다가 다시 켜진 후에도 설정이 그대로 유지됨)되었는지 여부를 나타내는 저장소 유형
- SNMP 사용자와 연계된 표준 IP 액세스 목록인 활성 액세스 목록
- 활성인지 또는 비활성인지 나타내는 행 상태
- 사용 중인 인증 프로토콜을 식별하는 인증 프로토콜(옵션은 MD5, SHA 또는 none). 소프트웨어 이미지에서 인증이 지원되지 않는 경우에는 이 필드가 표시되지 않습니다.

- DES 패킷 암호화가 활성화되었는지 여부를 나타내는 개인 정보 프로토콜. 소프트웨어 이미지에서 개인 정보가 지원되지 않는 경우에는 이 필드가 표시되지 않습니다.
- 사용자가 속한 SNMP 그룹을 나타내는 그룹 이름. SNMP 그룹은 VACM(보기 기반 액세스 제어 모델)에 따라 정의됨

사용 지침

SNMP 사용자는 SNMP 그룹에 속해야 합니다. *username* 인수를 입력하지 않으면 **show snmp-server user** 명령에서 구성된 모든 사용자에 대한 정보가 표시됩니다. *username* 인수를 입력한 경우 사용자가 존재하면 해당 사용자에 대한 정보가 표시됩니다.

관련 명령

명령	설명
clear configure snmp-server	SNMP 서버 컨피그레이션을 지웁니다.
show running-config snmp-server	SNMP 서버 컨피그레이션을 표시합니다.
snmp-server	SNMP 서버를 구성합니다.

show software authenticity file

특정 이미지 파일에 대한 소프트웨어 인증과 관련된 디지털 서명 정보를 표시하려면 특권 EXEC 모드에서 **show software authenticity file** 명령을 사용합니다.

show software authenticity [*filename*]

구문 설명

filename	(선택 사항) 특정 이미지 파일을 식별합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

예

다음은 **show software authenticity file** 명령의 샘플 출력입니다.

```
ciscoasa# show software authenticity file asa913.SSA
File Name                     : disk0:/asa913.SSA
Image type                    : Development
    Signer Information
        Common Name           : Cisco
        Organization Unit     : ASA5585-X
        Organization Name     : Engineering
    Certificate Serial Number : abcd1234efgh5678
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

이 출력은 다음 정보를 제공합니다.

- 메모리에 있는 파일의 이름인 파일 이름
- 표시되는 이미지의 유형인 이미지 유형
- 다음과 같은 서명 정보를 지정하는 서명자 정보
  - 소프트웨어 제조업체의 이름인 공통 이름
  - 소프트웨어 이미지가 배포된 하드웨어를 나타내는 조직 구성 단위
  - 소프트웨어 이미지의 소유자인 조직 이름
- 디지털 서명에 대한 인증서 일련 번호인 인증서 일련 번호

- 디지털 서명 확인에 사용되는 해시 알고리즘의 유형을 나타내는 해시 알고리즘
- 디지털 서명 확인에 사용되는 서명 알고리즘의 유형을 식별하는 서명 알고리즘
- 확인에 사용되는 키 버전을 나타내는 키 버전

관련 명령

명령	설명
show version	소프트웨어 버전, 하드웨어 컨피그레이션, 라이센스 키 및 관련 가동 시간 데이터를 표시합니다.

show ssh sessions

ASA의 활성 SSH 세션에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show ssh sessions** 명령을 사용합니다.

show ssh sessions [**hostname** or **A.B.C.D**] [**hostname** or **X:X:X:X::X**] [**detail**]

구문 설명

hostname or **A.B.C.D**	(선택 사항) 지정된 SSH 클라이언트 IPv4 주소에 대한 SSH 세션 정보만 표시합니다.
hostname or **X:X:X:X::X**	(선택 사항) 지정된 SSH 클라이언트 IPv6 주소에 대한 SSH 세션 정보만 표시합니다.
detail	자세한 SSH 세션 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.1(2)	**detail** 옵션이 추가되었습니다.

사용 지침

SID는 SSH 세션을 식별하는 고유 번호입니다. Client IP는 SSH 클라이언트를 실행하는 시스템의 IP 주소입니다. Version은 SSH 클라이언트에서 지원하는 프로토콜 버전 번호입니다. SSH에서 SSH 버전 1만 지원하는 경우에는 Version 열에 1.5가 표시됩니다. SSH 클라이언트가 SSH 버전 1과 SSH 버전 2를 둘 다 지원하는 경우에는 Version 열에 1.99가 표시됩니다. SSH 클라이언트가 SSH 버전 2만 지원하는 경우에는 Version 열에 2.0가 표시됩니다. Encryption 열은 SSH 클라이언트에서 사용 중인 암호화 유형을 표시합니다. State 열은 클라이언트가 ASA와 상호 작용할 때의 진행 상황을 표시합니다. Username 열은 세션에 대해 인증된 로그인 사용자 이름을 나열합니다. Mode 열은 SSH 데이터 스트림의 방향을 설명합니다.

같거나 다른 암호화 알고리즘을 사용할 수 있는 SSH 버전 2의 경우 Mode 필드에는 in 및 out이 표시됩니다. 양방향에서 동일한 암호화를 사용하는 SSH 버전 1의 경우 Mode 필드에는 nil('-')이 표시되고 연결당 하나의 항목만 허용됩니다.

예

다음은 **show ssh sessions** 명령의 샘플 출력입니다.

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

다음은 **show ssh sessions detail** 명령의 샘플 출력입니다.

```
ciscoasa# show ssh sessions detail
SSH Session ID              : 0
>   Client IP               : 161.44.66.200
>   Username                : root
>   SSH Version             : 2.0
>   State                   : SessionStarted
>   Inbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Received         : 2224
>   Outbound Statistics
>    Encryption             : aes256-cbc
>    HMAC                   : sha1
>    Bytes Transmitted      : 2856
>   Rekey Information
>    Time Remaining (sec)   : 3297
>    Data Remaining (bytes): 996145356
>    Last Rekey             : 16:17:19.732 EST Wed Jan 2 2013
>    Data-Based Rekeys      : 0
>    Time-Based Rekeys      : 0
```

관련 명령

명령	설명
ssh disconnect	활성 SSH 세션의 연결을 해제합니다.
ssh timeout	유휴 SSH 세션에 대한 시간 제한 값을 설정합니다.

show ssl

ASA의 활성 SSL 세션에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show ssl** 명령을 사용합니다.

show ssl [**cache** | **ciphers** | **errors** | **mib** | **objects**]

구문 설명

cache	(선택 사항) SSL 세션 캐시 통계를 표시합니다.
ciphers	(선택 사항) 사용할 수 있는 SSL 암호를 표시합니다.
errors	(선택 사항) SSL 오류를 표시합니다.
mib	(선택 사항) SSL MIB 통계를 표시합니다.
objects	(선택 사항) SSL 개체 통계를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.
9.1(2)	**detail** 옵션이 추가되었습니다.
9.3(2)	TLSv1.1 및 TLSv1.2에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 활성화된 암호 순서, 비활성화된 암호, 사용 중인 SSL 신뢰 지점, 인증서 인증 사용 여부 등 현재 SSLv2 및 SSLv3 세션에 대한 정보를 표시합니다.

예

다음은 **show ssl** 명령의 샘플 출력입니다.

```
ciscoasa# show ssl

Accept connections using SSLv2 or greater and negotiate to TLSv1.2 or greater
Start connections using SSLv3 and negotiate to SSLv3 or greater
SSL DH Group: group2

SSL trust-points:
  Self-signed RSA certificate available
  Default: certsha256
  Interface inside: certsha256
Certificate authentication is not enabled
```

관련 명령

명령	설명
license-server port	서버가 참가자의 SSL 연결을 수신 대기하는 포트를 설정합니다.

show ssl ciphers

지정된 수준에서 사용할 수 있는 암호에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show ssl ciphers** 명령을 사용합니다.

show ssl ciphers *level*

구문 설명

level	암호의 강도를 지정하고 지원되는 최소 암호 수준을 나타냅니다. 증가하는 강도 순서의 유효한 값은 다음과 같습니다. • **all** - NULL-SHA를 비롯한 모든 암호를 포함합니다. • **low** - NULL-SHA를 제외한 모든 암호를 포함합니다. • **medium** - NULL-SHA, DES-CBC-SHA 및 RC4-MD5를 제외한 모든 암호를 포함합니다. • **fips** - 모든 FIPS 호환 암호(NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA 및 DES-CBC3-SHA 제외)를 포함합니다. • **high**(TLSv1.2에만 적용됨) - SHA-2 암호를 사용하는 AES-256만 포함합니다.

기본값

기본값은 모든 프로토콜 버전에 대해 **medium**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

show ssl ciphers 명령을 사용하여 **ssl cipher** 명령으로 구성된 수준에 따라 사용하도록 구성된 암호를 표시할 수 있습니다. **show ssl ciphers** *level* 명령을 사용하여 지정된 수준에서 사용할 수 있는 암호에 대한 정보를 표시할 수 있습니다.

예

다음은 **show ssl ciphers** 명령의 샘플 출력입니다.

```
ciscoasa# show ssl ciphers

Current cipher configuration:
default (medium):
  DHE-RSA-AES256-SHA256
```

```
  AES256-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
sslv3 (medium):
  AES256-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
```

다음은 **show ssl ciphers fips** 명령의 샘플 출력입니다.

```
ciscoasa# show ssl ciphers fips

DHE-RSA-AES256-SHA256(tlsv1.2)
  AES256-SHA256(tlsv1.2)
  DHE-RSA-AES128-SHA256(tlsv1.2)
  AES128-SHA256(tlsv1.2)
  DHE-RSA-AES256-SHA(tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA(sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA(tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA(sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
```

관련 명령

명령	설명
show ssl	인증서를 비롯한 SSL 컨피그레이션 정보를 표시합니다.
ssl ciphers	SSL, DTLS 및 TLS 프로토콜에 대한 암호화 알고리즘을 지정합니다.

show startup-config

시작 컨피그레이션 또는 시작 컨피그레이션 로드 시 오류를 표시하려면 특권 EXEC 모드에서 **show startup-config** 명령을 사용합니다.

show startup-config [**errors**]

구문 설명

errors	(선택 사항) ASA에서 시작 컨피그레이션을 로드할 때 생성된 모든 오류를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템[1]
특권 EXEC	• 예	• 예	• 예	• 예	• 예

1. **errors** 키워드는 단일 모드 및 시스템 실행 공간에서만 사용할 수 있습니다.

명령 기록

릴리스	수정 사항
7.0(1)	**errors** 키워드가 추가되었습니다.
8.3(1)	명령 출력에 암호화된 비밀번호가 표시됩니다.

사용 지침

다중 상황 모드에서 **show startup-config** 명령은 현재 실행 공간에 대한 시작 컨피그레이션을 표시합니다(시스템 컨피그레이션 또는 보안 상황).

show startup-config 명령 출력에는 비밀번호 암호화가 활성화되거나 비활성화된 경우 암호화된 비밀번호, 마스킹된 비밀번호 또는 일반 텍스트 비밀번호가 표시됩니다.

메모리에서 시작 오류를 지우려면 **clear startup-config errors** 명령을 사용합니다.

예

다음은 **show startup-config** 명령의 샘플 출력입니다.

```
ciscoasa# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.X(X)
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 209.165.200.224
 webvpn enable
```

```
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 209.165.200.225
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 209.165.200.226
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

다음은 **show startup-config errors** 명령의 샘플 출력입니다.

```
ciscoasa# show startup-config errors

ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', "nameif inside"
.....
*** Output from config line 37, "config-url disk:/admin..."
```

관련 명령

명령	설명
clear startup-config errors	메모리에서 시작 오류를 지웁니다.
show running-config	실행 중인 컨피그레이션을 표시합니다.

show sunrpc-server active

Sun RPC 서비스에 대해 열려 있는 핀홀을 표시하려면 특권 EXEC 모드에서 **show sunrpc-server active** 명령을 사용합니다.

show sunrpc-server active

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show sunrpc-server active 명령을 사용하여 Sun RPC 서비스에 대해 열려 있는 핀홀(예: NFS 및 NIS)을 표시할 수 있습니다.

예

Sun RPC 서비스에 대해 열려 있는 핀홀을 표시하려면 **show sunrpc-server active** 명령을 입력합니다. 다음은 **show sunrpc-server active** 명령의 샘플 출력입니다.

```
ciscoasa# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

관련 명령

명령	설명
clear configure sunrpc-server	ASA에서 Sun 원격 프로세서 호출 서비스를 지웁니다.
clear sunrpc-server active	Sun RPC 서비스에 대해 열려 있는 핀홀(예: NFS 및 NIS)을 지웁니다.
inspect sunrpc	Sun RPC 애플리케이션 검사를 활성화하거나 비활성화하고 사용되는 포트를 구성합니다.
show running-config sunrpc-server	SunRPC 서비스 컨피그레이션에 대한 정보를 표시합니다.

show switch mac-address-table

내장형 스위치가 있는 모델(예: ASA 5505 Adaptive Security Appliance)의 경우 스위치 MAC 주소 테이블을 보려면 특권 EXEC 모드에서 **show switch mac-address-table** 명령을 사용합니다.

show switch mac-address-table

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 내장형 스위치가 있는 모델에만 적용됩니다. 스위치 MAC 주소 테이블에는 스위치 하드웨어의 각 VLAN 내 트래픽에 대한 MAC 주소-스위치 포트 매핑이 유지됩니다. 투명 방화벽 모드에서 ASA 소프트웨어의 브리지 MAC 주소 테이블을 보려면 **show mac-address-table** 명령을 사용합니다. 브리지 MAC 주소 테이블에는 VLAN 사이를 통과하는 트래픽에 대한 MAC 주소-VLAN 인터페이스 매핑이 유지됩니다.

MAC 주소 항목은 5분 후에 폐기됩니다.

예

다음은 **show switch mac-address-table** 명령의 샘플 출력입니다.

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |       Type        | Age | Port
-----------------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic       | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic       | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic       | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic       | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static        |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast  |  -  | In0/1,Et0/0-7
Total Entries: 6
```

표 12-4에는 각 필드에 대한 설명이 나와 있습니다.

표 12-4 show switch mac-address-table 필드

필드	설명
Mac Address	MAC 주소를 표시합니다.
VLAN	MAC 주소와 연결된 VLAN을 표시합니다.
Type	MAC 주소가 동적으로 학습되었는지 또는 정적 멀티캐스트 주소처럼 정적으로 학습되었는지 표시합니다. 내부 백플레인 인터페이스에 대한 항목만 정적 항목입니다.
Age	MAC 주소 테이블에 있는 동적 항목의 기간을 표시합니다.
Port	MAC 주소가 있는 호스트에 연결할 수 있는 스위치 포트를 표시합니다.

관련 명령

명령	설명
show mac-address-table	내장형 스위치가 없는 모델에 대한 MAC 주소 테이블을 표시합니다.
show switch vlan	VLAN과 실제 MAC 주소 간의 연계를 표시합니다.

show switch vlan

내장형 스위치가 있는 모델(예: ASA 5505 Adaptive Security Appliance)의 경우 VLAN 및 연결된 스위치 포트를 보려면 특권 EXEC 모드에서 **show switch vlan** 명령을 사용합니다.

show switch vlan

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 내장형 스위치가 있는 모델에만 적용됩니다. 다른 모델의 경우 **show vlan** 명령을 사용합니다.

예

다음은 **show switch vlan** 명령의 샘플 출력입니다.

```
ciscoasa# show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et0/0, Et0/1
200  outside                         up        Et0/7
300  -                               down      Et0/1, Et0/2
400  backup                          down      Et0/3
```

표 12-5에는 각 필드에 대한 설명이 나와 있습니다.

표 12-5 show switch vlan 필드

필드	설명
VLAN	VLAN 번호를 표시합니다.
Name	VLAN 인터페이스의 이름을 표시합니다. **nameif** 명령을 사용하여 설정된 이름이 없거나 **interface vlan** 명령이 없는 경우 대시(-)가 표시됩니다.
Status	스위치의 VLAN과 트래픽을 주고받는 상태(up 또는 down)를 표시합니다. VLAN 상태가 up이 되려면 VLAN의 스위치 포트 중 하나 이상이 up 상태여야 합니다.
Ports	각 VLAN에 할당된 스위치 포트를 표시합니다. 스위치 포트가 여러 VLAN에 대해 나열된 경우 이는 트렁크 포트입니다. 위 샘플 출력에서는 Ethernet 0/1이 VLAN 100 및 300을 전송하는 트렁크 포트임을 보여 줍니다.

관련 명령

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
interface vlan	VLAN 인터페이스를 생성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show vlan	내장형 스위치가 없는 모델에 대한 VLAN을 표시합니다.
switchport mode	스위치 포트의 모드를 액세스 또는 트렁크 모드로 설정합니다.

13 장

show tcpstat through show traffic 명령

show tcpstat

ASA TCP 스택의 상태 및 ASA에서 종료되는 TCP 연결을 표시하려면(디버깅용) 특권 EXEC 모드에서 **show tcpstat** 명령을 사용합니다. 이 명령은 IPv4 및 IPv6 주소를 지원합니다.

show tcpstat

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show tcpstat 명령을 사용하여 TCP 스택의 상태 및 ASA에서 종료되는 TCP 연결을 표시할 수 있습니다. 표시되는 TCP 통계는 표 28에 설명되어 있습니다.

표 13-1 show tcpstat 명령의 TCP 통계

통계	설명
tcb_cnt	TCP 사용자 수입니다.
proxy_cnt	TCP 프록시 수입니다. TCP 프록시는 사용자 권한 부여에서 사용됩니다.
tcp_xmt pkts	TCP 스택에서 전송된 패킷 수입니다.
tcp_rcv good pkts	TCP 스택에서 수신된 정상 패킷 수입니다.
tcp_rcv drop pkts	TCP 스택에서 삭제된 수신 패킷 수입니다.
tcp bad chksum	체크섬이 잘못된 수신 패킷 수입니다.
tcp user hash add	해시 테이블에 추가된 TCP 사용자 수입니다.
tcp user hash add dup	새 사용자를 추가하려고 할 때 TCP 사용자가 해시 테이블에 이미 존재한 횟수입니다.
tcp user srch hash hit	검색할 때 해시 테이블에서 TCP 사용자가 발견된 횟수입니다.

표 13-1 show tcpstat 명령의 TCP 통계 (계속)

통계	설명
tcp user srch hash miss	검색할 때 해시 테이블에서 TCP 사용자가 발견되지 않은 횟수입니다.
tcp user hash delete	해시 테이블에서 TCP 사용자가 삭제된 횟수입니다.
tcp user hash delete miss	사용자를 삭제하려고 할 때 해시 테이블에서 TCP 사용자가 발견되지 않은 횟수입니다.
lip	TCP 사용자의 로컬 IP 주소입니다.
fip	TCP 사용자의 외부 IP 주소입니다.
lp	TCP 사용자의 로컬 포트입니다.
fp	TCP 사용자의 외부 포트입니다.
st	TCP 사용자의 상태입니다(RFC 793 참고). 가능한 값은 다음과 같습니다. 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	TCP 사용자의 재전송 대기열 기간입니다.
inqlen	TCP 사용자의 입력 대기열 기간입니다.
tw_timer	TCP 사용자의 time_wait 타이머 값(밀리초)입니다.
to_timer	TCP 사용자의 비활성 시간 제한 타이머 값(밀리초)입니다.
cl_timer	TCP 사용자의 닫기 요청 타이머 값(밀리초)입니다.
per_timer	TCP 사용자의 지속 타이머 값(밀리초)입니다.
rt_timer	TCP 사용자의 재전송 타이머 값(밀리초)입니다.
tries	TCP 사용자의 재전송 횟수입니다.

예

다음 예에서는 ASA의 TCP 스택 상태를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
```

```
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

관련 명령

명령	설명
show conn	사용된 연결 및 사용할 수 있는 연결을 표시합니다.

show tech-support

기술 지원 분석가가 진단에 사용하는 정보를 표시하려면 특권 EXEC 모드 **show tech-support** 명령을 사용합니다.

show tech-support [**detail** | **file** | **no-config** | **performance**]

구문 설명

detail	(선택 사항) 자세한 정보를 나열합니다.
file	(선택 사항) 명령 출력을 파일에 기록합니다.
no-config	(선택 사항) 실행 중인 컨피그레이션의 출력을 제외합니다.
performance	(선택 사항) 성능 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	**detail** 및 **file** 키워드가 추가되었습니다.
7.2(1)	CPU를 호그하는 프로세스에 대한 보다 자세한 정보를 표시하도록 출력이 향상되었습니다.
9.1(2)	**show environment** 명령의 정보를 포함하도록 출력이 향상되었습니다.
9.1(3)	**show memory detail**, **show memory top-usage** 및 **show vlan** 명령의 정보를 포함하도록 출력이 향상되었습니다.
9.2(1)	**show memory detail**, **show cpu detail**, **show blocks queue history core-local**, **show asp drop**, **show asp event dp-cp**, **show cpu usage history**, 및 **show traffic summary** 명령의 정보를 포함하도록 출력이 향상되었습니다. **show kernel cgroup-controller detail** 명령의 출력이 제거되고, **performance** 키워드가 추가되었습니다.
9.2(1)	**show vlan** 명령의 정보를 포함하도록 출력이 향상되었습니다.
9.3(2)	**show route-summary** 명령 출력이 **show tech-support detail** 명령에 추가되었습니다.

사용 지침

show tech-support 명령을 사용하여 기술 지원 분석가가 문제를 진단하는 데 필요한 정보를 나열할 수 있습니다. 이 명령은 **show** 명령과 함께 기술 지원 분석가에게 가장 많은 정보를 제공합니다.

예

다음 예에서는 기술 지원 분석가용으로 사용되는 정보를 표시하는 방법을 보여 줍니다. 이 출력은 **show module** 명령의 출력부터 시작하도록 단축되었습니다.

```
ciscoasa# show tech-support | beg show module

------------------ show module ------------------

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAD1626056J

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 a493.4c43.0d68 to a493.4c43.0d73  2.0          2.0(13)0     100.8(0)229

Mod SSP Application Name           Status           SSP Application Version
--- ------------------------------ ---------------- --------------------------

Mod Status              Data Plane Status     Compatibility
--- ------------------- --------------------- -------------
  0 Up Sys              Not Applicable

------------------ show environment ------------------

Cooling Fans:
-------------------------------------

   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7200 RPM - OK  (Fan Module Fan)

Power Supplies:
-------------------------------------
   Power Supply Unit Redundancy: N/A

   Temperature:
   --------------------------------
   Left Slot (PS0): 30 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 31 C - OK  (Fan Module Temperature)

   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7100 RPM - OK  (Fan Module Fan)

Temperature:
-------------------------------------

   Processors:
   --------------------------------
   Processor 1: 47.0 C - OK  (CPU1 Core Temperature)

   Chassis:
   --------------------------------
   Ambient 1: 31.5 C - OK  (Chassis Front Temperature)
   Ambient 2: 37.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 31.25 C - OK  (CPU1 Front Temperature)
   Ambient 4: 32.0 C - OK  (CPU1 Back Temperature)

   IO Hub:
   --------------------------------
   Circuit Die: 49.0 C - OK  (Circuit Die Temperature)
```

```
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 30 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 31 C - OK  (Fan Module Temperature)

Voltage:
-----------------------------------
   Channel 1:  3.325 V -   (3.3V (U142 VX1))
   Channel 2:  1.496 V -   (1.5V (U142 VX2))
   Channel 3:  1.048 V -   (1.05V (U142 VX3))
   Channel 4:  3.337 V -   (3.3V_STDBY (U142 VP1))
   Channel 5: 11.665 V -   (12V (U142 VP2))
   Channel 6:  4.950 V -   (5.0V (U142 VP3))
   Channel 7:  6.853 V -   (7.0V (U142 VP4))
   Channel 8:  9.616 V -   (IBV (U142 VH))
   Channel 9:  1.046 V -   (1.05VB (U209 VX2))
   Channel 10:  1.213 V -   (1.2V (U209 VX3))
   Channel 11:  1.110 V -   (1.1V (U209 VX4))
   Channel 12:  1.006 V -   (1.0V (U209 VX5))
   Channel 13:  3.335 V -   (3.3V STDBY (U209 VP1))
   Channel 14:  2.499 V -   (2.5V (U209 VP2))
   Channel 15:  1.803 V -   (1.8V (U209 VP3))
   Channel 16:  1.894 V -   (1.9V (U209 VP4))
   Channel 17:  9.611 V -   (IBV (U209 VH))
   Channel 18:  2.048 V -   (VTT CPU0 (U83 VX2))
   Channel 19:  0.000 V -   (VTT CPU1 (U83 VX3))
   Channel 20:  2.048 V -   (VCC CPU0 (U83 VX4))
   Channel 21:  1.772 V -   (VCC CPU1 (U83 VX5))
   Channel 22:  1.516 V -   (1.5VA (U83 VP1))
   Channel 23:  0.000 V -   (1.5VB (U83 VP2))
   Channel 24:  8.937 V -   (IBV (U83 VH))

------------------ show memory ------------------

Free memory:        4927975152 bytes (76%)
Used memory:        1514475792 bytes (24%)
-------------     ------------------
Total memory:       6442450944 bytes (100%)

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show vpn-sessiondb summary ------------------


No sessions to display.


------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     0   1450   1450   1450
     4    100     99     99
    80   1000   1000   1000

------------------ show asp drop ------------------
Frame drop:
  Flow is denied by configured rule (acl-drop)                           290272
```

```
  Slowpath security checks failed (sp-security-failed)                    22489
  Interface is down (interface-down)                                         49
Last clearing: Never
Flow drop:
Last clearing: Never

------------------ show asp event dp-cp ------------------
DP-CP EVENT QUEUE                  QUEUE-LEN  HIGH-WATER
Punt Event Queue                           0           1
Identity-Traffic Event Queue               0           1
General Event Queue                        0           2
Syslog Event Queue                         0           3
Non-Blocking Event Queue                   0          22
Midpath High Event Queue                   0           0
Midpath Norm Event Queue                   0           1
SRTP Event Queue                           0           0
HA Event Queue                             0           3
Threat-Detection Event Queue               0           0
ARP Event Queue                            0          10
IDFW Event Queue                           0           0
CXSC Event Queue                           0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt                18079          0    18079        0    18079           0
  inspect-gtp       18079          0    18079        0    18079           0
drop-flow             0            0    36158        0    36158           0
midpath-norm          9            0        9        0        9           0
adj-absent          18079          0    18079        0    18079           0
arp-in            7683820          0  7683820        0  7683820           0
identity-traffic       16          0       16        0       16           0
syslog             117503            0     117503         0     117503           0
scheduler             89          0       89        0       89           0
ha-msg           48812863          0 48812863        0 48812863           5

------------------ show blocks queue history core-local ------------------

History buffer memory usage: 3744 bytes (default)
History analysis time limit: 100 msec

------------------ show blocks core ------------------
CORE  LIMIT  ALLOC   HIGH    CNT       FAILED
   0  24576     24     25   1111            0
   1  24576   4425   6155    899            0
   2  24576   2045   2873    743            0
   3  24576   3129   4648    817            0
   4  24576     18     18   1994            0
   5  24576    338    936   1412            0
   6  24576     40     44   2011            0
   7  24576    124    129   1155            0

------------------ show cpu detail ------------------

Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 4       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 5       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 6       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 7       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)

Current control point elapsed versus the maximum control point elapsed for:
```

```
      5 seconds = 66.7%; 1 minute: 66.7%; 5 minutes: 66.7%
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%

Total CPU utilization for:
      5 seconds = 0.3%; 1 minute: 0.1%; 5 minutes: 0.1%

------------------ show memory detail ------------------
Free memory:                    10213725472 bytes (79%)
Used memory:
     Allocated memory in use:      789891808 bytes ( 6%)
     Reserved memory:             1881284608 bytes (15%)
----------------------------   ------------------
Total memory:                   12884901888 bytes (100%)

Least free memory:      10213420912 bytes (79%)
Most used memory:        2671480976 bytes (21%)

MEMPOOL_DMA_ALT1 POOL STATS:

Non-mmapped bytes allocated =    291766272
Number of free chunks       =            1
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    291766272
Keepcost                    =    263907584
Max contiguous free mem     =    263907584
Allocated memory in use     =     27858592
Free memory                 =    263907680

----- fragmented memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
          96             1             96**
    263907584            1      263907584*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
         8192            16         131072
     12582912             1       12582912

MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =    291766272
Number of free chunks       =          131
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    291766272
Keepcost                    =    252590992
Max contiguous free mem     =    252590992
Allocated memory in use     =     39118960
Free memory                 =    252647312

----- fragmented memory statistics -----
```

```
fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           96             1             96**
          256            64          20480
          384            32          15360
          512            33          20208
    252590992             1      252590992*

*  - top most releasable chunk.
** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           96             1             96
          144             2            288
          256             2            512
          384             3           1152
          512             3           1536
         1024           128         131072
         2048             1           2048
         8192             5          40960
        12288            25         307200
        16384             1          16384
        32768             2          65536
        65536             1          65536
        98304             2         196608
       131072             3         393216
       196608             5         983040
       262144             3         786432
       393216             1         393216
       524288             2        1048576
       786432             2        1572864
      1048576             1        1048576
      1572864             2        3145728
      2097152             2        4194304
      3145728             2        6291456
     12582912             1       12582912

MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =  11003617280
Number of free chunks       =          492
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =  11003617280
Keepcost                    =  10213402128
Max contiguous free mem     =  10213402128
Allocated memory in use     =    789891808
Free memory                 =  10213725472

----- fragmented memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           32           201           6432
           48           131           6288
           64           138           8832
           96             1             96**
          112             2            224
```

```
          256             5           1392
          512             1            592
         2048             1           2160
        24576            11         284784
  10213402128             1    10213402128*

*  - top most releasable chunk.
** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           80          1485         118800
           96          8525         818400
          112          3287         368144
          128          1867         238976
          144         10842        1561248
          160           876         140160
          176           476          83776
          192           448          86016
          208           795         165360
          224          1130         253120
          240           191          45840
          256          2733         699648
          384           415         159360
          512          1225         627200
          768           869         667392
         1024          1507        1543168
         1536          5345        8209920
         2048           329         673792
         3072           186         571392
         4096          5001       20484096
         6144            58         356352
         8192           349        2859008
        12288            94        1155072
        16384            85        1392640
        24576            17         417792
        32768           172        5636096
        49152            38        1867776
        65536           172       11272192
        98304            44        4325376
       131072            41        5373952
       196608            36        7077888
       262144            40       10485760
       393216            20        7864320
       524288            15        7864320
       786432            50       39321600
      1048576            32       33554432
      1572864             1        1572864
      2097152            12       25165824
      3145728             2        6291456
      4194304             1        4194304
      6291456             1        6291456
      8388608             1        8388608
     12582912             5       62914560

Summary for all pools:

Non-mmapped bytes allocated =  11587149824
Number of free chunks       =          624
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
```

```
Max memory footprint        =  11587149824
Keepcost                    =  10729900704
Allocated memory in use     =    856869360
Free memory                 =  10730280464


------------------ show memory top-usage ------------------

MEMPOOL_DMA pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
     12582912             1       12582912
      2097152             2        4194304
      3145728             1        3145728
      1048576             2        2097152
      1572864             1        1572864
       786432             1         786432
       196608             3         589824
       262144             2         524288
       393216             1         393216
        98304             3         294912

----- Binsize PC top usage -----

Binsize: 12582912               total (bytes): 12582912

pc = 0x805ada0, size = 12960071 , count = 1

Binsize: 2097152                total (bytes): 4194304

pc = 0x805ada0, size = 5758350  , count = 2

Binsize: 3145728                total (bytes): 3145728

pc = 0x987071c, size = 3178567  , count = 1

Binsize: 1048576                total (bytes): 2097152

pc = 0x805ada0, size = 2309774  , count = 2

Binsize: 1572864                total (bytes): 1572864

pc = 0x805ada0, size = 1740871  , count = 1

Binsize: 786432                 total (bytes): 786432

pc = 0x805ada0, size = 915271   , count = 1

Binsize: 196608                 total (bytes): 589824

pc = 0x805ada0, size = 484622   , count = 2
pc = 0x80567f1, size = 259271   , count = 1

Binsize: 262144                 total (bytes): 524288

pc = 0x805ada0, size = 352071   , count = 1
pc = 0x80567f1, size = 310471   , count = 1

Binsize: 393216                 total (bytes): 393216
```

```
pc = 0x805ada0, size = 505671   , count = 1

Binsize: 98304                  total (bytes): 294912

pc = 0x805ada0, size = 129671   , count = 1
pc = 0x80567f1, size = 227342   , count = 2


MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:

----- allocated memory statistics -----

 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
      8388608             2       16777216
        65536           126        8257536
       524288            14        7340032
      4194304             1        4194304
      3145728             1        3145728
       131072            21        2752512
      1048576             2        2097152
      2097152             1        2097152
        16384           127        2080768
       262144             7        1835008

----- Binsize PC top usage -----

Binsize: 8388608                total (bytes): 16777216

pc = 0x825b333, size = 16777216 , count = 2

Binsize: 65536                  total (bytes): 8257536

pc = 0x916e48d, size = 7531232  , count = 107
pc = 0x982de33, size = 263056   , count = 4
pc = 0x982db72, size = 324956   , count = 4
pc = 0x82d9092, size = 65536    , count = 1
pc = 0x819b8f9, size = 77824    , count = 1
pc = 0x819b65e, size = 77824    , count = 1
pc = 0x9334871, size = 65536    , count = 1
pc = 0x8a01e5a, size = 65536    , count = 1
pc = 0x8a109f0, size = 65536    , count = 1
pc = 0x9162fb0, size = 163968   , count = 2
pc = 0x8f13da8, size = 66048    , count = 1
pc = 0x8056c11, size = 66528    , count = 1
pc = 0x8056bf5, size = 66528    , count = 1

Binsize: 524288                 total (bytes): 7340032

pc = 0x8a9f8eb, size = 643264   , count = 1
pc = 0x982db72, size = 5325112  , count = 8
pc = 0x807bcb4, size = 524312   , count = 1
pc = 0x821944f, size = 1282600  , count = 2
pc = 0x9187575, size = 524312   , count = 1
pc = 0x8056a14, size = 524352   , count = 1

Binsize: 4194304                total (bytes): 4194304

pc = 0x8cc1f27, size = 5242924  , count = 1

Binsize: 3145728                total (bytes): 3145728

pc = 0x821944f, size = 3698788  , count = 1
```

```
Binsize: 131072                 total (bytes): 2752512

pc = 0x9137bc4, size = 163904   , count = 1
pc = 0x806e421, size = 393216   , count = 3
pc = 0x8f3f649, size = 154136   , count = 1
pc = 0x911894b, size = 131072   , count = 1
pc = 0x89f3fd0, size = 141212   , count = 1
pc = 0x982de33, size = 593580   , count = 4
pc = 0x8167e2b, size = 160864   , count = 1
pc = 0x982db72, size = 983250   , count = 6
pc = 0x9162fb0, size = 327808   , count = 2
pc = 0x806e024, size = 184800   , count = 1

Binsize: 1048576                total (bytes): 2097152

pc = 0x982de33, size = 1081507  , count = 1
pc = 0x821944f, size = 1120100  , count = 1

Binsize: 2097152                total (bytes): 2097152

pc = 0x8aa1252, size = 2097152  , count = 1

Binsize: 16384                  total (bytes): 2080768

pc = 0x806e421, size = 1474560  , count = 90
pc = 0x982de33, size = 135545   , count = 7
pc = 0x9173a77, size = 36928    , count = 2
pc = 0x88a6fec, size = 163840   , count = 10
pc = 0x8f3f649, size = 24160    , count = 1
pc = 0x982db72, size = 96195    , count = 5
pc = 0x8a765c0, size = 17408    , count = 1
pc = 0x92cb71b, size = 17388    , count = 1
pc = 0x982dbee, size = 119925   , count = 7
pc = 0x879defa, size = 19456    , count = 1
pc = 0x8ebd433, size = 16432    , count = 1
pc = 0x8ebd415, size = 16432    , count = 1

Binsize: 262144                 total (bytes): 1835008

pc = 0x982db72, size = 1573315  , count = 5
pc = 0x982de33, size = 580878   , count = 2

------------------ show route-summary----------

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          0           1           0           88          288
eigrp 11        0           3000        0           324000      864000
bgp 200         2           45          0           4136        13536
  External: 47 Internal: 0 Local: 0
ospf 100        0           538         0           47344       157096
  Intra-area: 38 Inter-area: 0 External-1: 500 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal        7                                               288976
Total           9           3586        0           375744      1324472

------------------ show vlan ------------------

64, 66, 70-72, 80-82, 142, 151, 950-951, 960-961
```

관련 명령

명령	설명
show clock	syslog 서버(PFSS) 및 PKI(Public Key Infrastructure) 프로토콜에서 사용할 클럭을 표시합니다.
show conn count	사용된 연결 및 사용할 수 있는 연결을 표시합니다.
show cpu	CPU 사용률 정보를 표시합니다.
show failover	연결 상태 및 활성화된 ASA를 표시합니다.
show memory	운영 체제에 사용 가능한 최대 실제 메모리 및 현재 사용 가능한 메모리에 대한 요약을 표시합니다.
show perfmon	ASA의 성능에 대한 정보를 표시합니다.
show processes	실행 중인 프로세스 목록을 표시합니다.
show running-config	ASA에서 현재 실행 중인 컨피그레이션을 표시합니다.
show xlate	변환 슬롯에 대한 정보를 표시합니다.

show threat-detection memory

threat-detection statistics 명령의 의해 활성화된 고급 위협 감지 통계에서 사용되는 메모리를 표시하려면 특권 EXEC 모드에서 **show threat-detection memory** 명령을 사용합니다.

show threat-detection memory

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.

사용 지침

일부 통계는 많은 메모리를 사용하고 ASA 성능에 영향을 줄 수 있습니다. 이 명령을 사용하면 메모리 사용량을 모니터링할 수 있으므로 필요한 경우 컨피그레이션을 조정할 수 있습니다.

예

다음은 **show threat-detection memory** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection memory
Cached chunks:
       CACHE TYPE             BYTES USED
TD Host                         70245888
TD Port                             2724
TD Protocol                         1476
TD ACE                               728
TD Shared counters                 14256
============================
Subtotal TD Chunks              70265072


Regular memory                BYTES USED
TD Port                             33824
TD Control block                   162064
============================
Subtotal Regular Memory            195888


Total TD memory:                70460960
```

관련 명령

명령	설명
show threat-detection statistics host	호스트 통계를 표시합니다.
show threat-detection statistics port	포트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
show threat-detection statistics top	상위 10개의 통계를 표시합니다.
threat-detection statistics	고급 위협 감지 통계를 활성화합니다.

show threat-detection rate

threat-detection basic-threat 명령을 사용하여 기본 위협 감지를 활성화한 경우 특권 EXEC 모드에서 **show threat-detection rate** 명령을 사용합니다.

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

구문 설명

acl-drop	(선택 사항) 액세스 목록 거부로 인해 삭제된 패킷의 비율을 표시합니다.
min-display-rate *min_display_rate*	(선택 사항) 최소 표시 비율(초당 이벤트 수)을 초과하는 통계로 표시를 제한합니다. 0~2147483647 범위에서 *min_display_rate*를 설정할 수 있습니다.
bad-packet-drop	(선택 사항) 잘못된 패킷 형식(예: invalid-ip-header 또는 invalid-tcp-hdr-length) 거부로 인해 삭제된 패킷의 비율을 표시합니다.
conn-limit-drop	(선택 사항) 연결 제한(시스템 수준 리소스 제한 및 컨피그레이션에 설정된 제한) 초과로 인해 삭제된 패킷의 비율을 표시합니다.
dos-drop	(선택 사항) 감지된 DoS 공격(예: 잘못된 SPI, 상태 저장 방화벽 확인 실패)으로 인해 삭제된 패킷의 비율을 표시합니다.
fw-drop	(선택 사항) 기본 방화벽 확인 실패로 인해 삭제된 패킷의 비율을 표시합니다. 이 옵션은 이 명령의 모든 방화벽 관련 패킷 삭제를 포함하는 통합 속도입니다. 방화벽과 관련되지 않은 삭제(예: **interface-drop**, **inspect-drop** 및 **scanning-threat**)는 포함하지 않습니다.
icmp-drop	(선택 사항) 의심스러운 ICMP 패킷 감지 거부로 인해 삭제된 패킷의 비율을 표시합니다.
inspect-drop	(선택 사항) 애플리케이션 검사에 실패한 패킷으로 인해 삭제된 패킷의 비율 제한을 표시합니다.
interface-drop	(선택 사항) 인터페이스 오버로드로 인해 삭제된 패킷의 비율 제한을 표시합니다.
scanning-threat	(선택 사항) 감지된 스캔 공격으로 인해 삭제된 패킷의 비율을 표시합니다. 이 옵션은 스캔 공격을 모니터링합니다. 예를 들어 첫 번째 TCP 패킷이 SYN 패킷이 아닌 경우 또는 3방향 핸드셰이크에 실패한 TCP 연결을 모니터링합니다. 전체 스캔 위협 감지(**threat-detection scanning-threat** 명령 참고)에서는 이 스캔 공격 속도 정보를 가져와 호스트를 공격자로 분류하고 이를 자동으로 차단하는 등의 방식으로 조치를 취합니다.
syn-attack	(선택 사항) 불완전한 세션(예: TCP SYN 공격 또는 데이터 없는 UDP 세션 공격)으로 인해 삭제된 패킷의 비율을 표시합니다.

기본값

이벤트 유형을 지정하지 않으면 모든 이벤트가 표시됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 ㅊ모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.2(1)	버스트 속도 간격이 평균 속도의 1/60에서 1/30로 변경되었습니다.
8.2(2)	위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

출력에 표시되는 정보는 다음과 같습니다.

- 고정된 기간 동안의 평균 비율(이벤트/초)
- 마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)
- 비율이 초과된 횟수
- 고정된 기간 동안의 총 이벤트 수

ASA에서는 평균 비율 간격 동안 이벤트 수를 30번 계산합니다. 즉, ASA에서는 총 30번의 완료된 버스트 간격 동안 각 버스트 기간이 끝날 때마다 비율을 확인합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 10분인 경우 버스트 간격은 10초입니다. 마지막 버스트 간격이 3:00:00~3:00:10인 경우 3:00:15에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다.

이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 59번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.

예

다음은 **show threat-detection rate** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection rate

                     Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:             0              0       0                   16
  1-hour ACL  drop:             0              0       0                  112
  1-hour SYN attck:             5              0       2                21438
  10-min  Scanning:             0              0      29                  193
  1-hour  Scanning:           106              0      10               384776
  1-hour Bad  pkts:            76              0       2               274690
  10-min  Firewall:             0              0       3                   22
  1-hour  Firewall:            76              0       2               274844
  10-min DoS attck:             0              0       0                    6
  1-hour DoS attck:             0              0       0                   42
  10-min Interface:             0              0       0                  204
  1-hour Interface:            88              0       0               318225
```

관련 명령

명령	설명
clear threat-detection rate	기본 위협 감지 통계를 지웁니다.
show running-config all threat-detection	개별적으로 구성하지 않은 기본 속도 설정을 포함하여 위협 감지 컨피그레이션을 표시합니다.
threat-detection basic-threat	기본 위협 감지를 활성화합니다.
threat-detection rate	이벤트 유형별 위협 감지 속도 제한을 설정합니다.
threat-detection scanning-threat	스캔 위협 감지를 활성화합니다.

show threat-detection scanning-threat

threat-detection scanning-threat 명령을 사용하여 스캔 위협 감지를 활성화한 경우 특권 EXEC 모드에서 **show threat-detection scanning-threat** 명령을 사용하여 공격자 및 대상으로 분류된 호스트를 볼 수 있습니다.

show threat-detection scanning-threat [**attacker** | **target**]

구문 설명

attacker	(선택 사항) 공격하는 호스트 IP 주소를 표시합니다.
target	(선택 사항) 대상으로 지정된 호스트 IP 주소를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.0(4)	머리글 텍스트에 “& Subnet List”를 포함하도록 화면이 수정되었습니다.
8.2(2)	위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

예

다음은 **show threat-detection scanning-threat** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
```

관련 명령

명령	설명
clear threat-detection shun	호스트를 차단 대상에서 해제합니다.
show threat-detection shun	현재 차단된 호스트를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
show threat-detection statistics top	상위 10개의 통계를 표시합니다.
threat-detection scanning-threat	스캔 위협 감지를 활성화합니다.

show threat-detection shun

threat-detection scanning-threat 명령을 사용하여 스캔 위협 감지를 활성화하고 공격 호스트를 자동으로 차단한 경우 특권 EXEC 모드에서 **show threat-detection shun** 명령을 사용하여 현재 차단된 호스트를 볼 수 있습니다.

show threat-detection shun

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.2(2)	위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

호스트의 차단을 해제하려면 **clear threat-detection shun** 명령을 사용합니다.

예

다음은 **show threat-detection shun** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
```

관련 명령

명령	설명
clear threat-detection shun	호스트를 차단 대상에서 해제합니다.
show threat-detection statistics host	호스트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
show threat-detection statistics top	상위 10개의 통계를 표시합니다.
threat-detection scanning-threat	스캔 위협 감지를 활성화합니다.

show threat-detection statistics host

threat-detection statistics host 명령을 사용하여 위협 통계를 활성화한 후 특권 EXEC 모드에서 **show threat-detection statistics host** 명령을 사용하여 호스트 통계를 볼 수 있습니다. 위협 감지 통계에는 허용된 트래픽 비율과 삭제된 트래픽 비율이 모두 표시됩니다.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

구문 설명

ip_address	(선택 사항) 특정 호스트에 대한 통계를 표시합니다.
mask	(선택 사항) 호스트 IP 주소의 서브넷 마스크를 설정합니다.
min-display-rate *min_display_rate*	(선택 사항) 최소 표시 비율(초당 이벤트 수)을 초과하는 통계로 표시를 제한합니다. 0~2147483647 범위에서 *min_display_rate*를 설정할 수 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.2(1)	버스트 비율 간격이 평균 비율의 1/60에서 1/30로 변경되었습니다.
8.2(2)	위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

출력에 표시되는 정보는 다음과 같습니다.

- 고정된 기간 동안의 평균 비율(이벤트/초)
- 마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)
- 비율 이 초과된 횟수(삭제된 트래픽 통계에만 해당)
- 고정된 기간 동안의 총 이벤트 수

ASA에서는 평균 비율 간격 동안 이벤트 수를 30번 계산합니다. 즉, ASA에서는 총 30번의 완료된 버스트 간격 동안 각 버스트 기간이 끝날 때마다 비율을 확인합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다.

이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.

예

다음은 **show threat-detection statistics host** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:             2938               0       0             10580308
  8-hour Sent byte:              367               0       0             10580308
 24-hour Sent byte:              122               0       0             10580308
  1-hour Sent pkts:               28               0       0               104043
  8-hour Sent pkts:                3               0       0               104043
 24-hour Sent pkts:                1               0       0               104043
  20-min Sent drop:                9               0       1                10851
  1-hour Sent drop:                3               0       1                10851
  1-hour Recv byte:             2697               0       0              9712670
  8-hour Recv byte:              337               0       0              9712670
 24-hour Recv byte:              112               0       0              9712670
  1-hour Recv pkts:               29               0       0               104846
  8-hour Recv pkts:                3               0       0               104846
 24-hour Recv pkts:                1               0       0               104846
  20-min Recv drop:               42               0       3                50567
  1-hour Recv drop:               14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                0               0       0                  614
  8-hour Sent byte:                0               0       0                  614
 24-hour Sent byte:                0               0       0                  614
  1-hour Sent pkts:                0               0       0                    6
  8-hour Sent pkts:                0               0       0                    6
 24-hour Sent pkts:                0               0       0                    6
  20-min Sent drop:                0               0       0                    4
  1-hour Sent drop:                0               0       0                    4
  1-hour Recv byte:                0               0       0                  706
  8-hour Recv byte:                0               0       0                  706
 24-hour Recv byte:                0               0       0                  706
  1-hour Recv pkts:                0               0       0                    7
```

표 13-2에는 각 필드에 대한 설명이 나와 있습니다.

표 13-2 show threat-detection statistics host 필드

필드	설명
Host	호스트 IP 주소를 표시합니다.
tot-ses	데이터베이스에 추가된 이후의 이 호스트에 대한 총 세션 수를 표시합니다.
act-ses	호스트가 현재 참여한 총 활성 세션 수를 표시합니다.
fw-drop	방화벽 삭제 수를 표시합니다. 방화벽 삭제 수는 액세스 목록 거부, 잘못된 패킷, 연결 제한 초과, DoS 공격 패킷, 의심스러운 ICMP 패킷, TCP SYN 공격 패킷, 데이터 없는 UDP 공격 패킷 등 기본 위협 감지에서 추적된 모든 방화벽 관련 패킷 삭제를 포함하는 통합 속도입니다. 인터페이스 오버로드, 애플리케이션 검사에 실패한 패킷, 스캔 공격 감지 등 방화벽과 관련이 없는 삭제는 포함되지 않습니다.
insp-drop	애플리케이션 검사에 실패했기 때문에 삭제된 패킷 수를 표시합니다.

표 13-2 show threat-detection statistics host 필드 (계속)

필드	설명
null-ses	30초 시간 제한 이내에 완료되지 않은 TCP SYN 세션 및 세션이 시작된 후 3초 이내에 해당 서버에서 데이터가 전송되지 않은 UDP 세션인 null 세션 수를 표시합니다.
bad-acc	닫힌 상태의 호스트 포트에 대한 잘못된 액세스 시도 횟수를 표시합니다. 포트가 null 세션(위 참고)에 있는 것으로 확인된 경우에는 호스트의 포트 상태가 HOST_PORT_CLOSE로 설정됩니다. 이 호스트의 포트에 액세스하는 모든 클라이언트는 시간 제한을 대기할 필요 없이 잘못된 액세스로 즉시 분류됩니다.
Average(eps)	각 기간 동안의 평균 비율(이벤트/초)을 표시합니다. 보안 어플라이언스는 총 30번의 완료된 버스트 간격에 대해 각 버스트 기간이 끝날 때마다 개수를 저장합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
Current(eps)	마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)을 표시합니다. Average(eps) 설명에 지정된 예의 경우 현재 비율은 3:19:30에서 3:20:00까지의 비율입니다.
Trigger	삭제된 패킷 비율 제한을 초과한 횟수를 표시합니다. 보내고 받은 바이트 및 패킷 행에 식별된 유효한 트래픽의 경우 유효한 트래픽에 대해 트리거되는 비율 제한이 없기 때문에 이 값은 항상 0입니다.
Total events	각 비율 간격 동안의 총 이벤트 수를 표시합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 총 이벤트에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
20-min, 1-hour, 8-hour 및 24-hour	기본적으로 세 가지 비율 간격이 표시됩니다. **threat-detection statistics host number-of-rate** 명령을 사용하여 비율 간격 수를 줄일 수 있습니다. 호스트 통계는 많은 메모리를 사용하기 때문에 비율 간격 수를 기본값 3에서 줄이면 메모리 사용량이 줄어듭니다. 이 키워드를 1로 설정하면 가장 짧은 비율 간격 통계가 유지됩니다. 이 값을 2로 설정하면 두 개의 가장 짧은 간격이 유지됩니다.
Sent byte	호스트에서 성공적으로 전송한 바이트 수를 표시합니다.
Sent pkts	호스트에서 성공적으로 전송한 패킷 수를 표시합니다.
Sent drop	호스트에서 전송한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.
Recv byte	호스트에서 성공적으로 수신한 바이트 수를 표시합니다.

표 13-2 show threat-detection statistics host 필드 (계속)

필드	설명
Recv pkts	호스트에서 성공적으로 수신한 패킷 수를 표시합니다.
Recv drop	호스트에서 수신한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.

관련 명령

명령	설명
threat-detection scanning-threat	스캔 위협 감지를 활성화합니다.
show threat-detection statistics top	상위 10개의 통계를 표시합니다.
show threat-detection statistics port	포트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
threat-detection statistics	위협 통계를 활성화합니다.

show threat-detection statistics port

threat-detection statistics port 명령을 사용하여 위협 통계를 활성화한 후 특권 EXEC 모드에서 **show threat-detection statistics port** 명령을 사용하여 TCP 및 UDP 포트 통계를 볼 수 있습니다. 위협 감지 통계에는 허용된 트래픽 비율과 삭제된 트래픽 비율이 모두 표시됩니다.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]

구문 설명

start_port[**-***end_port*]	(선택 사항) 특정 포트 또는 포트 범위(0~65535)에 대한 통계를 표시합니다.
min-display-rate *min_display_rate*	(선택 사항) 최소 표시 비율(초당 이벤트 수)을 초과하는 통계로 표시를 제한합니다. 0~2147483647 범위에서 *min_display_rate*를 설정할 수 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.2(1)	버스트 비율 간격이 평균 비율의 1/60에서 1/30로 변경되었습니다.
8.2(2)	위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

출력에 표시되는 정보는 다음과 같습니다.

- 고정된 기간 동안의 평균 비율(이벤트/초)
- 마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)
- 비율 이 초과된 횟수(삭제된 트래픽 통계에만 해당)
- 고정된 기간 동안의 총 이벤트 수

ASA에서는 평균 비율 간격 동안 이벤트 수를 30번 계산합니다. 즉, ASA에서는 총 30번의 완료된 버스트 간격 동안 각 버스트 기간이 끝날 때마다 비율을 확인합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다.

이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.

예

다음은 **show threat-detection statistics port** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics port

                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939              0       0             10580922
  8-hour Sent byte:                367          22043       0             10580922
 24-hour Sent byte:                122           7347       0             10580922
  1-hour Sent pkts:                 28              0       0               104049
  8-hour Sent pkts:                  3            216       0               104049
 24-hour Sent pkts:                  1             72       0               104049
  20-min Sent drop:                  9              0       2                10855
  1-hour Sent drop:                  3              0       2                10855
  1-hour Recv byte:               2698              0       0              9713376
  8-hour Recv byte:                337          20236       0              9713376
 24-hour Recv byte:                112           6745       0              9713376
  1-hour Recv pkts:                 29              0       0               104853
  8-hour Recv pkts:                  3            218       0               104853
 24-hour Recv pkts:                  1             72       0               104853
  20-min Recv drop:                 24              0       2                29134
  1-hour Recv drop:                  8              0       2                29134
```

표 13-3에는 각 필드에 대한 설명이 나와 있습니다.

표 13-3 show threat-detection statistics port 필드

필드	설명
Average(eps)	각 기간 동안의 평균 비율(이벤트/초)을 표시합니다. 보안 어플라이언스는 총 30번의 완료된 버스트 간격에 대해 각 버스트 기간이 끝날 때마다 개수를 저장합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
Current(eps)	마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)을 표시합니다. Average(eps) 설명에 지정된 예의 경우 현재 비율은 3:19:30에서 3:20:00까지의 비율입니다.
Trigger	삭제된 패킷 비율 제한을 초과한 횟수를 표시합니다. 보내고 받은 바이트 및 패킷 행에 식별된 유효한 트래픽의 경우 유효한 트래픽에 대해 트리거되는 비율 제한이 없기 때문에 이 값은 항상 0입니다.

표 13-3 show threat-detection statistics port 필드 (계속)

필드	설명
Total events	각 비율 간격 동안의 총 이벤트 수를 표시합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 총 이벤트에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
port_number/*port_name*	패킷 또는 바이트가 전송, 수신 또는 삭제된 포트 번호 및 이름을 표시합니다.
tot-ses	이 포트에 대한 총 세션 수를 표시합니다.
act-ses	포트가 현재 참여한 총 활성 세션 수를 표시합니다.
20-min, 1-hour, 8-hour 및 24-hour	이러한 고정 비율 간격 동안의 통계를 표시합니다.
Sent byte	포트에서 성공적으로 전송한 바이트 수를 표시합니다.
Sent pkts	포트에서 성공적으로 전송한 패킷 수를 표시합니다.
Sent drop	포트에서 전송한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.
Recv byte	포트에서 성공적으로 수신한 바이트 수를 표시합니다.
Recv pkts	포트에서 성공적으로 수신한 패킷 수를 표시합니다.
Recv drop	포트에서 수신한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.

관련 명령

명령	설명
threat-detection scanning-threat	스캔 위협 감지를 활성화합니다.
show threat-detection statistics top	상위 10개의 통계를 표시합니다.
show threat-detection statistics host	호스트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
threat-detection statistics	위협 통계를 활성화합니다.

show threat-detection statistics protocol

threat-detection statistics protocol 명령을 사용하여 위협 통계를 활성화한 후 특권 EXEC 모드에서 **show threat-detection statistics protocol** 명령을 사용하여 IP 프로토콜 통계를 볼 수 있습니다. 위협 감지 통계에는 허용된 트래픽 비율과 삭제된 트래픽 비율이 모두 표시됩니다.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

구문 설명

protocol_number	(선택 사항) 특정 프로토콜 번호(0~255)에 대한 통계를 표시합니다.
min-display-rate *min_display_rate*	(선택 사항) 최소 표시 비율(초당 이벤트 수)을 초과하는 통계로 표시를 제한합니다. 0~2147483647 범위에서 *min_display_rate*를 설정할 수 있습니다.
protocol_name	(선택 사항) 특정 프로토콜 이름에 대한 통계를 표시합니다. • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.2(1)	버스트 비율 간격이 평균 비율의 1/60에서 1/30로 변경되었습니다.
8.2(2)	위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

출력에 표시되는 정보는 다음과 같습니다.

- 고정된 기간 동안의 평균 비율(이벤트/초)
- 마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)
- 비율이 초과된 횟수(삭제된 트래픽 통계에만 해당)
- 고정된 기간 동안의 총 이벤트 수

ASA에서는 평균 비율 간격 동안 이벤트 수를 30번 계산합니다. 즉, ASA에서는 총 30번의 완료된 버스트 간격 동안 각 버스트 기간이 끝날 때마다 비율을 확인합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다.

이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.

예

다음은 **show threat-detection statistics protocol** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

표 13-4에는 각 필드에 대한 설명이 나와 있습니다.

표 13-4 show threat-detection statistics protocol 필드

필드	설명
Average(eps)	각 기간 동안의 평균 비율(이벤트/초)을 표시합니다. 보안 어플라이언스는 총 30번의 완료된 버스트 간격에 대해 각 버스트 기간이 끝날 때마다 개수를 저장합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
Current(eps)	마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)을 표시합니다. Average(eps) 설명에 지정된 예의 경우 현재 비율은 3:19:30에서 3:20:00까지의 비율입니다.
Trigger	삭제된 패킷 비율 제한을 초과한 횟수를 표시합니다. 보내고 받은 바이트 및 패킷 행에 식별된 유효한 트래픽의 경우 유효한 트래픽에 대해 트리거되는 비율 제한이 없기 때문에 이 값은 항상 0입니다.
Total events	각 비율 간격 동안의 총 이벤트 수를 표시합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 총 이벤트에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
protocol_number/ protocol_name	패킷 또는 바이트가 전송, 수신 또는 삭제된 프로토콜 번호 및 이름을 표시합니다.
tot-ses	현재 사용되지 않습니다.
act-ses	현재 사용되지 않습니다.
20-min, 1-hour, 8-hour 및 24-hour	이러한 고정 비율 간격 동안의 통계를 표시합니다.
Sent byte	프로토콜에서 성공적으로 전송한 바이트 수를 표시합니다.
Sent pkts	프로토콜에서 성공적으로 전송한 패킷 수를 표시합니다.
Sent drop	프로토콜에서 전송한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.
Recv byte	프로토콜에서 성공적으로 수신한 바이트 수를 표시합니다.
Recv pkts	프로토콜에서 성공적으로 수신한 패킷 수를 표시합니다.
Recv drop	프로토콜에서 수신한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.

관련 명령

명령	설명
threat-detection scanning-threat	스캔 위협 감지를 활성화합니다.
show threat-detection statistics top	상위 10개의 통계를 표시합니다.
show threat-detection statistics port	포트 통계를 표시합니다.
show threat-detection statistics host	호스트 통계를 표시합니다.
threat-detection statistics	위협 통계를 활성화합니다.

show threat-detection statistics top

threat-detection statistics 명령을 사용하여 위협 통계를 활성화한 후 특권 EXEC 모드에서 **show threat-detection statistics top** 명령을 사용하여 상위 10개 통계를 볼 수 있습니다. 특정 유형에 대한 위협 감지 통계를 활성화하지 않은 경우에는 이 명령을 사용하여 해당 통계를 볼 수 없습니다. 위협 감지 통계에는 허용된 트래픽 비율과 삭제된 트래픽 비율이 모두 표시됩니다.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] [**detail**] [**long**]]

구문 설명

access-list	(선택 사항) 허용 및 거부 ACE를 포함하여 패킷과 일치하는 상위 10개의 ACE를 표시합니다. 허용된 트래픽과 거부된 트래픽은 이 화면에서 구분되지 않습니다. **threat-detection basic-threat** 명령을 사용하여 기본 위협 감지를 활성화한 경우 **show threat-detection rate access-list** 명령을 사용하여 액세스 목록 거부를 추적할 수 있습니다.
all	(선택 사항) TCP 가로채기에 대해 추적된 모든 서버의 내역 데이터를 표시합니다.
detail	(선택 사항) TCP 가로채기에 대해 내역 샘플링 데이터를 표시합니다.
host	(선택 사항) 각 고정 기간 동안의 상위 10개 호스트 통계를 표시합니다. **참고** 위협 감지 알고리즘으로 인해 대체작동 링크 또는 상태 링크에 사용된 인터페이스는 상위 10개의 호스트 중 하나로 표시될 수 있습니다. 특히 하나의 인터페이스를 대체작동 링크와 상태 링크 둘 다에 사용하는 경우에 그럴 가능성이 더 높습니다. 이는 예상된 동작이며, 화면에서 이 IP 주소를 무시할 수 있습니다.
long	(선택 사항) 서버의 실제 IP 주소 및 변환되지 않은 IP 주소와 함께 긴 형식의 통계 내역을 표시합니다.
min-display-rate *min_display_rate*	(선택 사항) 최소 표시 비율(초당 이벤트 수)을 초과하는 통계로 표시를 제한합니다. 0~2147483647 범위에서 *min_display_rate*를 설정할 수 있습니다.
port-protocol	(선택 사항) TCP/UDP 포트와 IP 프로토콜 유형이 조합된 상위 10개의 통계를 표시합니다. TCP(프로토콜 6) 및 UDP(프로토콜 17)는 IP 프로토콜에 대한 표시에는 포함되지 않지만 포트에 대한 표시에는 포함됩니다. 이러한 유형 중 하나(포트 또는 프로토콜)에 대해서만 통계를 활성화한 경우에는 활성화한 통계만 볼 수 있습니다.
rate-1	(선택 사항) 표시할 수 있는 가장 작은 고정 비율 간격에 대한 통계를 표시합니다. 예를 들어 지난 1시간, 8시간 및 24시간에 대한 통계가 표시된 경우 **rate-1** 키워드를 사용하면 ASA에서 1시간 간격만 표시합니다.
rate-2	(선택 사항) 표시할 수 있는 중간 고정 비율 간격에 대한 통계를 표시합니다. 예를 들어 지난 1시간, 8시간 및 24시간에 대한 통계가 표시된 경우 **rate-2** 키워드를 사용하면 ASA에서 8시간 간격만 표시합니다.
rate-3	(선택 사항) 표시할 수 있는 가장 큰 고정 비율 간격에 대한 통계를 표시합니다. 예를 들어 지난 1시간, 8시간 및 24시간에 대한 통계가 표시된 경우 **rate-3** 키워드를 사용하면 ASA에서 24시간 간격만 표시합니다.
tcp-intercept	TCP 가로채기 통계를 표시합니다. 공격에서 보호된 상위 10개의 서버가 포함됩니다.

기본값

이벤트 유형을 지정하지 않으면 모든 이벤트가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.0(4)	**tcp-intercept** 키워드가 추가되었습니다.
8.2(1)	버스트 비율 간격이 평균 비율의 1/60에서 1/30로 변경되었습니다.
8.2(2)	**long** 키워드가 **tcp-intercept**에 대해 추가되었습니다. 위협 이벤트의 경우 심각도 수준이 경고에서 알림으로 변경되었습니다. 위협 이벤트는 5분마다 트리거될 수 있습니다.

사용 지침

출력에 표시되는 정보는 다음과 같습니다.

- 고정된 기간 동안의 평균 비율(이벤트/초)
- 마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)
- 비율 이 초과된 횟수(삭제된 트래픽 통계에만 해당)
- 고정된 기간 동안의 총 이벤트 수

ASA에서는 평균 비율 간격 동안 이벤트 수를 30번 계산합니다. 즉, ASA에서는 총 30번의 완료된 버스트 간격 동안 각 버스트 기간이 끝날 때마다 비율을 확인합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다.

이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.

예

다음은 **show threat-detection statistics top access-list** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics top access-list

                    Top     Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]              173               0       0               623488
              200/2[1]               43               0       0               156786
              100/1[2]               43               0       0               156786
  8-hour ACL hits:
              100/3[0]               21            1298       0               623488
              200/2[1]                5             326       0               156786
              100/1[2]                5             326       0               156786
```

표 13-5에는 각 필드에 대한 설명이 나와 있습니다.

표 13-5 show threat-detection statistics top access-list 필드

필드	설명
Top	기간 내 ACE의 순위([0](최대 개수)~[9](최소 개수))를 표시합니다. 10개 위치 모두에 대한 통계가 부족할 수 있으므로 10개 미만의 ACE가 나열될 수도 있습니다.
Average(eps)	각 기간 동안의 평균 비율(이벤트/초)을 표시합니다. 보안 어플라이언스는 총 30번의 완료된 버스트 간격에 대해 각 버스트 기간이 끝날 때마다 개수를 저장합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 평균 비율에 포함되지 않습니다. 예를 들어 평균 비율 간격이 20분인 경우 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20인 경우 3:00:25에 **show** 명령을 사용하면 마지막 5초만 출력에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
Current(eps)	마지막으로 완료된 버스트 간격(평균 비율 간격의 1/30과 10초 중 큰 값)에서의 현재 버스트 비율(이벤트/초)을 표시합니다. Average(eps) 설명에 지정된 예의 경우 현재 비율은 3:19:30에서 3:20:00까지의 비율입니다.
Trigger	액세스 목록 트래픽에 의해 트리거되는 비율 제한이 없기 때문에 이 열은 항상 0입니다. 허용된 트래픽과 거부된 트래픽은 이 화면에서 구분되지 않습니다. **threat-detection basic-threat** 명령을 사용하여 기본 위협 감지를 활성화한 경우 **show threat-detection rate access-list** 명령을 사용하여 액세스 목록 거부를 추적할 수 있습니다.
Total events	각 비율 간격 동안의 총 이벤트 수를 표시합니다. 현재 발생 중인 완료되지 않은 버스트 간격은 총 이벤트에 포함되지 않습니다. 이 규칙의 유일한 예외는 총 이벤트를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(1/30)의 이벤트 수를 이미 초과한 경우입니다. 이 경우 ASA는 나머지 29번의 완료 간격에 대한 총 이벤트와 완료되지 않은 버스트 간격에서 현재까지의 이벤트를 합산합니다. 이러한 예외를 통해 이벤트 급증을 실시간으로 모니터링할 수 있습니다.
1-hour, 8-hour	이러한 고정 비율 간격 동안의 통계를 표시합니다.
acl_name/line_number	거부를 일으킨 액세스 목록 번호와 ACE 줄 번호를 표시합니다.

다음은 **show threat-detection statistics top access-list rate-1** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics top access-list rate-1

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
               100/3[0]              173                0       0               623488
               200/2[1]               43                0       0               156786
               100/1[2]               43                0       0               156786
```

다음은 **show threat-detection statistics top port-protocol** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics top port-protocol

Top           Name    Id     Average(eps)     Current(eps) Trigger      Total events
  1-hour Recv byte:
 1          gopher    70               71                0       0          32345678
 2   btp-clnt/dhcp    68               68                0       0          27345678
 3          gopher    69               65                0       0          24345678
 4     Protocol-96 * 96               63                0       0          22345678
 5       Port-7314 7314               62                0       0          12845678
 6 BitTorrent/trc 6969               61                0       0          12645678
 7      Port-8191-65535              55                0       0          12345678
 8            SMTP  366              34                0       0           3345678
 9          IPinIP *  4              30                0       0           2345678
10           EIGRP * 88              23                0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...
```

참고: 앞에 *가 있는 ID는 해당 ID가 IP 프로토콜 유형임을 나타냅니다.

표 13-6에는 각 필드에 대한 설명이 나와 있습니다.

표 13-6 show threat-detection statistics top port-protocol 필드

필드	설명
Top	통계 기간/유형 내 포트 또는 프로토콜의 순위([0](최대 개수)~[9](최소 개수))를 표시합니다. 10개 위치 모두에 대한 통계가 부족할 수 있으므로 10개 미만의 포트/프로토콜이 나열될 수도 있습니다.
Name	포트/프로토콜 이름을 표시합니다.
Id	포트/프로토콜 ID 번호를 표시합니다. 별표(*)는 ID가 IP 프로토콜 번호임을 의미합니다.
Average(eps)	표 13-2의 설명을 참고하십시오.
Current(eps)	표 13-2의 설명을 참고하십시오.

표 13-6 show threat-detection statistics top port-protocol 필드 (계속)

필드	설명
Trigger	삭제된 패킷 비율 제한을 초과한 횟수를 표시합니다. 보내고 받은 바이트 및 패킷 행에 식별된 유효한 트래픽의 경우 유효한 트래픽에 대해 트리거되는 비율 제한이 없기 때문에 이 값은 항상 0입니다.
Total events	표 13-2의 설명을 참고하십시오.
Time_interval Sent byte	각 기간 동안 나열된 포트 및 프로토콜에서 성공적으로 전송한 바이트 수를 표시합니다.
Time_interval Sent packet	각 기간 동안 나열된 포트 및 프로토콜에서 성공적으로 전송한 패킷 수를 표시합니다.
Time_interval Sent drop	각 기간 동안 나열된 포트 및 프로토콜에서 전송한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.
Time_interval Recv byte	각 기간 동안 나열된 포트 및 프로토콜에서 성공적으로 수신한 바이트 수를 표시합니다.
Time_interval Recv packet	각 기간 동안 나열된 포트 및 프로토콜에서 성공적으로 수신한 패킷 수를 표시합니다.
Time_interval Recv drop	각 기간 동안 나열된 포트 및 프로토콜에서 수신한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.
port_number/ *port_name*	패킷 또는 바이트가 전송, 수신 또는 삭제된 포트 번호 및 이름을 표시합니다.
protocol_number/ *protocol_name*	패킷 또는 바이트가 전송, 수신 또는 삭제된 프로토콜 번호 및 이름을 표시합니다.

다음은 **show threat-detection statistics top host** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics top host

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]             2938                0       0             10580308
  1-hour Sent pkts:
          10.0.0.1[0]               28                0       0               104043
  20-min Sent drop:
          10.0.0.1[0]                9                0       1                10851
  1-hour Recv byte:
          10.0.0.1[0]             2697                0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]               29                0       0               104846
  20-min Recv drop:
          10.0.0.1[0]               42                0       3                50567
  8-hour Sent byte:
          10.0.0.1[0]              367                0       0             10580308
  8-hour Sent pkts:
          10.0.0.1[0]                3                0       0               104043
  1-hour Sent drop:
          10.0.0.1[0]                3                0       1                10851
  8-hour Recv byte:
          10.0.0.1[0]              337                0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]                3                0       0               104846
  1-hour Recv drop:
          10.0.0.1[0]               14                0       1                50567
```

```
24-hour Sent byte:
         10.0.0.1[0]             122              0       0             10580308
24-hour Sent pkts:
         10.0.0.1[0]               1              0       0               104043
24-hour Recv byte:
         10.0.0.1[0]             112              0       0              9712670
24-hour Recv pkts:
         10.0.0.1[0]               1              0       0               104846
```

표 13-7에는 각 필드에 대한 설명이 나와 있습니다.

표 13-7 show threat-detection statistics top host 필드

필드	설명
Top	통계 기간/유형 내 호스트의 순위([0](최대 개수)~[9](최소 개수))를 표시합니다. 10개 위치 모두에 대한 통계가 부족할 수 있으므로 10개 미만의 호스트가 나열될 수도 있습니다.
Average(eps)	표 13-2의 설명을 참고하십시오.
Current(eps)	표 13-2의 설명을 참고하십시오.
Trigger	표 13-2의 설명을 참고하십시오.
Total events	표 13-2의 설명을 참고하십시오.
Time_interval Sent byte	각 기간 동안 나열된 호스트에 성공적으로 전송된 바이트 수를 표시합니다.
Time_interval Sent packet	각 기간 동안 나열된 호스트에 성공적으로 전송된 패킷 수를 표시합니다.
Time_interval Sent drop	각 기간 동안 나열된 호스트에 전송된 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.
Time_interval Recv byte	각 기간 동안 나열된 호스트에서 성공적으로 수신한 바이트 수를 표시합니다.
Time_interval Recv packet	각 기간 동안 나열된 포트 및 프로토콜에서 성공적으로 수신한 패킷 수를 표시합니다.
Time_interval Recv drop	각 기간 동안 나열된 포트 및 프로토콜에서 수신한 패킷 중 스캔 공격에 포함되었기 때문에 삭제된 패킷 수를 표시합니다.
host_ip_address	패킷 또는 바이트가 전송, 수신 또는 삭제된 호스트 IP 주소를 표시합니다.

다음은 **show threat-detection statistics top tcp-intercept** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

표 13-8에는 각 필드에 대한 설명이 나와 있습니다.

표 13-8 show threat-detection statistics top tcp-intercept 필드

필드	설명
Monitoring window size:	ASA에서 통계를 위해 데이터를 샘플링하는 기간을 표시합니다. 기본값은 30분입니다. **threat-detection statistics tcp-intercept rate-interval** 명령을 사용하여 이 설정을 변경할 수 있습니다. ASA에서는 이 간격 동안 데이터를 30번 샘플링합니다.
Sampling interval:	샘플 간의 간격을 표시합니다. 이 값은 항상 30으로 나눈 비율 간격입니다.
rank	순위(1~10)를 표시합니다. 1은 공격을 가장 많이 서버이고, 10은 공격을 가장 적게 받은 서버입니다.
server_ip:port	공격 받는 서버 IP 주소 및 포트를 표시합니다.
interface	서버가 공격 받는 인터페이스를 표시합니다.
avg_rate	샘플링 기간 동안의 평균 공격 비율(초당 공격 횟수)을 표시합니다.
current_rate	현재 공격 비율(초당 공격 횟수)을 표시합니다.
total	총 공격 횟수를 표시합니다.
attacker_ip	공격자 IP 주소를 표시합니다.
(*last_attack_time* ago)	마지막 공격이 발생한 시간을 표시합니다.

다음은 실제 소스 IP 주소를 괄호 안에 입력하여 실행한 **show threat-detection statistics top tcp-intercept long** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total>
<Source IP (Last Attack Time)>
--------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

다음은 **show threat-detection statistics top tcp-intercept detail** 명령의 샘플 출력입니다.

```
ciscoasa# show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
```

```
------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
      Sampling History (30 Samplings):
              95348      95337      95341      95339      95338      95342
              95337      95348      95342      95338      95339      95340
              95339      95337      95342      95348      95338      95342
              95337      95339      95340      95339      95347      95343
              95337      95338      95342      95338      95337      95342
              95348      95338      95342      95338      95337      95343
              95337      95349      95341      95338      95337      95342
              95338      95339      95338      95350      95339      95570
              96351      96351      96119      95337      95349      95341
              95338      95337      95342      95338      95338      95342
.......
```

표 13-9에는 각 필드에 대한 설명이 나와 있습니다.

표 13-9 show threat-detection statistics top tcp-intercept detail 필드

필드	설명
Monitoring window size:	ASA에서 통계를 위해 데이터를 샘플링하는 기간을 표시합니다. 기본값은 30분입니다. **threat-detection statistics tcp-intercept rate-interval** 명령을 사용하여 이 설정을 변경할 수 있습니다. ASA에서는 이 간격 동안 데이터를 30번 샘플링합니다.
Sampling interval:	샘플 간의 간격을 표시합니다. 이 값은 항상 30으로 나눈 비율 간격입니다.
rank	순위(1~10)를 표시합니다. 1은 공격을 가장 많이 서버이고, 10은 공격을 가장 적게 받은 서버입니다.
server_ip:port	공격 받는 서버 IP 주소 및 포트를 표시합니다.
interface	서버가 공격 받는 인터페이스를 표시합니다.
avg_rate	**threat-detection statistics tcp-intercept rate-interval** 명령을 통해 설정된 비율 간격(기본적으로 30분) 동안의 평균 공격 비율(초당 공격 횟수)을 표시합니다. ASA에서는 비율 간격 동안 30초마다 데이터를 샘플링합니다.
current_rate	현재 공격 비율(초당 공격 횟수)을 표시합니다.
total	총 공격 횟수를 표시합니다.
attacker_ip or <*various*> Last: *attacker_ip*	공격자 IP 주소를 표시합니다. 공격자가 둘 이상인 경우 마지막 공격자 IP 주소 앞에 “<various>”가 표시됩니다.
(*last_attack_time* ago)	마지막 공격이 발생한 시간을 표시합니다.
sampling data	각 간격의 공격 횟수를 나타내는 30개의 샘플링 데이터 값을 모두 표시합니다.

관련 명령

명령	설명
threat-detection scanning-threat	스캔 위협 감지를 활성화합니다.
show threat-detection statistics host	호스트 통계를 표시합니다.
show threat-detection statistics port	포트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
threat-detection statistics	위협 통계를 활성화합니다.

show tls-proxy

TLS 프록시 및 세션 정보를 표시하려면 글로벌 컨피그레이션 모드에서 **show tls-proxy** 명령을 사용합니다.

show tls-proxy *tls_name* [**session** [**host** *host_addr* | **detail** [**cert-dump** | **count**] [**statistics**]]

구문 설명

cert-dump	로컬 동적 인증서를 덤프합니다. 출력은 LDC의 16진수 덤프입니다.
count	세션 카운터만 표시합니다.
detail	각 SSL 레드 및 LDC에 대한 암호를 포함하여 자세한 TLS 프록시 정보를 표시합니다.
host *host_addr*	연결된 세션을 표시할 특정 호스트를 지정합니다.
session	활성 TLS 프록시 세션을 표시합니다.
statistics	TLS 세션 모니터링 및 관리에 대한 통계를 표시합니다.
tls_name	표시할 TLS 프록시의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC 모드	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.3(1)	**statistics** 키워드가 추가되었습니다.

예

다음은 **show tls-proxy** 명령의 샘플 출력입니다.

```
ciscoasa# show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
    Server proxy:
        Trust-point: local_ccm
    Client proxy:
        Local dynamic certificate issuer: ldc_signer
        Local dynamic certificate key-pair: phone_common
        Cipher-suite <unconfigured>
    Run-time proxies:
        Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
            Active sess 1, most sess 4, byte 3244
```

다음은 **show tls-proxy session** 명령의 샘플 출력입니다.

```
ciscoasa# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

다음은 **show tls-proxy session detail** 명령의 샘플 출력입니다.

```
ciscoasa# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
    Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
    Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
    Status: Available
    Certificate Serial Number: 29
    Certificate Usage: General Purpose
    Public Key Type: RSA (1024 bits)
    Issuer Name:
        cn=TLS-Proxy-Signer
    Subject Name:
        cn=SEP0002B9EB0AAD
        o=Cisco Systems Inc
        c=US
    Validity Date:
        start date: 00:47:12 PDT Feb 27 2007
        end   date: 00:47:12 PDT Feb 27 2008
    Associated Trustpoints:
```

다음은 **show tls-proxy session statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show tls-proxy session stastics
    TLS Proxy Sessions (Established: 600)
        Mobility:                               200
        UC-IME:                                 400

    Per-Session Licensed TLS Proxy Sessions
    (Established: 222, License Limit: 250)
        SIP:                                      2
        SCCP:                                    20
        Phone Proxy:                            200

    Total TLS Proxy Sessions
        Established:                            822
        Platform Limit:                        1000
```

관련 명령

명령	설명
client	암호 그룹을 정의하고 로컬 동적 인증서 발급자 또는 키 쌍을 설정합니다.
ctl-provider	CTL 공급자 인스턴스를 정의하고 공급자 컨피그레이션 모드를 시작합니다.
show running-config tls-proxy	모든 또는 지정된 TLS 프록시의 실행 중인 컨피그레이션을 표시합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

show track

추적 프로세스에 의해 추적된 개체에 대한 정보를 표시하려면 사용자 EXEC 모드에서 **show track** 명령을 사용합니다.

show track [*track-id*]

구문 설명

track-id	추적 항목 개체 ID입니다. 유효한 값은 1~500입니다.

기본값

*track-id*를 제공하지 않으면 추적하는 모든 개체에 대한 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음은 **show track** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 03:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

관련 명령

명령	설명
show running-config track	실행 중인 컨피그레이션의 **track rtr** 명령을 표시합니다.
track rtr	SLA를 폴링할 추적 항목을 생성합니다.

show traffic

인터페이스 전송 및 수신 활동을 표시하려면 특권 EXEC 모드에서 **show traffic** 명령을 사용합니다.

show traffic

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	ASA 5550에 대한 출력이 추가되었습니다.
9.3(1)	물리적 인터페이스에서 집계된 트래픽에 대한 출력이 추가되었습니다.

사용 지침

show traffic 명령은 **show traffic** 명령이 마지막으로 입력되거나 ASA가 온라인 상태가 된 이후에 각 인터페이스를 통해 이동한 패킷 및 바이트 수를 나열합니다. 시간(초)은 ASA가 마지막 재부팅 후 온라인 상태로 유지된 기간입니다(마지막 재부팅 후 **clear traffic** 명령이 입력되지 않은 경우). 마지막 재부팅 후 clear traffic 명령이 입력된 경우 시간(초)은 해당 명령이 입력된 이후의 기간입니다.

ASA 5550의 경우 **show traffic** 명령은 슬롯당 집계된 처리량도 표시합니다. ASA 5550에서는 최대 처리량을 위해 슬롯 간에 트래픽을 균일하게 분배해야 하기 때문에 이 출력은 트래픽이 균일하게 분배되었는지 확인하는 데 유용합니다.

물리적 인터페이스에서 집계된 트래픽을 표시하려면 먼저 **sysopt traffic detailed-statistics** 명령을 입력하여 이 기능을 설정해야 합니다.

예

다음은 **show traffic** 명령의 샘플 출력입니다.

```
ciscoasa# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
```

```
        received (in 102.080 secs):
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

ASA 5550의 경우 다음 텍스트가 마지막에 표시됩니다.

```
---------------------------------------
        Per Slot Throughput Profile
---------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|****************
    Slot 1:       3149  50%|****************

  Bytes-per-second profile:
    Slot 0:     427044  50%|****************
    Slot 1:     427094  50%|****************
```

다음 예에서는 물리적 인터페이스에서 집계된 트래픽에 대한 추가 출력을 보여 줍니다.

```
IP packet size distribution (values listed in percentages)
Total Packets = 1278:
      32    64    96   128   192   256   512
    00.0  43.5  10.4  10.1  26.1  01.4  03.6

    1024  1536  2048  4096  8192  9216
    03.6  06.6  00.0  00.0  00.0  00.0

Protocol         Total    Conns   Packets   Bytes  Packets    Total
--------         Conns     /Sec     /Conn    /Pkt     /Sec  Packets
TCP                  8      0.2        98     215      26.8     1279
TCP-inspected        0      0.0       N/A     N/A       0.0        0
UDP                  3      0.0         0      90       0.0        2
UDP-inspected        5      0.0         1     189       0.0       56
ICMP                 0      0.0         1      98       0.0        2
IP                   0      0.0       N/A     N/A       0.0        0
Total:              16      0.2        22     207      26.8     1433

Last clearing of statistics: Never
```

관련 명령

명령	설명
clear traffic	전송 및 수신 활동에 대한 카운터를 재설정합니다.

14 장

show uauth through show xlate 명령

show uauth

현재 인증된 한 명의 사용자 또는 모든 사용자, 해당 사용자가 바인딩된 호스트 IP 및 캐시된 모든 IP 및 포트 권한 부여 정보를 표시하려면 특권 EXEC 모드에서 **show uauth** 명령을 사용합니다.

show uauth [*username*]

구문 설명

username	(선택 사항) 표시할 사용자 인증 및 권한 부여 정보를 사용자 이름별로 지정합니다.

기본값

사용자 이름을 생략하면 모든 사용자에 대한 권한 부여 정보가 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.2(1)	유휴 시간이 출력에 추가되었습니다.
7.2(2)	유휴 시간이 출력에서 제거되었습니다.

사용 지침

show uauth 명령은 사용자 한 명 또는 모든 사용자에 대한 AAA 인증 및 권한 부여 캐시를 표시합니다.

이 명령은 **timeout** 명령과 함께 사용됩니다.

각 사용자 호스트 IP 주소에는 권한 부여 캐시가 연결되어 있습니다. 캐시에서는 각 사용자 호스트에 대한 최대 16개의 주소 및 서비스 쌍이 허용됩니다. 사용자가 올바른 호스트에서 캐시된 서비스에 액세스하려는 경우 ASA는 이를 사전 권한 부여된 것으로 간주하여 연결을 즉시 프록시합니다. 예를 들어 웹사이트에 액세스할 권한이 있는 경우 각 이미지가 로드될 때 권한 부여 서버에 연결하지 않습니다(동일한 IP 주소에서 이미지를 가져온 것으로 가정). 이 프로세스는 권한 부여 서버의 성능을 크게 향상시키고 부하를 감소시킵니다.

show uauth 명령의 출력에는 인증 및 권한 부여를 위해 권한 부여 서버에 제공된 사용자 이름, 해당 사용자 이름이 바인딩된 IP 주소, 사용자가 인증되기만 했는지 또는 캐시된 서비스가 있는지 등이 표시됩니다.

참고 Xauth를 활성화한 경우에는 클라이언트에 할당된 IP 주소에 대한 uauth 테이블(**show uauth** 명령으로 표시)에 항목이 추가됩니다. 그러나 네트워크 확장 모드에서 Easy VPN Remote 기능과 함께 Xauth를 사용할 때는 네트워크 간에 IPsec 터널이 생성되므로 방화벽 뒤에 있는 사용자를 단일 IP 주소와 연결할 수 없습니다. 따라서 Xauth 완료 시 uauth 항목을 생성할 수 없습니다. AAA 권한 부여 또는 계정 관리 서비스가 필요한 경우 AAA 인증 프록시를 활성화하여 방화벽 뒤에 있는 사용자를 인증할 수 있습니다. AAA 인증 프록시에 대한 자세한 내용은 **aaa** 명령을 참고하십시오.

timeout uauth 명령을 사용하여 사용자 연결이 유휴 상태가 된 후 캐시를 유지해야 하는 기간을 지정할 수 있습니다. **clear uauth** 명령을 사용하여 모든 사용자에 대한 모든 권한 부여 캐시를 삭제할 수 있습니다. 이 경우 사용자는 다음에 연결을 만들 때 다시 인증해야 합니다.

예

다음 예에서는 인증된 사용자가 없고 사용자 한 명에 대한 인증이 진행 중인 경우 **show uauth** 명령의 샘플 출력을 보여 줍니다.

```
ciscoasa(config)# show uauth
                        Current    Most Seen
Authenticated Users       1           1
Authen In Progress        0           1
user 'v039294' at 136.131.178.4, authenticated (idle for 0:00:00)
   access-list #ACSACL#-IP-v039294-521b0b8b (*)
   absolute   timeout: 0:00:00
   inactivity timeout: 0:05:00
```

다음 예에서는 세 명의 사용자가 인증되고 ASA를 통해 서비스를 사용할 권한을 부여받은 경우 **show uauth** 명령의 샘플 출력을 보여 줍니다.

```
ciscoasa(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

관련 명령

명령	설명
clear uauth	현재 사용자 인증 및 권한 부여 정보를 제거합니다.
timeout	최대 유휴 시간을 설정합니다.

show url-block

url-block 버퍼에서 유지되는 패킷 수 및 버퍼 제한 또는 재전송을 초과하여 삭제된 패킷 수(있는 경우)를 표시하려면 특권 EXEC 모드에서 **show url-block** 명령을 사용합니다.

show url-block [**block statistics**]

구문 설명

block statistics	(선택 사항) 블록 버퍼 사용 통계를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show url-block block statistics 명령은 url-block 버퍼에서 유지되는 패킷 수 및 버퍼 제한 또는 재전송을 초과하여 삭제된 패킷 수(있는 경우)를 표시합니다.

예

다음은 **show url-block** 명령의 샘플 출력입니다.

```
ciscoasa# show url-block
|url-block url-mempool 128|url-block url-size 4|url-block block 128
```

이는 URL 블록 버퍼의 컨피그레이션을 보여 줍니다.

다음은 **show url-block block statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128|
Cumulative number of packets held:|896
Maximum number of packets held (per URL):|3
Current number of packets held (global):|38
Packets dropped due to
|exceeding url-block buffer limit:|7546
|HTTP server retransmission:|10
Number of packets released back to client:|0
```

관련 명령

명령	설명
clear url-block block statistics	블록 버퍼 사용 카운터를 지웁니다.
filter url	URL 필터링 서버로 트래픽을 전송합니다.
url-block	웹 서버 응답에 사용되는 URL 버퍼를 관리합니다.
url-cache	N2H2 또는 Websense 서버에서 응답이 보류 중인 동안 URL 캐싱을 활성화하고 캐시 크기를 설정합니다.
url-server	**filter** 명령에서 사용할 N2H2 또는 Websense 서버를 식별합니다.

show url-cache statistics

N2H2 또는 Websense 필터링 서버에서 받은 URL 응답에 사용되는 url-cache에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show url-cache statistics** 명령을 사용합니다.

show url-cache statistics

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show url-cache statistics 명령은 다음 항목을 표시합니다.

- Size - **url-cache** *size* 옵션으로 설정된 캐시 크기(킬로바이트)입니다.
- Entries - 캐시 크기에 따른 최대 캐시 항목 수입니다.
- In Use - 캐시의 현재 항목 수입니다.
- Lookups - ASA에서 캐시 항목을 조회한 횟수입니다.
- Hits - ASA에서 캐시 항목을 찾은 횟수입니다.

show perfmon 명령을 사용하여 N2H2 Sentian 또는 Websense 필터링 활동에 대한 추가 정보를 확인할 수 있습니다.

예

다음은 **show url-cache statistics** 명령의 샘플 출력입니다.

```
ciscoasa# show url-cache statistics

URL Filter Cache Stats
----------------------
 Size :     1KB
 Entries :     36
  In Use :     30
 Lookups :     300
 Hits :     290
```

관련 명령

명령	설명
clear url-cache statistics	컨피그레이션에서 **url-cache** 명령문을 제거합니다.
filter url	URL 필터링 서버로 트래픽을 전송합니다.
url-block	웹 서버 응답에 사용되는 URL 버퍼를 관리합니다.
url-cache	N2H2 또는 Websense 서버에서 받은 응답에 대해 URL 캐싱을 활성화하고 캐시 크기를 설정합니다.
url-server	**filter** 명령에서 사용할 N2H2 또는 Websense 서버를 식별합니다.

show url-server

URL 필터링 서버에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show url-server** 명령을 사용합니다.

show url-server statistics

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

show url-server statistics 명령은 URL 서버 공급업체, 총/허용된/거부된 URL 수, 총/허용된/거부된 HTTPS 연결 수, 총/허용된/거부된 TCP 연결 수 및 URL 서버 상태를 표시합니다.

show url-server 명령은 다음 정보를 표시합니다.

- N2H2의 경우 **url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol** [{**TCP | UDP**}{**version 1 | 4**}]
- Websense의 경우 **url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol** [{**TCP | UDP**}]

예

다음은 **show url-server statistics** 명령의 샘플 출력입니다.

```
ciscoasa## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
FTPs allowed by cache/server      70483/85165
FTPs denied by cache/server       801920/36819
```

```
Requests dropped                  28715
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                       UP
Vendor                            websense
Port                              17035
Requests total/allowed/denied     366519/255495/110457
Server timeouts/retries           567/1350
Responses received                365952
Response time average 60s/300s    2/1 seconds/request
192.168.0.2                       DOWN
Vendor                            websense
Port                              17035
Requests total/allowed/denied     0/0/0
Server timeouts/retries           0/0
Responses received                0
Response time average 60s/300s    0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                 Sent    Received
STATUS_REQUEST          411     0
LOOKUP_REQUEST          366519  365952
LOG_REQUEST             0       NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0

Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis. The output is reformatted to provide: more-detailed information and
per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

관련 명령

명령	설명
clear url-server	URL 필터링 서버 통계를 지웁니다.
filter url	URL 필터링 서버로 트래픽을 전송합니다.
url-block	웹 서버 응답에 사용되는 URL 버퍼를 관리합니다.
url-cache	N2H2 또는 Websense 서버에서 응답이 보류 중인 동안 URL 캐싱을 활성화하고 캐시 크기를 설정합니다.
url-server	**filter** 명령에서 사용할 N2H2 또는 Websense 서버를 식별합니다.

show user-identity ad-agent

ID 방화벽의 AD 에이전트에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show user-identity ad-agent** 명령을 사용합니다.

show user-identity ad-agent [**statistics**]

구문 설명

statistics	(선택 사항) AD 에이전트에 대한 통계 정보를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

ID 방화벽의 AD 에이전트 구성 요소를 모니터링할 수 있습니다.

show user-identity ad-agent 명령을 사용하여 AD 에이전트에 대한 문제 해결 정보를 가져올 수 있습니다. 이 명령은 기본 및 보조 AD 에이전트에 대한 다음 정보를 표시합니다.

- AD 에이전트의 상태
- 도메인의 상태
- AD 에이전트에 대한 통계

표 14-1 명령 출력에 대한 설명

유형	값	설명
Mode	컨피그레이션 모드	전체 다운로드 또는 온디맨드 다운로드를 지정합니다.
AD Agent IP Address	IP 주소	활성 AD 에이전트 IP 주소를 표시합니다.
Backup	IP 주소	백업 AD 에이전트 IP 주소를 표시합니다.

표 14-1 명령 출력에 대한 설명 (계속)

유형	값	설명
AD Agent Status	• Disabled • Down • Up (registered) • Probing	• ID 방화벽이 비활성화되어 있습니다. • AD 에이전트가 중단되었습니다. • AD 에이전트가 작동 및 실행 중입니다. • ASA가 등록되었으며 AD 에이전트가 작동 및 실행 중입니다. • ASA가 AD 에이전트에 연결하려고 합니다.
Authentication Port	udp/1645	AD 에이전트 인증 포트를 표시합니다.
Accounting Port	udp/1646	AD 에이전트 계정 관리 포트를 표시합니다.
ASA Listening Port	udp/3799	ASA 수신 대기 포트를 표시합니다.
Interface	인터페이스	ASA가 AD 에이전트에 연결하는 데 사용하는 인터페이스를 표시합니다.
IP Address	IP 주소	ASA가 AD 에이전트에 연결하는 데 사용하는 IP 주소를 표시합니다.
Uptime	시간	AD 에이전트 가동 시간을 표시합니다.
Average RTT	밀리초	ASA가 AD 에이전트에 연결하는 데 사용하는 평균 왕복 시간을 표시합니다.
Domain	도메인 별칭 상태: up 상태: down	AD 에이전트의 Microsoft Active Directory 도메인을 표시합니다.

예

다음 예에서는 ID 방화벽의 AD 에이전트에 대한 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity ad-agent
Primary AD Agent:
 Status                    up (registered)
 Mode:                     full-download
 IP address:               172.23.62.125
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  15 mins 41 secs
 Average RTT:              57 msec

Secondary AD Agent:
 Status                    up
 Mode:                     full-download
 IP address:               172.23.62.136
 Authentication port:      udp/1645
 Accounting port:          udp/1646
 ASA Listening port:       udp/3799
 Interface:                mgmt
 Up time:                  7 mins 56 secs
 Avg RTT:                  15 msec
```

관련 명령

명령	설명
clear user-identity ad-agent statistics	ASA에서 유지 관리하는 ID 방화벽의 AD 에이전트에 대한 통계 데이터를 지웁니다.
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.
show user-identity ad-group-members	ID 방화벽의 AD 에이전트 도메인에 있는 그룹 멤버를 표시합니다.

show user-identity ad-group-members

ID 방화벽의 AD 에이전트 도메인에 있는 그룹 멤버를 표시하려면 특권 EXEC 모드에서 **show user-identity ad-group-members** 명령을 사용합니다.

show user-identity ad-group-members [*domain_nickname*\]*user_group_name* [**timeout seconds** *seconds*]

구문 설명

domain_nickname	(선택 사항) ID 방화벽에 대한 도메인 이름을 지정합니다.
timeout seconds *seconds*	(선택 사항) 그룹 멤버 통계 검색을 위한 타이머를 설정하고 타이머의 기간을 지정합니다.
user_group_name	(선택 사항) 통계를 검색할 그룹 이름을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity ad-group-members 명령은 지정된 사용자 그룹의 직접 멤버(사용자 및 그룹)를 표시합니다.

참고 **object-group user** 명령을 사용하여 구성된 ASA에 로컬로 정의된 그룹에 대한 정보는 표시하지 않습니다.

ASA는 Active Directory 서버에 구성된 Active Directory 그룹에 대한 LDAP 쿼리를 전송합니다. 이 명령을 실행하는 것은 지정된 사용자 그룹의 멤버를 확인할 수 있는 LDAP 브라우저 명령을 실행하는 것과 같습니다. ASA는 하나의 LDAP 쿼리 수준을 실행하여 지정된 그룹의 직접 멤버를 distinguishedName 형식으로 검색합니다. 이 명령을 실행해도 가져온 사용자 그룹의 ASA 내부 캐시는 업데이트되지 않습니다.

*domain_nickname*을 지정하지 않으면 ASA에서 기본 도메인에 있는 *user_group_name*을 가진 그룹에 대한 정보를 표시합니다. 인수 *domain_nickname*은 실제 도메인 별칭 또는 LOCAL일 수 있습니다.

그룹 이름은 CN 이름이 아니라 AD 그룹의 고유한 sAMAccountName입니다. 특정 그룹 sAMAccountName에 대한 정보를 표시하려면 **show user-identity ad-groups filter** *filter_string* 명령을 사용하여 해당 그룹의 sAMAccountName을 검색합니다.

예

다음 예에서는 ID 방화벽에 대한 sample1 그룹의 멤버를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity ad-group-member group.sample1
Domain:CSCO        AAA Server Group:  CISCO_AD_SERVER
Group Member List Retrieved Successfully
Number of Members in AD Group group.schiang: 12
dn: CN=user1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
dn: CN=user2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
...
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.
show user-identity ad-groups	ID 방화벽의 AD 에이전트에 대한 정보를 표시합니다.

show user-identity ad-groups

ID 방화벽의 특정 그룹에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show user-identity ad-groups** 명령을 사용합니다.

show user-identity ad-groups *domain_nickname* {**filter** *filter_string* | **import-user-group** [**count**]}

구문 설명

count	(선택 사항) 활성화된 그룹 수를 표시합니다.
domain_nickname	ID 방화벽에 대한 도메인 이름을 지정합니다.
filter *filter_string*	Microsoft Active Directory 도메인 컨트롤러의 CN 특성에 지정된 필터 문자열을 포함하는 그룹을 표시하려면 지정합니다.
import-user-group	ID 방화벽의 활성화된 그룹만 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity ad-groups 명령을 실행하면 ASA에서 Microsoft Active Directory로 LDAP 쿼리를 보내 지정된 도메인 별칭의 일부인 모든 사용자 그룹을 검색합니다. 인수 *domain_nickname*은 실제 도메인 별칭 또는 LOCAL일 수 있습니다. ASA는 group objectclass 특성이 있는 그룹만 검색합니다. ASA는 distinguishedName 형식으로 검색한 그룹을 표시합니다.

filter *filter_string* 키워드 및 인수를 지정하면 ASA에서 도메인 컨트롤러의 CN 특성에 지정된 필터 문자열을 포함하는 그룹을 표시합니다. **access-list** 및 **object-group** 명령은 sAMAccountName만 가져오기 때문에 **show user-identity ad-users filter** *filter_string* 명령을 실행하여 그룹의 sAMAccountName을 검색할 수 있습니다. **filter** *filter_string*을 지정하지 않으면 ASA에서 모든 Active Directory 그룹을 표시합니다.

import-user-group count 키워드를 지정하면 ASA에서 활성화되고(access-group, import-user-group 또는 service-policy 컨피그레이션의 일부이기 때문) 로컬 데이터베이스에 저장된 모든 Active Directory 그룹을 표시합니다. ASA는 그룹의 sAMAccountName만 표시합니다.

예

다음 예에서는 ID 방화벽에 대한 지정된 도메인 별칭의 일부인 사용자 그룹을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity ad-groups CSCO filter sampleuser1
Domain: CSCO        AAA Server Group:       CISCO_AD_SERVER
Group list retrieved successfully
Number of Active Directory Groups       6
dn: CN=group.reg.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.reg.sampleuser1
dn: CN=group.temp.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.temp.sampleuser1
...


ciscoasa# show user-identity ad-groups CSCO import-user-group count
Total AD groups in domain CSCO stored in local: 2


ciscoasa# show user-identity ad-groups CSCO import-user-group
Domain: CSCO
Groups:
        group.SampleGroup1
        group.SampleGroup2
...
```

다음 예에서는 명령을 실행하여 access-list 및 object-group 명령의 결과에 필터 문자열을 적용하는 방법을 보여 줍니다. **show user-identity ad-users CSCO filter SampleGroup1** 명령을 실행하면 지정된 문자열의 sAMAccountName이 표시됩니다.

```
ciscoasa# show user-identity ad-users CSCO filter SampleGroup1
Domain:CSCO    AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 2
dn: CN=SampleUser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: SampleUser2
dn: CN=SAMPLEUSER2-WXP05,OU=Workstations,OU=Cisco Computers,DC=cisco,DC=com
sAMAccountName: SAMPLEUSER2-WXP05$
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity ad-users

ID 방화벽의 Microsoft Active Directory 사용자를 표시하려면 특권 EXEC 모드에서 **show user-identity ad-users** 명령을 사용합니다.

show user-identity ad-users *domain_nickname* [**filter** *filter_string*]

구문 설명

domain_nickname	ID 방화벽에 대한 도메인 이름을 지정합니다.
filter *filter_string*	(선택 사항) Microsoft Active Directory 도메인 컨트롤러의 CN 특성에 지정된 필터 문자열을 포함하는 사용자를 표시하려면 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity ad-users 명령을 실행하면 ASA에서 Microsoft Active Directory로 LDAP 쿼리를 보내 지정된 도메인 별칭의 일부인 모든 사용자를 검색합니다. 인수 *domain_nickname*은 실제 도메인 별칭 또는 LOCAL일 수 있습니다.

filter *filter_string* 키워드 및 인수를 지정하면 ASA에서 도메인 컨트롤러의 CN 특성에 지정된 필터 문자열을 포함하는 사용자를 표시합니다. ASA는 Active Directory 서버에 구성된 Active Directory 그룹에 대한 LDAP 쿼리를 전송합니다.

ASA는 user objectclass 특성이 있고 samAccountType 특성이 805306368인 사용자만 검색합니다. 시스템 개체와 같은 다른 개체는 user objectclass에 포함될 수 있지만 비사용자 개체는 samAccountType 805306368에 의해 필터링됩니다. 필터 문자열을 지정하지 않으면 ASA에서 모든 Active Directory 사용자를 표시합니다.

ASA는 distinguishedName 형식으로 검색한 사용자를 표시합니다.

예

다음 예에서는 ID 방화벽의 Active Directory 사용자에 대한 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity ad-users CSCO filter user
Domain: CSCO        AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 10
dn: CN=sampleuser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser1
dn: CN=sampleuser2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser2
dn: CN=user3,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: user3
...
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity group

ID 방화벽에 대해 구성된 사용자 그룹을 표시하려면 특권 EXEC 모드에서 **show user-identity group** 명령을 사용합니다.

show user-identity group

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니11.5다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity group 명령을 사용하여 ID 방화벽에 대해 구성된 사용자 그룹에 대한 문제 해결 정보를 가져올 수 있습니다. ASA는 Active Directory 서버에 구성된 Active Directory 그룹에 대한 LDAP 쿼리를 전송합니다. 이 명령은 활성화된 사용자 그룹 목록을 다음 형식으로 표시합니다.

domain\group_name

ASA는 보안 정책에 적용된 상위 그룹만 표시합니다. 활성화된 최대 상위 그룹 수는 256개입니다. 그룹은 access-group, import-user-group 또는 service-policy 컨피그레이션의 일부인 경우 활성화됩니다.

예

다음 예에서는 ID 방화벽의 활성화된 그룹을 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity group
Group ID        Activated Group Name (Domain\\Group)
--------        ------------------------------------
       1        LOCAL\\og1
       2        LOCAL\\marketing
       3        CISCO\\group.sampleuser1
       4        IDFW\\grp1
...
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity ip-of-user

ID 방화벽의 지정된 사용자에 대한 IP 주소를 표시하려면 특권 EXEC 모드에서 **show user-identity ip-of-user** 명령을 사용합니다.

show user-identity ip-of-user [*domain_nickname*\]*user-name* [**detail**]

구문 설명

detail	(선택 사항) 사용자 및 IP 주소에 대한 자세한 출력을 표시합니다.
domain_nickname	(선택 사항) ID 방화벽에 대한 도메인 이름을 지정합니다.
user-name	IP 주소를 가져올 사용자를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

이 명령은 지정된 사용자에 대한 사용자 정보 및 IP 주소를 표시합니다. 사용자는 둘 이상의 IP 주소에 연결되어 있을 수 있습니다.

domain_nickname 인수를 지정하지 않으면 ASA에서 기본 도메인에 있는 *user_name*을 가진 사용자에 대한 정보를 표시합니다. 인수 *domain_nickname*은 실제 도메인 별칭 또는 LOCAL일 수 있습니다.

detail 키워드를 지정하면 ASA에서 지정된 사용자의 모든 IP 주소에 대해 총 활성 연결 수, 사용자 통계 기간 및 삭제 수, 일정 기간 동안의 입력 패킷 및 출력 패킷을 표시합니다. **detail** 옵션을 지정하지 않으면 ASA에서 각 IP 주소의 도메인 별칭 및 상태만 표시합니다.

참고 ASA는 ID 방화벽에 대해 사용자 통계 스캔 또는 계정 관리를 활성화한 경우에만 받은 패킷, 보낸 패킷, 지정된 기간 동안 삭제된 패킷 등의 자세한 사용자 통계를 표시합니다. ID 방화벽 컨피그레이션에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.

예

다음 예에서는 ID 방화벽의 지정된 사용자에 대한 IP 주소를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity ip-of-user sampleuser1
CSCO\172.1.1.1 (Login)
CSCO\172.100.3.23 (Login)
CSCO\10.23.51.3 (Inactive)


ciscoasa# show user-identity ip-of-user sampleuser1 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 2 active conns
CSCO\172.100.3.23 (Login) Login time: 20 mins;  Idle time: 10 mins; 10 active conns
CSCO\10.23.51.3 (Inactive) Login time: 3000 mins;  Idle time: 2040 mins; 8 active conns
Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560


ciscoasa# show user-identity ip-of-user sampleuser2
ERROR: no such user


ciscoasa# show user-identity ip-of-user sampleuser3
ERROR: no IP address, user not login now
```

IPv6 support

```
ciscoasa# show user-identity ip-of-user sampleuser4
CSCO\172.1.1.1 (Login)
CSCO\8080:1:3::56 (Login)
CSCO\8080:2:3::34 (Inactive)


ciscoasa# show user-identity ip-of-user sampleuser4 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 8 active conns
CSCO\8080:1:3::56 (Login) Login time: 20 mins;  Idle time: 10 mins; 12 active conns
CSCO\8080:2:3::34 (Inactive) Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.
show user-identity user-of-ip	지정된 IP 주소에 연결된 사용자 정보를 표시합니다.

show user-identity memory

ID 방화벽의 여러 모듈에 대한 메모리를 표시하려면 특권 EXEC 모드에서 **show user-identity memory** 명령을 사용합니다.

show user-identity memory

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

ASA에서 ID 방화벽의 메모리 사용량을 모니터링할 수 있습니다. **show user-identity memory** 명령을 실행하면 사용자 레코드, 그룹 레코드, 호스트 레코드 및 해당 관련 해시 테이블에 대한 메모리가 표시됩니다. ASA는 ID 기반 tmatch 테이블에서 사용하는 메모리도 표시합니다.

이 명령은 ID 방화벽의 여러 모듈에서 사용하는 메모리 사용량을 바이트 단위로 표시합니다.

- 사용자
- 그룹
- 사용자 통계
- LDAP

ASA는 Active Directory 서버에 구성된 Active Directory 그룹에 대한 LDAP 쿼리를 전송합니다. Active Directory 서버는 사용자를 인증하고 사용자 로그온 보안 로그를 생성합니다.

- AD 에이전트
- 기타
- 총 메모리 사용량

AD 에이전트에서 사용자 정보를 검색하도록 ID 방화벽을 구성하는 방법은 이 기능에서 사용하는 메모리 양에 영향을 줍니다. ASA에서 온디맨드 검색을 사용하는지 또는 전체 다운로드 검색을 사용하는지 지정할 수 있습니다. On Demand를 선택하면 받은 패킷의 사용자만 쿼리 및 저장되므로 보다 적은 메모리가 사용됩니다. 이러한 옵션에 대한 설명은 CLI 컨피그레이션 가이드에서 "ID 옵션 구성"을 참고하십시오.

예

다음 예에서 ID 방화벽의 모듈에 대한 메모리 상태를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity memory
Users:       22416048 bytes
Groups:           320 bytes
User stats:         0 bytes
LDAP:             300 bytes
AD agent:         500 bytes
Misc:           32428 bytes
Total:       22449596 bytes
Users:       22416048 bytes
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity statistics

ID 방화벽의 사용자 또는 사용자 그룹에 대한 통계를 표시하려면 특권 EXEC 모드에서 **show user-identity statistics** 명령을 사용합니다.

show user-identity statistics [**user** [*domain_nickname*\]*user_name* | **user-group** [*domain_nickname*\]*user_group_name*]

구문 설명

domain_nickname	(선택 사항) ID 방화벽에 대한 도메인 이름을 지정합니다.
user *user_name*	(선택 사항) 통계를 검색할 사용자 이름을 지정합니다.
user-group *domain_nickname*\ *user_group_name*	(선택 사항) 통계를 검색할 그룹 이름을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity statistics 명령을 실행하여 사용자 또는 사용자 그룹에 대한 통계를 표시할 수 있습니다.

user 키워드와 함께 *domain_nickname* 인수를 지정하지 않으면 ASA에서 기본 도메인에 있는 *user_name*을 가진 사용자에 대한 정보를 표시합니다.

user-group 키워드와 함께 *domain_nickname*을 지정하지 않으면 ASA에서 기본 도메인에 있는 *user_group_name*을 가진 그룹에 대한 정보를 표시합니다. 인수 *domain_nickname*은 실제 도메인 별칭 또는 LOCAL일 수 있습니다.

예

다음 예에서 ID 방화벽의 사용자에 대한 통계를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity statistics user
Current monitored users:11  Total not monitored users:0
                          Average(eps)    Current(eps) Trigger      Total events
User: CSCO\user1 tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:                4              10      14              4861
    1-hour Recv pkts:                 1               10       0               4901
User: CSCO\user2 tot-ses:2456 act-ses:607 fw-drop:0 insp-drop:0 null-ses:2431 bad-acc:0
  20-min Sent attack:                4              10        4              4862
  1-hour Sent pkts:                    0               5         0              2451
...


ciscoasa# show user-identity statistics user user1
Current                           Average(eps)    Current(eps) Trigger      Total events
User: -(user1-) tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:                4              10       14              4861
  1-hour Recv pkts:                 1              10       0               4901
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity statistics top user

ID 방화벽의 상위 10명의 사용자에 대한 통계를 표시하려면 특권 EXEC 모드에서 **show user-identity statistics top user** 명령을 사용합니다.

show user-identity statistics top user

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity statistics top user 명령은 상위 10명의 사용자에 대한 받은 EPS 패킷, 보낸 EPS 패킷 및 받은 공격 통계를 표시합니다. 각 사용자(*domain\user_name*으로 표시)에 대해 ASA는 평균 EPS 패킷, 현재 EPS 패킷, 트리거 및 해당 사용자의 총 이벤트를 표시합니다.

예

다음 예에서는 ID 방화벽의 상위 10명의 사용자에 대한 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity statistics top user
Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv pkts:
01    APAC\sampleuser1
                                  0               0       0               391
  1-hour Sent pkts:
01    APAC\sampleuser2
                                  0               0       0               196
02    CSCO\sampleuser3
                                  0               0       0               195
  10-min Sent attack:
01    CSCO\sampleuser4
                                  0               0       0               352
02    CSCO\sampleuser3
                                  0               0       0               350
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity user active

ID 방화벽의 활성 사용자를 표시하려면 특권 EXEC 모드에서 **show user-identity user active** 명령을 사용합니다.

show user-identity user active [**domain** *domain_nickname* | **user-group** [*domain_nickname*\]*user_group_name* | **user** [*domain_nickname*\]*user_name*] [**list** [**detail**]]

구문 설명

detail	(선택 사항) 활성 사용자 세션의 자세한 출력을 표시합니다.
domain *domain_nickname*	지정된 도메인에 있는 활성 사용자에 대한 통계 자료를 표시합니다.
list	(선택 사항) 활성 사용자 통계를 요약한 목록을 표시합니다.
user *domain_nickname\user_name*	(선택 사항) 지정된 사용자에 대한 통계를 표시합니다.
user-group *domain_nickname\user_group_name*	(선택 사항) 지정된 사용자 그룹에 대한 통계를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

ID 방화벽에서 사용하는 IP-사용자 매핑 데이터베이스에 포함된 모든 사용자에 대한 정보를 표시할 수 있습니다.

show user-identity user active 명령은 사용자에 대한 다음 정보를 표시합니다.

- *domain\user_name*
- 활성 연결
- 유휴 시간(분)

기본 도메인 이름은 실제 도메인 이름, 특정 예약어 또는 LOCAL일 수 있습니다. ID 방화벽은 로컬로 정의된 모든 사용자 그룹 또는 로컬로 정의된 모든 사용자(VPN 또는 웹 포털을 사용하여 로그인 및 인증하는 사용자)에 LOCAL 도메인 이름을 사용합니다. 기본 도메인을 지정하지 않은 경우 LOCAL이 기본 도메인이 됩니다.

사용자의 이름에는 유휴 시간(분)이 추가됩니다. 로그인 시간 및 유휴 시간은 사용자의 IP 주소 대신 사용자별로 저장됩니다.

user-group 키워드를 지정하면 활성화된 사용자 그룹만 표시됩니다. 그룹은 access-group, import-user-group 또는 service-policy 컨피그레이션의 일부인 경우 활성화됩니다.

user-group 키워드와 함께 *domain_nickname*을 지정하지 않으면 ASA에서 기본 도메인에 있는 *user_group_name*을 가진 그룹에 대한 정보를 표시합니다.

참고 **user-identity action domain-controller-down** 명령이 **disable-user-identity-rule** 키워드와 함께 구성된 경우 지정된 도메인이 중단되거나, **user-identity action ad-agent-down** 명령이 **disable-user-identity-rule** 키워드와 함께 구성된 경우 AD 에이전트가 중단되면 로그온된 모든 사용자가 사용자 통계에 비활성화된 것으로 표시됩니다.

참고 ASA는 ID 방화벽에 대해 사용자 통계 스캔 또는 계정 관리를 활성화한 경우에만 받은 패킷, 보낸 패킷, 지정된 기간 동안 삭제된 패킷 등의 자세한 사용자 통계를 표시합니다. ID 방화벽 컨피그레이션에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.

예

다음 예에서는 ID 방화벽의 활성 사용자에 대한 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity user active
Total active users: 30  Total IP addresses: 35
  LOCAL: 0 users, 0 IP addresses
  cisco.com: 0 users, 0 IP addresses
  d1: 0 users, 0 IP addresses
  IDFW: 0 users, 0 IP addresses
  idfw.com: 0 users, 0 IP addresses
  IDFWTEST: 30 users, 35 IP addresses


ciscoasa# show user-identity user active domain CSCO
Total active users: 48020 Total IP addresses:10000
  CSCO: 48020 users, 10000 IP addresses


ciscoasa# show user-identity user active domain CSCO list
Total active users: 48020 Total IP addresses: 10000
  CSCO: 48020 users, 10000 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 5 mins
   CSCO\member-2: 20 active conns; idle 20 mins
   CSCO\member-3: 3 active conns; idle 101 mins
   …


ciscoasa# show user-identity user active list
Total active users: 48032  Total IP addresses: 10000
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 6 mins
   APAC\sampleuser2: 20 active conns; idle 0 mins
   CSCO\member-2: 20 active conns; idle 1 mins
```

```
   CSCO\member-3: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 22 mins
   CSCO\member-4: 3 active conns; idle 101 mins
   …
ciscoasa# show user-identity user active list detail
Total active users: 48032 Total IP addresses: 10010
  CSCO: 48020 users, 10000 IP addresses
  APAC: 12 users, 10 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
     172.1.1.1: login 360 mins, idle 0 mins, 15 active conns
     172.100.3.23: login 200 min, idle 15 mins , 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
   CSCO\member-1: 4 active connections;  idle 350 mins
   …
  APAC\sampleuser12: 3 active conns; idle 101 mins
     172.1.1.1: login 360 mins, idle 101 mins, 1 active conns
     172.100.3.23: login 200 min, idle 150 mins, 2 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560


ciscoasa# show user-identity user active list detail
Total users: 25  Total IP addresses: 5
   LOCAL\idfw: 0 active conns
    6.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
    20.0.0.3: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser4: 0 active conns; idle 0 mins
    20.0.0.2: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser5: 0 active conns
  ...


ciscoasa# show user-identity user active user sampleuser1 list detail
CSCO\sampleuser1: 20 active conns; idle 3 mins
     172.1.1.1: login 360 mins, idle 20 mins, 15 active conns
     172.100.3.23: login 200 mins, idle 3 mins, 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560


ciscoasa# show user-identity user active user APAC\sampleuser2
APAC\sampleuser2: 20 active conns; idle 2 mins


ciscoasa# show user-identity user active user-group APAC\\marketing list

   APAC\sampleuser1: 20 active conns; idle 2 mins
   APAC\member-1: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 0 mins
   APAC\member-3: 20 active conns; idle 6 mins
...

ciscoasa# show user-identity user active user-group APAC\\inactive list
ERROR: group is not activated
```

관련 명령

명령	설명
clear user-identity active-user-database	ID 방화벽의 지정된 사용자, 지정된 사용자 그룹에 속한 모든 사용자 또는 로그아웃된 모든 사용자에 대한 상태를 설정합니다.
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity user all

ID 방화벽의 사용자에 대한 통계를 표시하려면 특권 EXEC 모드에서 **show user-identity user all** 명령을 사용합니다.

show user-identity user all [**list**] [**detail**]

구문 설명

detail	(선택 사항) ID 방화벽의 모든 사용자에 대한 자세한 출력을 표시합니다.
list	(선택 사항) ID 방화벽의 모든 사용자에 대한 통계를 요약한 목록을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity all 명령을 사용하여 ID 방화벽에서 사용하는 IP-사용자 매핑 데이터베이스에 포함된 모든 사용자에 대한 정보를 표시할 수 있습니다.

이 명령에 detail 키워드를 포함한 경우 명령 출력에 IP 주소가 활성 상태로 표시되면 해당 IP 주소는 사용자와 연결되지 않은 것입니다. 따라서 이 IP 주소와 연결된 사용자를 검색하면 오류가 반환됩니다.

참고 **user-identity action domain-controller-down** 명령이 **disable-user-identity-rule** 키워드와 함께 구성된 경우 지정된 도메인이 중단되거나, **user-identity action ad-agent-down** 명령이 **disable-user-identity-rule** 키워드와 함께 구성된 경우 AD 에이전트가 중단되면 로그온된 모든 사용자가 사용자 통계에 비활성화된 것으로 표시됩니다.

참고 ASA는 ID 방화벽에 대해 사용자 통계 스캔 또는 계정 관리를 활성화한 경우에만 받은 패킷, 보낸 패킷, 지정된 기간 동안 삭제된 패킷 등의 자세한 사용자 통계를 표시합니다. ID 방화벽 컨피그레이션에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.

예

다음 예에서는 ID 방화벽의 모든 사용자에 대한 통계를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity user all list
Total inactive users: 1201  Total IP addresses: 100


ciscoasa# show user-identity user all list
Total users: 7
  LOCAL\idfw: 0 active conns
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
  cisco.com\sampleuser4: 0 active conns; idle 300 mins
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
  cisco.com\sampleuser7: 0 active conns


ciscoasa# show user-identity user all list detail
Total users: 7 Total IP addresses: 3
  LOCAL\idfw: 0 active conns
    10.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns; idle 300 mins
    171.69.42.8: inactive
    10.0.0.2: login 300 mins, idle 300 mins, 5 active conns
  cisco.com\sampleuser4: 0 active conns
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity user inactive

ID 방화벽의 비활성 사용자에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show user-identity user inactive** 명령을 사용합니다.

show user-identity user inactive [**domain** *domain_nickname* | **user-group** [*domain_nickname*\]*user_group_name*]

구문 설명

domain *domain_nickname*	(선택 사항) ID 방화벽의 지정된 도메인 이름에 있는 비활성 사용자에 대한 통계를 표시합니다.
user-group *domain_nickname*\ *user_group_name*	(선택 사항) 지정된 사용자 그룹의 비활성 사용자에 대한 통계를 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity user inactive 명령을 사용하여 **user-identity inactive-user-timer** 명령으로 구성된 값보다 더 오랜 기간 동안 활성 트래픽이 없는 사용자에 대한 정보를 표시할 수 있습니다.

user-group 키워드를 지정하면 활성화된 사용자 그룹만 표시됩니다. 그룹은 access-group, import-user-group 또는 service-policy 컨피그레이션의 일부인 경우 활성화됩니다.

user-group 키워드와 함께 *domain_nickname*을 지정하지 않으면 ASA에서 기본 도메인에 있는 *user_group_name*을 가진 그룹에 대한 정보를 표시합니다. 인수 *domain_nickname*은 실제 도메인 별칭 또는 LOCAL일 수 있습니다.

예

다음 예에서 ID 방화벽의 비활성 사용자에 대한 상태를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity user inactive
Total inactive users: 1201
   APAC\sampleuser1
   CSCO\sampleuser2
172.1.1.1: inactive     …
...

ciscoasa# show user-identity user inactive domain CSCO
Total inactive users: 1101
    CSCO: 1101
   CSCO\sampleuser1
   CSCO\sampleuser2
   CSCO\sampleuser3
...


ciscoasa# show user-identity user inactive user-group CSCO\\marketing
Total inactive users: 21
   CSCO\sampleuser1
   CSCO\sampleuser2
...
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.
user-identity inactive-user-timer	사용자가 Cisco ID 방화벽 인스턴스에서 유휴 상태로 간주되기 전의 기간을 지정합니다.

show user-identity user-not-found

ID 방화벽의 Active Directory에 없는 사용자에 대한 IP 주소를 표시하려면 특권 EXEC 모드에서 **show user-identity user-not-found** 명령을 사용합니다.

show user-identity user-not-found

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity user-not-found 명령을 사용하여 Microsoft Active Directory에 없는 사용자의 IP 주소를 표시할 수 있습니다.

ASA는 이러한 IP 주소의 로컬 user-not-found 데이터베이스를 유지 관리합니다. 그러나 전체 목록이 아니라 user-not-found 목록의 마지막 1024개 패킷(동일한 소스 IP 주소의 연속 패킷은 하나의 패킷으로 간주됨)만 데이터베이스에 유지됩니다.

예

다음 예에서는 ID 방화벽의 not-found 사용자에 대한 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
…
```

관련 명령

명령	설명
clear user-identity user-not-found	ID 방화벽의 ASA 로컬 user-not-found 데이터베이스를 지웁니다.
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.
user-identity user-not-found	ID 방화벽에 대한 user-not-found 추적을 활성화합니다.

show user-identity user-of-group

ID 방화벽의 지정된 사용자 그룹에 속한 사용자를 표시하려면 특권 EXEC 모드에서 **show user-identity user-of-group** 명령을 사용합니다.

show user-identity user-of-group [*domain_nickname*\]*user_group_name*

구문 설명

domain_nickname	ID 방화벽에 대한 도메인 이름을 지정합니다.
user_group_name	통계를 표시할 사용자 그룹을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity user-of-group 명령을 사용하여 해당 그룹 ID가 지정된 사용자 그룹과 일치하는 사용자를 표시할 수 있습니다. ASA는 Active Directory로 LDAP 쿼리를 보내지 않고 IP-사용자 해시 목록에서 이 정보를 검색합니다. AD 에이전트는 사용자 ID와 IP 주소 매핑의 캐시를 유지하며 ASA에 변경 사항을 알려 줍니다.

지정한 사용자 그룹 이름은 활성화되어 있어야 합니다. 즉, 그룹이 가져오기 사용자 그룹(액세스 목록 또는 서비스 정책 컨피그레이션에서 사용자 그룹으로 정의됨) 또는 로컬 사용자 그룹(object-group user에서 정의됨)이어야 합니다.

그룹에는 둘 이상의 사용자 멤버가 있을 수 있습니다. 사용자 그룹의 멤버는 모두 지정된 그룹의 직접 멤버(사용자 및 그룹 포함)입니다.

user_group_name 인수와 함께 *domain_nickname*을 지정하지 않으면 ASA에서 기본 도메인에 있는 *user_group_name*을 가진 그룹에 대한 정보를 표시합니다. 인수 *domain_nickname*은 실제 도메인 별칭 또는 LOCAL일 수 있습니다.

명령 출력에 사용자의 상태가 비활성으로 나타나는 경우에는 사용자가 로그아웃했거나 로그인한 적이 없을 수 있습니다.

예

다음 예에서는 ID 방화벽의 지정된 사용자 그룹에 속한 사용자를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity user-of-group group.samplegroup1
Group: CSCO\\group.user1 Total users: 13
CSCO\user2 10.0.0.10(Login) 20.0.0.10(Inactive) …
CSCO\user3 10.0.0.11(Inactive)
CSCO\user4 10.0.0.12 (Login)
CSCO\user5 10.0.0.13 (Login)
CSCO\user6 10.0.0.14 (Inactive)
....


ciscoasa# show user-identity user-of-group group.local1
Group: LOCAL\\group.local1    Total users: 2
CSCO\user1 10.0.4.12 (Login)
LOCAL\user2 10.0.3.13 (Login)
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show user-identity user-of-ip

특정 IP 주소를 가진 ID 방화벽 사용자에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show user-identity user-of-ip** 명령을 사용합니다.

show user-identity user-of-ip *ip_address* [**detail**]

구문 설명

detail	(선택 사항) 지정된 IP 주소를 가진 사용자에 대한 자세한 출력을 표시합니다.
ip_address	정보를 표시할 사용자의 IP 주소를 나타냅니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령이 도입되었습니다.

사용 지침

show user-identity user-of-ip 명령을 사용하여 지정된 IP 주소와 연결된 사용자 정보를 표시할 수 있습니다.

detail 키워드를 지정하면 ASA에서 사용자 로그인 시간, 유휴 시간, 활성 연결 수, 사용자 통계 기간 및 삭제 수, 해당 기간 동안의 입력 패킷 및 출력 패킷을 표시합니다. **detail** 키워드를 지정하지 않으면 ASA에서 도메인 별칭, 사용자 이름 및 상태만 표시합니다.

사용자 상태가 비활성인 경우에는 사용자가 로그아웃했거나 로그인한 적이 없을 수 있습니다.

이 명령에 **detail** 키워드를 포함한 경우 IP 주소에 대한 명령 출력에 오류가 표시되면 IP 주소가 비활성 상태, 즉 IP 주소가 사용자와 연결되어 있지 않음을 나타냅니다.

참고 ASA는 ID 방화벽에 대해 사용자 통계 스캔 또는 계정 관리를 활성화한 경우에만 받은 패킷, 보낸 패킷, 지정된 기간 동안 삭제된 패킷 등의 자세한 사용자 통계를 표시합니다. ID 방화벽 컨피그레이션에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.

예

다음 예에서는 ID 방화벽의 활성 사용자에 대한 상태를 표시하는 방법을 보여 줍니다.

```
ciscoasa# show user-identity user-of-ip 172.1.1.1
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 172.1.1.1 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 172.1.2.2 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 172.1.7.7
ERROR: no user with this IP address
```

IPv6 Support

```
ciscoasa# show user-identity user-of-ip 8080:1:1::4
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 8080:1:1::4 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60


ciscoasa# show user-identity user-of-ip 8080:1:1::6 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60

ciscoasa# show user-identity user-of-ip 8080:1:1::100
ERROR: no user with this IP address
```

관련 명령

명령	설명
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

show version

소프트웨어 버전, 하드웨어 컨피그레이션, 라이센스 키 및 가동 시간 데이터를 표시하려면 사용자 EXEC 모드에서 **show version** 명령을 사용합니다.

show version

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.2(1)	상태 저장 대체작동 모드에서는 클러스터 가동 시간을 나타내는 추가 줄이 표시됩니다.
8.3(1)	이제 출력에 기능에서 영구 키를 사용할지 또는 시간 기반 키를 사용할지 여부 및 사용 중인 시간 기반 키의 기간이 포함됩니다.
8.4(1)	NPE(No Payload Encryption: 페이로드 암호화 없음) 모델에 대한 지원이 추가되었습니다.
9.3(2)	REST API 에이전트가 활성화된 경우 해당 버전 번호가 표시됩니다.

사용 지침

show version 명령을 사용하면 소프트웨어 버전, 마지막으로 재부팅된 이후의 작동 시간, 프로세서 유형, 플래시 파티션 유형, 인터페이스 보드, 일련 번호(BIOS ID), 액티베이션 키 값, 라이센스 유형, 컨피그레이션이 마지막으로 수정된 시간에 대한 타임스탬프 등을 표시할 수 있습니다.

REST API 에이전트가 설치되고 활성화된 경우에는 해당 버전 번호도 표시됩니다.

show version 명령을 통해 나열되는 일련 번호는 플래시 파티션 BIOS의 일련 번호입니다. 이는 섀시의 일련 번호와 다릅니다. 소프트웨어 업그레이드를 받을 때는 섀시 번호가 아니라 **show version** 명령에 표시된 일련 번호가 필요합니다.

대체작동 클러스터 가동 시간 값은 대체작동 집합이 실행된 기간을 나타냅니다. 하나의 디바이스가 실행이 중지된 경우 활성 디바이스가 계속 작동하는 한 가동 시간 값은 계속 증가합니다. 따라서 대체작동 클러스터 가동 시간은 개별 디바이스의 가동 시간보다 클 수 있습니다. 대체작동을 일시적으로 비활성화했다가 다시 활성화한 경우 대체작동 클러스터 가동 시간에는 대체작동이 비활성화되기 전에 디바이스가 가동된 시간과 대체작동이 비활성화되어 있는 동안 디바이스가 가동된 시간이 합산된 값이 보고됩니다.

No Payload Encryption 모델이 있는 경우에는 라이센스를 볼 때 VPN 및 유니파이드 커뮤니케이션 라이센스가 나열되지 않습니다.

ASA 5505에 대한 총 VPN 피어 수의 경우 모든 유형의 총 통합 VPN 세션 수는 라이센스에 따라 달라집니다. AnyConnect Essentials를 사용하는 경우 총 세션 수는 모델의 최대값인 25입니다. AnyConnect Premium을 사용하는 경우 총 세션 수는 AnyConnect Premium 값과 Other VPN 값을 더한 값이지만 25개 세션을 초과할 수 없습니다. Other VPN 값이 모든 VPN 세션에 대한 모델 제한과 동일한 다른 모델과 달리, ASA 5505는 Other VPN 값이 모델 제한보다 낮으므로 총 값은 AnyConnect Premium 라이센스에 따라 다를 수 있습니다.

예

다음은 소프트웨어 버전, 하드웨어 컨피그레이션, 라이센스 키 및 관련 가동 시간 정보를 표시하는 **show version** 명령의 샘플 출력입니다. 상태 저장 대체작동이 구성된 환경에서는 대체작동 클러스터 가동 시간을 나타내는 추가 줄이 표시됩니다. 대체작동이 구성되어 있지 않으면 이 줄이 표시되지 않습니다. 다음 화면에서는 최소 메모리 필요 조건에 대한 경고 메시지를 보여 줍니다.

```
**************************************************************************
**                                                                      **
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***    **
**                                                                      **
**          ----> Minimum Memory Requirements NOT Met! <----            **
**                                                                      **
**  Installed RAM:  512 MB                                              **
**  Required  RAM: 2048 MB                                              **
**  Upgrade part#: ASA5520-MEM-2GB=                                     **
**                                                                      **
**  This ASA does not meet the minimum memory requirements needed to    **
**  run this image. Please install additional memory (part number       **
**  listed above) or downgrade to ASA version 8.2 or earlier.           **
**  Continuing to run without a memory upgrade is unsupported, and      **
**  critical system features will not function properly.                **
**                                                                      **
**************************************************************************

Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)

Compiled on Thu 20-Jan-12 04:05 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/tomm_backup.cfg"

asa3 up 3 days 3 hours

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 128MB
BIOS Flash AT49LW080 @ 0xfff00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.06
 0: Ext: GigabitEthernet0/0  : address is 0013.c480.82ce, irq 9
 1: Ext: GigabitEthernet0/1  : address is 0013.c480.82cf, irq 9
 2: Ext: GigabitEthernet0/2  : address is 0013.c480.82d0, irq 9
 3: Ext: GigabitEthernet0/3  : address is 0013.c480.82d1, irq 9
 4: Ext: Management0/0       : address is 0013.c480.82cd, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5
```

```
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.
The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days

Serial Number: JMX0938K0C0
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Configuration register is 0x1
Configuration last modified by docs at 15:23:22.339 EDT Fri Oct 30 2012
```

다음 메시지는 **eject** 명령을 실행한 후 **show version** 명령을 입력했지만 디바이스가 물리적으로 제거되지 않은 경우에 표시됩니다.

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

관련 명령

명령	설명
eject	외부 Compact Flash 디바이스를 ASA에서 물리적으로 제거하기 전에 종료할 수 있도록 합니다.
show hardware	자세한 하드웨어 정보를 표시합니다.
show serial	하드웨어 일련 정보를 표시합니다.
show uptime	ASA가 가동된 기간을 표시합니다.

show vlan

ASA에 구성된 모든 VLAN을 표시하려면 특권 EXEC 모드에서 **show vlan** 명령을 사용합니다.

show vlan

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예에서는 구성된 VLAN을 표시합니다.

```
ciscoasa# show vlan
10-11,30,40,300
```

관련 명령

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show vm

ASAv의 가상 플랫폼 정보를 표시하려면 특권 EXEC 모드에서 **show vm** 명령을 사용합니다.

show vm

구문 설명

이 명령에는 키워드 또는 인수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

ASAv의 경우 다음 라이센싱 지침에 유의하십시오.

- 허용되는 vCPU 수는 설치된 vCPU 플랫폼 라이센스에 따라 결정됩니다.
  - 라이센스가 있는 vCPU 수가 프로비전된 vCPU 수와 일치하는 경우에는 상태가 Compliant입니다.
  - 라이센스가 있는 vCPU 수가 프로비전된 vCPU 수보다 적은 경우에는 상태가 Noncompliant: Over-provisioned입니다.
  - 라이센스가 있는 vCPU 수가 프로비전된 vCPU 수보다 많은 경우에는 상태가 Compliant: Under-provisioned입니다.
- 메모리 제한은 프로비전된 vCPU 수에 따라 결정됩니다.
  - 프로비전된 메모리가 허용 한도에 도달한 경우에는 상태가 Compliant입니다.
  - 프로비전된 메모리가 허용 한도를 초과한 경우에는 상태가 Noncompliant: Over-provisioned입니다.
  - 프로비전된 메모리가 허용 한도에 미달하는 경우에는 상태가 Compliant: Under-provisioned입니다.
- 주파수 예약 제한은 프로비전된 vCPU 수에 따라 결정됩니다.
  - 주파수 예약 메모리가 필수 최소값(1000MHz)이거나 이를 초과하는 경우에는 상태가 Compliant입니다.
  - 주파수 예약 메모리가 필수 최소값(1000MHz)에 미달하는 경우에는 상태가 Under-provisioned입니다.

예를 들어 적용된 라이센스가 없는 경우 다음 출력이 표시됩니다. 허용되는 vCPU 수는 라이센스가 있는 수를 의미하며, Noncompliant: Over-provisioned는 제품이 라이센스보다 더 많은 리소스로 실행되고 있음을 나타냅니다.

```
Virtual platform CPU resources
------------------------------
Number of vCPUs              :        1
Number of allowed vCPUs      :        0
vCPU Status                  :        Noncompliant: Over-provisioned
```

예

다음 예에서는 가상 플랫폼 정보를 표시합니다.

```
ciscoasa# show vm

Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     4
Processor Memory             :  8192 MB
Minimum Processor Frequency  :  1000 MHz
Maximum Processor Frequency  :  20000 MHz

Virtual Platform Resource Status
--------------------------------
Number of vCPUs                 :     4     (Compliant)
Processor Memory                :  8192 MB  (Compliant)
Processor Frequency Reservation :  1000 MHz (Compliant)
Processor Frequency Limit       :  20000 MHz (Compliant)
Average Usage (30 seconds)      :   103 MHz
```

관련 명령

명령	설명
show cpu detail	vCPU별로 vCPU 정보를 표시합니다.

show vpn load-balancing

VPN 부하 균형 가상 클러스터 컨피그레이션에 대한 런타임 통계를 표시하려면 글로벌 컨피그레이션, 특권 EXEC 또는 VPN 부하 균형 모드에서 **show vpn-load-balancing** 명령을 사용합니다.

show vpn load-balancing

구문 설명

이 명령에는 변수 또는 인수가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—
VPN 부하 균형	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
7.1(1)	출력 예의 Load (%) 표시 및 Session 표시 모두에 대해 별도의 IPsec 및 SSL 열이 추가되었습니다.
8.4(2)	표시되는 출력에 새 정보가 추가되었습니다.

사용 지침

show vpn load-balancing 명령은 가상 VPN 부하 균형 클러스터에 대한 통계 정보를 표시합니다. 로컬 디바이스가 VPN 부하 균형 클러스터에 참여하지 않는 경우 이 명령은 해당 디바이스에 대해 VPN 부하 균형이 구성되지 않았음을 나타냅니다.

출력에서 별표(*)는 연결된 ASA의 IP 주소를 나타냅니다.

예

다음 예에서는 로컬 디바이스가 VPN 부하 균형 클러스터에 참여하는 경우 **show vpn load-balancing** 명령의 출력을 보여 줍니다.

```
ciscoasa# sh vpn load-balancing
------------------------------------------------------------------------------
    Status     Role   Failover   Encryption        Cluster IP   Peers
------------------------------------------------------------------------------
   Enabled   Master        n/a     Disabled 192.0.2.255   0

Peers:
------------------------------------------------------------------------------
       Public IP     Role  Pri             Model  Load-Balancing Version
------------------------------------------------------------------------------
        192.0.2.255    Master    5          ASA-5520            3

Total License Load:
------------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials          Other VPN
                    ------------------------------   ---------------------
                         Limit    Used   Load          Limit    Used   Load
------------------------------------------------------------------------------
     192.0.2.255       750       0     0%            750       1     0%

Licenses Used By Inactive Sessions :
------------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials     Inactive Load
------------------------------------------------------------------------------
     192.0.2.255                      0                0%
```

기본 디바이스의 경우에는 Total License Load 출력에 기본 및 백업 디바이스에 대한 정보가 포함되지만, 백업 디바이스의 경우에는 백업 디바이스에 대한 정보만 표시되고 기본 디바이스에 대한 정보는 표시되지 않습니다. 따라서 기본 디바이스는 라이센스가 있는 모든 멤버를 인식하지만 라이센스가 있는 멤버 자체는 자신이 소유한 라이센스만 알고 있습니다.

출력에는 License Used by Inactive Session 섹션도 포함됩니다. AnyConnect 세션이 비활성 상태가 되면 ASA는 세션이 정상적으로 종료되지 않은 한 해당 세션을 유지합니다. 따라서 다시 인증할 필요 없이 동일한 webvpn 쿠키를 사용하여 AnyConnect 세션을 다시 연결할 수 있습니다. 비활성 세션은 AnyConnect 클라이언트가 세션을 다시 시작하거나 유휴 시간 제한이 발생할 때까지 이 상태로 그대로 유지됩니다. 해당 세션에 대한 라이센스는 이러한 비활성 세션에 대해 유지되며, 이 License Used by Inactive Session 섹션에 표시됩니다.

로컬 디바이스가 VPN 부하 균형 클러스터에 참여하지 않는 경우에는 **show vpn load-balancing** 명령에 다른 결과가 표시됩니다.

```
ciscoasa(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

관련 명령

명령	설명
clear configure vpn load-balancing	컨피그레이션에서 **vpn load-balancing** 명령문을 제거합니다.
show running-config vpn load-balancing	현재 VPN 부하 균형 가상 클러스터 컨피그레이션을 표시합니다.
vpn load-balancing	VPN 부하 균형 모드를 시작합니다.

show vpn-sessiondb

VPN 세션에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show vpn-sessiondb** 명령을 사용합니다. 이 명령은 전체 정보 또는 자세한 정보를 표시하는 옵션을 포함하며, 표시할 세션 유형을 지정할 수 있도록 하고, 정보를 필터링 및 정렬할 수 있는 옵션을 제공합니다. 그에 따라 구문 테이블 및 사용 참고 선택 항목이 구성됩니다.

show vpn-sessiondb [**detail**] [**ospfv3**] [**failover**] [**full**] [**summary**] [**ratio** {**encryption** | **protocol**}] [**license-summary**] {**anyconnect** | **email-proxy** | **index** *indexnumber* | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **vpn-lb** | **webvpn**} [**filter** {**name** username | **ipaddress** *IPaddr* | **a-ipaddress** *IPaddr* | **p-ipaddress** *IPaddr* | **tunnel-group** *groupname* | **protocol** *protocol-name* | **encryption** *encryption-algo* | **inactive**}] [**sort** {**name** | **ipaddress** | **a-ipaddress** | **p-ip address** | **tunnel-group** | **protocol** | **encryption** | **inactivity**}]

구문 설명

anyconnect	OSPFv3 세션 정보를 포함하여 AnyConnect VPN 클라이언트 세션을 표시합니다.
detail	(선택 사항) 세션에 대한 확장된 세부 정보를 표시합니다. 예를 들어 IPsec 세션에 **detail** 옵션을 사용하면 IKE 해싱 알고리즘, 인증 모드 및 키 재설정 간격과 같은 추가 세부 정보가 표시됩니다. **detail** 및 **full** 옵션을 선택한 경우 ASA는 컴퓨터에서 판독할 수 있는 형식으로 자세한 출력을 표시합니다.
email-proxy	이메일 프록시 세션을 표시합니다.
encryption	암호화 유형 비율을 총 세션 수의 비율로 표시합니다.
failover	대체작동 IPsec 터널에 대한 세션 정보를 표시합니다.
filter *filter_criteria*	(선택 사항) 하나 이상의 필터 옵션을 사용하여 지정한 정보만 표시하도록 출력을 필터링합니다. *filter_criteria* 옵션 목록은 "사용 지침" 섹션을 참고하십시오.
full	(선택 사항) 스트리밍되고 잘리지 않은 출력을 표시됩니다. 출력은 레코드 사이의 | 문자 및 || 문자열로 구분됩니다.
index *indexnumber*	인덱스 번호별 단일 세션을 표시합니다. 세션에 대한 인덱스 번호(1~750)를 지정합니다.
l2l	VPN LAN-to-LAN 세션 정보를 표시합니다.
license-summary	VPN 라이센스 요약 정보를 표시합니다.
ospfv3	OSPFv3 세션 정보를 표시합니다.
protocol	프로토콜 유형 비율을 총 세션 수의 비율로 표시합니다.
ra-ikev1-ipsec	IPsec IKEv1 세션을 표시합니다.
ra-ikev2-ipsec	IKEv2 원격 액세스 클라이언트 연결에 대한 자세한 정보를 표시합니다.
sort *sort_criteria*	(선택 사항) 지정한 정렬 옵션에 따라 출력을 정렬합니다. *sort_criteria* 옵션 목록은 "사용 지침" 섹션을 참고하십시오.
summary	VPN 세션 요약 정보를 표시합니다.
vpn-lb	VPN 부하 균형 관리 세션을 표시합니다.
webvpn	OSPFv3 세션 정보를 포함하여 클라이언트리스 SSL VPN 세션을 표시합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.
8.0(2)	VLAN 필드 설명이 추가되었습니다.
8.0(5)	**inactive**가 **filter** 옵션으로 추가되고 **inactivity**가 **sort** 옵션으로 추가되었습니다.
8.2(1)	라이센스 정보가 결과에 추가되었습니다.
8.4(1)	**svc** 키워드가 **anyconnect**로 변경되었습니다. **remote** 키워드가 **ra-ikev1-ipsec** 으로 변경되었습니다.**ratio** 키워드가 추가되었습니다.
9.0(1)	**ospfv3** 키워드가 추가되고, 이제 OSPFv3 세션 정보가 VPN 세션 요약에 포함됩니다. IPv4 또는 IPv6 주소가 할당된 모든 AnyConnect, LAN-to-LAN 및 클라이언트리스 SSL VPN 세션에서 필터링할 수 있도록 **fitler a-ipversion** 및 **filter p-ipversion** 옵션이 추가되었습니다.
9.1(2)	대체작동 IPsec 터널을 지원하기 위해 대체작동 터널 유형 및 **failover** 키워드가 추가되었습니다. **failover ipsec pre-shared-key** 명령을 참고하십시오.
9.1(4)	**detail anyconnect** 옵션을 사용할 때의 출력이 할당된 IPv6 주소를 반영하고 IKEv2 이중 트래픽을 수행할 때 GRE Transport Mode 보안 연계를 나타내도록 업데이트되었습니다.
9.3(2)	IKEv2 원격 액세스 클라이언트 연결에 대한 세부 정보를 표시하기 위해 **ra-ikev2-ipsec** 키워드가 추가되었습니다**.** VPN 세션 요약 출력이 IKEv2 원격 액세스 클라이언트 연결과 IKEv2 및 IPsec 터널 수를 포함하도록 업데이트되었습니다. VPN 라이센스 사용 요약 출력이 IKEv2 원격 액세스 클라이언트 연결을 추가하도록 업데이트되었습니다.

사용 지침

다음 옵션을 사용하여 세션 표시를 필터링 및 정렬할 수 있습니다.

Filter/Sort 옵션	설명
filter a-ipaddress *IPaddr*	지정한 할당된 IP 주소에 대한 정보만 표시하도록 출력을 필터링합니다.
sort a-ipaddress	할당된 IP 주소별로 표시를 정렬합니다.
filter a-ipversion {v4 | v6}	IPv4 또는 IPv6 주소가 할당된 모든 AnyConnect 세션에 대한 정보를 표시하도록 출력을 필터링합니다.

Filter/Sort 옵션	설명
filter encryption *encryption-algo*	지정된 암호화 알고리즘을 사용하는 세션에 대한 정보만 표시하도록 출력을 필터링합니다.
sort encryption	암호화 알고리즘별로 표시를 정렬합니다. 암호화 알고리즘에는 aes128, aes192, aes256, des, 3des, rc4 등이 있습니다.
filter inactive	유휴 상태가 되고 연결이 끊어졌을 수 있는(하이버네이션, 모바일 디바이스 연결 해제 등으로 인해) 비활성 세션을 필터링합니다. AnyConnect 클라이언트의 응답 없이 ASA에서 TCP 연결 유지를 전송한 경우 비활성 세션 수가 증가합니다. 각 세션에는 SSL 터널 연결 해제 시간이 포함된 타임스탬프가 지정됩니다. 세션이 SSL 터널을 통해 능동적으로 트래픽을 전달하는 경우에는 00:00m:00s가 표시됩니다. **참고** ASA는 배터리 수명을 절약하기 위해 일부 디바이스(예: iPhone, iPad, 및 iPod)에는 TCP 연결 유지를 전송하지 않으므로 연결 해제와 절전 간에 오류 감지를 구분할 수 없습니다. 이러한 이유로 비활성 카운터는 00:00:00 카운터로 그대로 유지되도록 설계되어 있습니다.
sort inactivity	비활성 세션을 정렬합니다.
filter ipaddress *IPaddr*	지정한 내부 IP 주소에 대한 정보만 표시하도록 출력을 필터링합니다.
sort ipaddress	내부 IP 주소별로 표시를 정렬합니다.
filter name *username* **sort name**	지정된 사용자 이름에 대한 세션을 표시하도록 출력을 필터링합니다. 사용자 이름을 기준으로 사전순으로 표시를 정렬합니다.
filter p-address *IPaddr*	지정한 외부 IP 주소에 대한 정보만 표시하도록 출력을 필터링합니다.
sort p-address	지정한 외부 IP 주소별로 표시를 정렬합니다.
filter p-ipversion {v4 | v6}	IPv4 또는 IPv6 주소가 있는 엔드포인트에서 시작된 AnyConnect 세션에 대한 정보를 표시하도록 출력을 필터링합니다.
filter protocol *protocol-name*	지정된 프로토콜을 사용하는 세션에 대한 정보만 표시하도록 출력을 필터링합니다.
sort protocol	프로토콜별로 표시를 정렬합니다. 프로토콜에는 IKE, IMAP4S, IPsec, IPsecLAN2LAN, IPsecLAN2LANOverNatT, IPsecOverNatT, IPsecoverTCP, IPsecOverUDP, SMTPS, userHTTPS, vcaLAN2LAN 등이 있습니다.
filter tunnel-group *groupname*	지정한 터널 그룹에 대한 정보만 표시하도록 출력을 필터링합니다.
sort tunnel-group	터널 그룹별로 표시를 정렬합니다.
|	{begin | include | exclude | grep | [-v]} {reg_exp} 인수를 사용하여 출력을 수정합니다.

예

다음은 **show vpn-sessiondb** 명령의 샘플 출력입니다.

```
ciscoasa# show vpn-sessiondb

--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------------
AnyConnect Client           :      1 :         78 :           2 :        0
  SSL/TLS/DTLS              :      1 :         72 :           2 :        0
  IKEv2 IPsec               :      0 :          6 :           1 :        0
IKEv2 Generic IPsec Client  :      0 :          0 :           0
Clientless VPN              :      0 :          8 :           2
  Browser                   :      0 :          8 :           2
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     86
Device Total VPN Capacity   :    750
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
IKEv2                       :      0 :          6 :               1
IPsecOverNatT               :      0 :          6 :               1
Clientless                  :      0 :         17 :               2
AnyConnect-Parent           :      1 :         69 :               2
SSL-Tunnel                  :      1 :         75 :               2
DTLS-Tunnel                 :      1 :         56 :               2
--------------------------------------------------------------------------------
Totals                      :      3 :        229
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
AnyConnect SSL/TLS/DTLS     :        :            :
  IPv6 Peer                 :      1 :         41 :           2
  Tunneled IPv6             :      1 :         70 :           2
AnyConnect IKEv2            :        :            :
  IPv6 Peer                 :      0 :          4 :           1
Clientless                  :        :            :
  IPv6 Peer                 :      0 :          1 :           1
--------------------------------------------------------------------------------
```

다음은 LAN-to-LAN 세션에 대한 자세한 정보를 보여 주는 **show vpn-sessiondb detail l2l** 명령의 샘플 출력입니다.

```
ciscoasa# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection   : 172.16.0.0
Index        : 1
IP Addr      : 172.16.0.0
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 240                   Bytes Rx     : 160
```

```
Login Time   : 14:50:35 UTC Tue May 1 2012
Duration     : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 1.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86389 Seconds
  PRF          : SHA1                   D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :

IPsec:
  Tunnel ID    : 1.2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel                 PFS Group    : 5
  Rekey Int (T): 120 Seconds            Rekey Left(T): 107 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 240                    Bytes Rx     : 160
  Pkts Tx      : 3                      Pkts Rx      : 2

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 13 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

다음은 **show vpn-sessiondb detail index 1** 명령의 샘플 출력입니다.

```
AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : user1
Index        : 1
Assigned IP  : 192.168.2.70           Public IP    : 10.86.5.114
Protocol     : IPsec                  Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                      Bytes Rx     : 604533
Client Type  : WinNT                  Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeysXauth
```

```
  Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 61078 Seconds
  D/H Group    : 2

IPsec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                     Bytes Rx     : 604533
  Pkts Tx      : 0                     Pkts Rx      : 8126

NAC:
  Reval Int (T): 3000 Seconds          Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds           EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds             Posture Token: Healthy
  Redirect URL : www.cisco.com
```

다음은 **show vpn-sessiondb ospfv3** 명령의 샘플 출력입니다.

```
asa# show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection   :
Index        : 1                     IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none        Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                     Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:13m:11s
```

다음은 **show vpn-sessiondb detail ospfv3** 명령의 샘플 출력입니다.

```
asa# show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection   :
Index        : 1                     IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none        Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                     Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
  Tunnel ID    : 1.1
  Local Addr   : ::/0/89/0
  Remote Addr  : ::/0/89/0
  Encryption   : none                  Hashing      : SHA1
  Encapsulation: Transport
  Idle Time Out: 0 Minutes             Idle TO Left : 0 Minutes
  Bytes Tx     : 0                     Bytes Rx     : 0
  Pkts Tx      : 0                     Pkts Rx      : 0

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 105268 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

다음은 **show vpn-sessiondb summary** 명령의 샘플 출력입니다.

```
ciscoasa# show vpn-sessiondb summary
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------
OSPFv3 IPsec                :      1 :          1 :           1
----------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :      1
Device Total VPN Capacity   :  10000
Device Load                 :     0%
----------------------------------------------------------------------
```

다음은 일반 IKEv2 IPsec 원격 액세스 세션에 대한 **show vpn-sessiondb summary** 명령의 샘플 출력입니다.

```
ciscoasa# show vpn-sessiondb summary
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------
Generic IKEv2 Remote Access :      1 :          1 :           1
----------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :      1
Device Total VPN Capacity   :    250
Device Load                 :     0%
----------------------------------------------------------------------------

----------------------------------------------------------------------------
Tunnels Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------
IKEv2                       :      1 :          1 :               1
IPsec                       :      1 :          1 :               1
----------------------------------------------------------------------------
Totals                      :      2 :          2
----------------------------------------------------------------------------
```

다음은 **show vpn-sessiondb det anyconnect** 명령의 샘플 출력입니다.

```
ciscoasa# show vpn-sessiondb det anyconnect

Session Type: AnyConnect Detailed

Username     : userab                 Index        : 2
Assigned IP  : 65.2.1.100             Public IP    : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : IKEv2: (1)3DES  IPsecOverNatT: (1)3DES  AnyConnect-Parent: (1)none
Hashing      : IKEv2: (1)SHA1  IPsecOverNatT: (1)SHA1  AnyConnect-Parent: (1)none
Bytes Tx     : 0                      Bytes Rx     : 21248
Pkts Tx      : 0                      Pkts Rx      : 238
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : test1
Login Time   : 22:44:59 EST Tue Aug 13 2013
Duration     : 0h:02m:42s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
```

```
VLAN Mapping : N/A                    VLAN         : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 75.2.1.60
  Encryption   : none                   Hashing      : none
  Auth Mode    : userPassword
  Idle Time Out: 400 Minutes            Idle TO Left : 397 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Client OS    : Windows
  Client Type  : AnyConnect
  Client Ver   : 3.1.05050

IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 64251                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : 3DES                   Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86241 Seconds
  PRF          : SHA1                   D/H Group    : 2
  Filter Name  : mixed1
  Client OS    : Windows

IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 75.2.1.23/255.255.255.255/47/0
  Remote Addr  : 75.2.1.60/255.255.255.255/47/0
  Encryption   : 3DES                   Hashing      : SHA1
  Encapsulation: Transport, GRE
  Rekey Int (T): 28400 Seconds          Rekey Left(T): 28241 Seconds
  Idle Time Out: 400 Minutes            Idle TO Left : 400 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 21326
  Pkts Tx      : 0                      Pkts Rx      : 239

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 165 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

다음 예는 **show vpn-sessiondb ra-ikev2-ipsec** 명령의 샘플 출력입니다.

```
ciscoasa(config)# show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username     : IKEV2TG               Index        : 1
Assigned IP  : 95.0.225.200          Public IP    : 85.0.224.12
Protocol     : IKEv2 IPsec
License      : AnyConnect Essentials
Encryption   : IKEv2: (1)3DES  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 0                     Bytes Rx     : 17844
Pkts Tx      : 0                     Pkts Rx      : 230
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG   Tunnel Group : IKEV2TG
Login Time   : 11:39:54 UTC Tue May 6 2014
Duration     : 0h:03m:17s
```

```
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

다음은 **show vpn-sessiondb license-summary** 명령의 샘플 출력입니다.

```
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                  Status : Capacity : Installed :  Limit
                                 ----------------------------------------
AnyConnect Premium               : DISABLED :      250 :        10 :   NONE
AnyConnect Essentials            :  ENABLED :      250 :       250 :   NONE
Other VPN (Available by Default) :  ENABLED :      250 :       250 :   NONE
Shared License Server            : DISABLED
Shared License Participant       : DISABLED
AnyConnect for Mobile            : DISABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     : DISABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   : DISABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
                        Local : Shared :   All  :   Peak :  Eff.  :
                       In Use : In Use : In Use : In Use :  Limit : Usage
                      ---------------------------------------------------
AnyConnect Essentials  :     1 :      0 :      1 :      1 :    250 :    0%
  AnyConnect Client    :                :      0 :      0          :    0%
    AnyConnect Mobile  :                :      0 :      0          :    0%
  Generic IKEv2 Client :                :      1 :      1          :    0%
Other VPN              :                :      0 :      0 :    250 :    0%
  Cisco VPN Client     :                :      0 :      0          :    0%

----------------------------------------------------------------------------
Shared License Network Summary
----------------------------------------------------------------------------
AnyConnect Premium
  Total shared licenses in network                                  : 500
  Shared licenses held by this participant                          :  0
  Shared licenses held by all participants in the network           :  0
----------------------------------------------------------------------------
```

위 예와 같이 **show vpn-sessiondb** 명령에 대한 응답에 표시되는 필드는 입력한 키워드에 따라 다릅니다. 표 14-2에는 이러한 필드에 대한 설명이 나와 있습니다.

표 14-2 show vpn-sessiondb Command 필드

필드	설명
Auth Mode	이 세션을 인증하는 데 사용된 프로토콜 또는 모드입니다.
Bytes Rx	ASA가 원격 피어 또는 클라이언트에서 수신한 총 바이트 수입니다.
Bytes Tx	ASA가 원격 피어 또는 클라이언트로 전송한 바이트 수입니다.
Client Type	원격 피어에서 실행되는 클라이언트 소프트웨어입니다(사용 가능한 경우).

표 14-2 show vpn-sessiondb Command 필드 (계속)

필드	설명
Client Ver	원격 피어에서 실행되는 클라이언트 소프트웨어의 버전입니다.
Connection	연결 또는 사설 IP 주소의 이름입니다.
D/H Group	Diffie-Hellman 그룹입니다. IPsec SA 암호화 키를 생성하는 데 사용된 알고리즘 및 키 크기입니다.
Duration	세션 로그인 시간과 마지막 화면 새로 고침 사이의 경과 시간(HH:MM:SS)입니다.
EAPoUDP Session Age	마지막으로 성공한 상태 검증 이후의 경과 시간(초)입니다.
Encapsulation	IPsec ESP(Encapsulating Security Payload) 프로토콜 암호화 및 인증을 적용하는 데 사용된 모드(즉, ESP를 적용한 원래 IP 패킷의 일부)입니다.
Encryption	이 세션에서 사용하는 데이터 암호화 알고리즘입니다(있는 경우).
EoU Age (T)	EAPoUDP 세션 기간입니다. 마지막으로 성공한 상태 검증 이후의 경과 시간(초)입니다.
Filter Name	세션 정보 표시를 제한하기 위해 지정된 사용자 이름입니다.
Hashing	IPsec 데이터 인증에 사용되는 패킷의 해시를 생성하는 데 사용된 알고리즘입니다.
Hold Left (T)	남은 보류 시간입니다. 마지막 상태 검증에 성공한 경우에는 0초입니다. 그렇지 않으면 다음 상태 검증 시도 시까지 남은 시간(초)입니다.
Hold-Off Time Remaining	마지막 상태 검증에 성공한 경우에는 0초입니다. 그렇지 않으면 다음 상태 검증 시도 시까지 남은 시간(초)입니다.
IKE Neg Mode	키 정보를 교환하고 SA를 설정하는 IKE(IPsec Phase 1) 모드입니다(Aggressive 또는 Main).
IKE Sessions	IKE(IPsec Phase 1) 세션 수입니다(일반적으로 1). 이러한 세션은 IPsec 트래픽에 대한 터널을 설정합니다.
Index	이 레코드의 고유 식별자입니다.
IP Addr	이 세션에서 원격 클라이언트에 할당된 사설 IP 주소입니다. “내부” 또는 “가상” IP 주소라고도 합니다. 클라이언트가 사설 네트워크에서 호스트처럼 보이도록 합니다.
IPsec Sessions	터널을 통과하는 데이터 트래픽 세션인 IPsec(Phase 2) 세션 수입니다. 각 IPsec 원격 액세스 세션에는 두 개의 IPsec 세션, 즉 터널 엔드포인트로 구성된 세션과 터널을 통해 연결할 수 있는 사설 네트워크로 구성된 세션이 있을 수 있습니다.
License Information	공유 SSL VPN 라이센스에 대한 정보를 표시합니다.
Local IP Addr	터널의 로컬 엔드포인트(ASA의 인터페이스)에 할당된 IP 주소입니다.
Login Time	세션에 로그인한 날짜 및 시간(MMM DD HH:MM:SS)입니다. 시간은 24시간 표기법으로 표시됩니다.

표 14-2 show vpn-sessiondb Command 필드 (계속)

필드	설명
NAC Result	NAC(Network Admission Control) 상태 검증의 상태입니다. 다음 중 하나일 수 있습니다. • Accepted - ACS에서 원격 호스트의 상태를 성공적으로 검증했습니다. • Rejected - ACS에서 원격 호스트의 상태를 성공적으로 검증할 수 없습니다. • Exempted - 원격 호스트가 ASA에 구성된 Posture Validation Exception(상태 검증 예외) 목록에 따라 상태 검증에서 제외되었습니다. • Non-Responsive - 원격 호스트가 EAPoUDP Hello 메시지에 응답하지 않았습니다. • Hold-off - 성공적인 상태 검증 후 ASA와 원격 호스트 간의 EAPoUDP 통신이 끊어졌습니다. • N/A - VPN NAC 그룹 정책에 따라 원격 호스트에 대한 NAC가 비활성화되었습니다. • Unknown - 상태 검증이 진행 중입니다.
NAC Sessions	Network Admission Control(EAPoUDP) 세션 수입니다.
Packets Rx	ASA가 원격 피어에서 수신한 패킷 수입니다.
Packets Tx	ASA가 원격 피어로 전송한 패킷 수입니다.
PFS Group	Perfect Forward Secrecy 그룹 번호입니다.
Posture Token	Access Control Server에서 구성할 수 있는 알림 텍스트 문자열입니다. ACS는 시스템 모니터링, 보고, 디버깅 및 로깅에 유용한 정보를 제공하기 위해 ASA로 상태 토큰을 다운로드합니다. 일반적인 상태 토큰은 Healthy, Checkup, Quarantine, Infected 또는 Unknown입니다.
Protocol	세션에서 사용하는 프로토콜입니다.
Public IP	클라이언트에 할당된 공개적으로 라우팅 가능한 IP 주소입니다.
Redirect URL	상태 검증 또는 클라이언트리스 인증 후 ACS는 세션에 대한 액세스 정책을 ASA로 다운로드합니다. 리디렉션 URL은 액세스 정책 페이로드의 선택적 부분입니다. ASA는 원격 호스트에 대한 모든 HTTP(포트 80) 및 HTTPS(포트 443) 요청을 리디렉션 URL(있는 경우)로 리디렉션합니다. 액세스 정책에 리디렉션 URL이 포함되지 않은 경우에는 ASA에서 원격 호스트의 HTTP 및 HTTPS 요청을 리디렉션하지 않습니다. 리디렉션 URL은 IPsec 세션이 종료되거나 상태 재검증이 수행될 때까지 유효한 상태로 유지되며, 그 동안 ACS는 리디렉션 URL을 포함하지 않거나 다른 리디렉션 URL을 포함할 수 있는 새 액세스 정책을 다운로드합니다.
Rekey Int (T)	IPsec(IKE) SA 암호화 키의 수명입니다.
Rekey Left (T)	IPsec(IKE) SA 암호화 키의 남은 수명입니다.
Rekey Time Interval	IPsec(IKE) SA 암호화 키의 수명입니다.
Remote IP Addr	터널의 원격 엔드포인트(원격 피어의 인터페이스)에 할당된 IP 주소입니다.
Reval Int (T)	재검증 시간 간격입니다. 각 성공적인 상태 검증 간에 필요한 간격(초)입니다.
Reval Left (T)	다음 재검증까지의 시간입니다. 마지막 상태 검증 시도에 실패한 경우 0입니다. 그렇지 않으면 Revalidation Time Interval과 마지막으로 상태 검증에 성공한 이후에 경과한 시간(초) 간의 차이입니다.

표 14-2 show vpn-sessiondb Command 필드 (계속)

필드	설명
Revalidation Time Interval	각 성공적인 상태 검증 간에 필요한 간격(초)입니다.
Session ID	세션 구성 요소(하위 세션)의 식별자입니다. 각 SA에는 고유한 식별자가 있습니다.
Session Type	세션의 유형입니다(LAN-to-LAN 또는 Remote).
SQ Int (T)	상태 쿼리 시간 간격입니다. 성공한 각 상태 검증 또는 상태 쿼리 응답과 다음 상태 쿼리 응답 간에 허용되는 시간(초)입니다. 상태 쿼리는 마지막 상태 검증 후 호스트의 상태가 변경되었는지 여부를 나타내기 위해 ASA에서 원격 호스트로 보내는 요청입니다.
Status Query Time Interval	성공한 각 상태 검증 또는 상태 쿼리 응답과 다음 상태 쿼리 응답 간에 허용되는 시간(초)입니다. 상태 쿼리는 마지막 상태 검증 후 호스트의 상태가 변경되었는지 여부를 나타내기 위해 ASA에서 원격 호스트로 보내는 요청입니다.
Time Until Next Revalidation	마지막 상태 검증 시도에 실패한 경우 0입니다. 그렇지 않으면 Revalidation Time Interval과 마지막으로 상태 검증에 성공한 이후에 경과한 시간(초) 간의 차이입니다.
Tunnel Group	이 터널에서 특성 값에 대해 참조한 터널 그룹의 이름입니다.
UDP Dst Port 또는 UDP Destination Port	원격 피어에서 UDP에 사용한 포트 번호입니다.
UDP Src Port 또는 UDP Source Port	ASA에서 UDP에 사용한 포트 번호입니다.
Username	세션을 설정하는 데 사용된 사용자 로그인 이름입니다.
VLAN	이 세션에 할당된 이그레스 VLAN 인터페이스입니다. ASA는 모든 트래픽을 이 VLAN으로 전달합니다. 다음 요소 중 하나에서 값을 지정합니다. • 그룹 정책 • 상속된 그룹 정책

관련 명령

명령	설명
show running-configuration vpn-sessiondb	VPN 세션 데이터베이스에서 실행 중인 구성(max-other-vpn-limit, max-anyconnect-premium-or-essentials-limit)을 표시합니다.
show vpn-sessiondb ratio	VPN 세션 암호화 또는 프로토콜 비율을 표시합니다.

show vpn-sessiondb ratio

현재 세션의 비율을 프로토콜 또는 암호화 알고리즘의 백분율로 표시하려면 특권 EXEC 모드에서 **show vpn-sessiondb ratio** 명령을 사용합니다.

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

구문 설명

encryption	표시할 암호화 프로토콜을 식별합니다. 2단계 암호화를 나타냅니다. 암호화 알고리즘은 다음과 같습니다. aes128 des aes192 3des aes256 rc4
filter *groupname*	지정한 터널 그룹에 대한 세션 비율만 포함하도록 출력을 필터링합니다.
protocol	표시할 프로토콜을 식별합니다. 프로토콜은 다음과 같습니다. IKEv1 L2TPOverIPsecOverNatT IKEv2 Clientless IPSec Port-Forwarding IPsecLAN2LAN IMAP4S IPsecLAN2LANOverNatT POP3S IPsecOverNatT SMTPS IPsecOverTCP AnyConnect-Parent IPsecOverUDP SSL-Tunnel L2TPOverIPsec DTLS-Tunnel

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.4(1)	IKEv2를 포함하도록 출력이 향상되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

예

다음은 **encryption**을 인수로 사용하여 실행한 **show vpn-sessiondb ratio** 명령의 샘플 출력입니다.

```
ciscoasa# show vpn-sessiondb ratio encryption
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions       Percent
none                     0               0%
DES                      1              20%
3DES                     0               0%
AES128                   4        80%
AES192                   0               0%
AES256                   0               0%
```

다음은 **protocol**을 인수로 사용하여 실행한 **show vpn-sessiondb ratio** 명령의 샘플 출력입니다.

```
ciscoasa# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions       Percent
IKE                      0               0%
IPsec                    1              20%
IPsecLAN2LAN             0               0%
IPsecLAN2LANOverNatT     0               0%
IPsecOverNatT            0               0%
IPsecOverTCP             1 20%
IPsecOverUDP             0               0%
L2TP                     0               0%
L2TPOverIPsec            0               0%
L2TPOverIPsecOverNatT    0               0%
PPPoE                    0               0%
vpnLoadBalanceMgmt       0               0%
userHTTPS                0               0%
IMAP4S                   3 30%
POP3S                    0               0%
SMTPS                    3 30%
```

관련 명령

명령	설명
show vpn-sessiondb	선택적으로 지정한 기준으로 필터링 및 정렬하여 확장 세부 정보와 함께 또는 확장 세부 정보 없이 세션을 표시합니다.
show vpn-sessiondb summary	총 현재 세션, 각 유형의 현재 세션, 피크 및 총 누적, 최대 동시 세션 수 등 세션 요약을 표시합니다.

show vpn-sessiondb summary

IPsec, Cisco AnyConnect 및 NAC 세션 수를 표시하려면 특권 EXEC 모드에서 **show vpn-sessiondb summary** 명령을 사용합니다.

show vpn-sessiondb summary

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(7)	이 명령이 도입되었습니다.
8.0(2)	VLAN Mapping Sessions 테이블이 추가되었습니다.
8.0(5)	active, cumulative, peak concurrent 및 inactive에 대한 새 출력이 추가되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

예

다음은 하나의 IPsec IKEv1 및 하나의 클라이언트리스 세션에 대한 **show vpn-sessiondb summary** 명령의 샘플 출력입니다.

참고 대기 상태의 디바이스는 활성 세션과 비활성 세션을 구분하지 않습니다 .

```
ciscoasa# show vpn-sessiondb summary

VPN Session Summary
Sessions:
                        Active :Cumulative :Peak Concurrent :Inactive :
    Clientless VPN            :       1:         2:             1
    Browser                   :       1:         2:             1
    IKEv1 IPsec/L2TP IPsec0   :       1:         1:             1

Total Active and Inactive: 2      Total Cumulative: 3
Device Total VPN Capacity: 10000
Device Load            : 0%

License Information:
    Shared VPN License Information:
        SSL VPN                      : 12000
            Allocated to this device  :    0
            Allocated to network      :    0
```

```
            Device limit              : 750

IPsec   :   750     Configured :750    Active : 0     Load : 0%
SSL VPN :   750     Configured :750    Active : 0     Load : 0%
                        Active : Cumulative : Peak Concurrent
SSL VPN         :           0 :         1 :            1
Totals          :           0 :         1 :

Active NAC Sessions:
  Accepted                : 0
  Rejected                : 0
  Exempted                : 0
  Non-responsive          : 0
Hold-off                : 0
  N/A                     : 0

Active VLAN Mapping Sessions:
  Static                  : 0
  Auth                    : 0
  Access                  : 0
  Guest                   : 0
  Quarantine              : 0
  N/A                     : 0

ciscoasa#
```

SSL 출력을 사용하여 라이센스 수에 대한 물리적 디바이스 리소스를 확인할 수 있습니다. 단일 사용자 세션에서 하나의 라이센스를 사용할 수 있지만 여러 터널을 이용할 수 있습니다. 예를 들어 DTLS를 사용하는 AnyConnect 사용자는 종종 상위 세션, SSL 터널 및 DTLS 터널에 연결되어 있습니다.

참고 상위 세션은 클라이언트가 능동적으로 연결되어 있지 않은 경우를 나타냅니다. 이는 암호화된 터널을 나타내지 않습니다. 클라이언트가 종료하거나 대기 상태에 있는 경우 IPsec, IKE, TLS 및 DLTLS 터널은 닫히지만 상위 세션은 유휴 시간 또는 최대 연결 시간 제한에 도달할 때까지 그대로 유지됩니다. 따라서 사용자는 재인증하지 않고도 다시 연결할 수 있습니다.

이 예에서는 한 명의 사용자만 로그인되어 있지만 디바이스에 세 개의 터널이 할당되어 있습니다. IPsec LAN-to-LAN 터널은 하나의 세션으로 계산되며, 터널을 통해 여러 호스트 간 연결을 허용합니다. IPsec 원격 액세스 세션은 하나의 사용자 연결을 지원하는 하나의 원격 액세스 터널입니다.

출력에서 어떤 세션이 활성 상태인지 알 수 있습니다. 세션에 연결된 기본 터널이 없는 경우 상태는 *waiting to resume* 모드(세션 출력에 clientless로 표시됨)입니다. 이 모드는 헤드 엔드 디바이스에서 데드 피어 감지가 시작되었으며, 헤드 엔드 디바이스가 클라이언트와 더 이상 통신할 수 없음을 의미합니다. 이 조건이 발생하면 사용자가 네트워크를 로밍하고, 대기 모드로 전환하고, 세션을 복구하는 등의 작업을 수행할 수 있도록 세션을 유지할 수 있습니다. 이러한 세션은 능동적으로 연결된 세션(라이센스 관점에서)으로 간주되며, 사용자 유휴 시간 제한, 사용자 로그아웃 또는 원래 세션 재개를 통해 지워집니다.

Active SSL VPN With Client 열은 데이터를 전달하는 활성 연결 수를 표시합니다. Cumulative SSL VPN With Client 열은 설정된 활성 세션 수를 표시합니다. 이 열은 비활성 세션을 포함하며, 새 세션이 추가된 경우에만 증가합니다. Peak Concurrent SSL VPN With Client 열은 데이터를 전달하는 동시 활성 세션의 피크 수를 표시합니다. Inactive SSL VPN With Client 열은 AnyConnect 클라이언트의 연결이 끊어진 기간을 표시합니다. 이 Inactivity timeout 값을 사용하여 라이센스가 만료되는 시점을 확인할 수 있습니다. 그런 다음 ASA에서 재연결이 가능한지 확인할 수 있습니다. 이는 활성 SSL 터널이 연결되지 않은 AnyConnect 세션입니다.

표 14-3에는 Active Sessions 및 Session Information 테이블의 필드에 대한 설명이 나와 있습니다.

표 14-3 show vpn-sessiondb summary 명령: Active Sessions 및 Session Information 필드

필드	설명
Concurrent Limit	이 ASA에서 허용되는 동시 활성 세션의 최대 수입니다.
Cumulative Sessions	ASA가 마지막으로 재부팅되거나 재설정된 이후 모든 유형의 세션 수입니다.
LAN-to-LAN	현재 활성 상태인 IPsec LAN-to-LAN 세션 수입니다.
Peak Concurrent	ASA가 마지막으로 재부팅되거나 재설정된 이후 동시에 활성화된 모든 유형의 최대 세션 수입니다.
Percent Session Load	사용 중인 VPN 세션 할당의 백분율입니다. 이 값은 Total Active Sessions를 사용 가능한 최대 세션 수로 나눠 백분율로 표시한 값과 같습니다. 사용 가능한 최대 세션 수는 다음 중 하나일 수 있습니다. • 라이센스가 있는 최대 IPsec 및 SSL VPN 세션 수 • **vpn-sessiondb ?** (구성된 최대 세션 수) • **max-anyconnect-premium-or-essentials-limit**(최대 AnyConnect Premium 또는 Essentials 세션 제한) • **max-other-vpn-limit**(최대 기타 VPN 세션 제한)
Remote Access	ra-ikev1-ipsec - 현재 활성 상태인 IKEv1 IPsec 원격 액세스 사용자, L2TP over IPsec 및 IPsec through NAT 세션 수입니다.
Total Active Sessions	현재 활성 상태인 모든 유형의 세션 수입니다.

Active NAC Sessions 테이블은 상태 검증 대상인 원격 피어에 대한 일반적인 통계를 표시합니다.

Cumulative NAC Sessions 테이블은 현재 상태 검증 대상이거나 이전에 대상이었던 원격 피어에 대한 일반적인 통계를 표시합니다.

표 14-2에는 Active NAC Sessions 및 Total Cumulative NAC Sessions 테이블의 필드에 대한 설명이 나와 있습니다.

표 14-4 show vpn-sessiondb summary 명령: Active NAC Sessions 및 Total Cumulative NAC Sessions 필드

필드	설명
Accepted	상태 검증에 통과하여 Access Control Server로부터 액세스 정책을 부여받은 피어 수입니다.
Exempted	ASA에 구성된 Posture Validation Exception(상태 검증 예외) 목록의 항목과 일치하기 때문에 상태 검증을 받을 필요가 없는 피어 수입니다.
Hold-off	성공적인 상태 검증 후 ASA에서 EAPoUDP 통신이 끊어진 피어 수입니다. NAC Hold Timer 특성(Configuration(구성) > VPN > NAC)에 따라 이 유형의 이벤트와 다음 상태 검증 시도 간의 지연 시간이 결정됩니다.
N/A	VPN NAC 그룹 정책에 따라 NAC가 비활성화된 피어 수입니다.

표 14-4 show vpn-sessiondb summary 명령: Active NAC Sessions 및 Total Cumulative NAC Sessions 필드 (계속)

필드	설명
Non-responsive	상태 검증을 위한 EAP(확장 가능 인증 프로토콜) over UDP 요청에 응답하지 않는 피어 수입니다. 실행 중인 CTA가 없는 피어는 이러한 요청에 응답하지 않습니다. ASA 컨피그레이션에서 클라이언트리스 호스트를 지원하는 경우 Access Control Server는 클라이언트리스 호스트와 연관된 액세스 정책을 이러한 피어의 ASA로 다운로드합니다. 그렇지 않으면 ASA는 NAC 기본 정책을 할당합니다.
Rejected	상태 검증에 실패하여 Access Control Server로부터 액세스 정책을 부여받지 못한 피어 수입니다.

Active VLAN Mapping Sessions 테이블은 상태 검증 대상인 원격 피어에 대한 일반적인 통계를 표시합니다.

Cumulative Mapping VLAN Sessions 테이블은 현재 상태 검증 대상이거나 이전에 대상이었던 원격 피어에 대한 일반적인 통계를 표시합니다.

표 14-5에는 Active VLAN Mapping Sessions 및 Cumulative VLAN Mapping Sessions 테이블의 필드에 대한 설명이 나와 있습니다.

표 14-5 show vpn-sessiondb summary 명령: Active VLAN Mapping Sessions 및 Cumulative Active VLAN Mapping Sessions 필드

필드	설명
Access	이후 사용을 위해 예약되었습니다.
Auth	이후 사용을 위해 예약되었습니다.
게스트	이후 사용을 위해 예약되었습니다.
N/A	이후 사용을 위해 예약되었습니다.
Quarantine	이후 사용을 위해 예약되었습니다.
Static	이 필드는 미리 구성된 VLAN에 할당된 VPN 세션 수를 표시합니다.

관련 명령

명령	설명
show vpn-sessiondb	선택적으로 지정한 기준으로 필터링 및 정렬하여 확장 세부 정보와 함께 또는 확장 세부 정보 없이 세션을 표시합니다.
show vpn-sessiondb ratio	VPN 세션 암호화 또는 프로토콜 비율을 표시합니다.

show wccp

WCCP(Web Cache Communication Protocol)와 관련된 전역 통계를 표시하려면 특권 EXEC 모드에서 **show wccp** 명령을 사용합니다.

show wccp {**web-cache** | *service-number*}[*detail* | *view*]

구문 설명

detail	(선택 사항) 라우터 및 모든 웹 캐시에 대한 정보를 표시합니다.
service-number	(선택 사항) 캐시에서 제어되는 웹 캐시 서비스 그룹의 식별 번호입니다. 이 번호는 0에서 256 사이일 수 있습니다. Cisco Cache Engine을 사용하는 웹 캐시의 경우 역방향 프록시 서비스는 값 99로 표시됩니다.
view	(선택 사항) 감지되거나 감지되지 않은 특정 서비스 그룹의 다른 멤버를 표시합니다.
web-cache	웹 캐시 서비스에 대한 통계를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예에서는 WCCP 정보를 표시하는 방법을 보여 줍니다.

```
ciscoasa(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
ciscoasa(config)#
```

관련 명령

명령	설명
wccp	서비스 그룹에 대한 WCCP 지원을 활성화합니다.
wccp redirect	WCCP 리디렉션 지원을 활성화합니다.

show webvpn csd

CSD가 활성화되었는지 여부를 확인하고, 실행 중인 컨피그레이션의 CSD 버전을 표시하고, 이미지에서 Host Scan 패키지를 제공하는지 확인하고, 파일을 테스트하여 유효한 CSD 배포 패키지인지 알아보려면 특권 EXEC 모드에서 **show webvpn csd** 명령을 사용합니다.

show webvpn csd [**image** *filename*]

구문 설명

filename	CSD 배포 패키지로 유효한지 테스트할 파일의 이름을 지정합니다. **csd_n.n.n-k9.pkg** 형식이어야 합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

예

show webvpn csd 명령을 사용하여 CSD의 작동 상태를 확인할 수 있습니다. CLI는 CSD가 설치되고 활성화되었는지, Host Scan이 설치되고 활성화되었는지, CSD 패키지와 Host Scan 패키지가 둘 다 설치된 경우 어떤 이미지에서 Host Scan 패키지를 제공하는지를 나타내는 메시지로 응답합니다.

```
ciscoasa# show webvpn csd
```

받을 수 있는 메시지는 다음과 같습니다.

- `Secure Desktop is not installed`

  `Hostscan is not installed`

- `Secure Desktop version n.n.n.n is currently installed but not enabled`

  `Standalone Hostscan package is not installed (Hostscan is currently installed via the CSD package but not enabled)`

- `Secure Desktop version n.n.n.n is currently installed and enabled`

  `Standalone Hostscan package is not installed (Hostscan is currently installed and enabled via the CSD package)`

"Secure Desktop version *n.n.n.n* is currently installed ..." 메시지는 이미지가 ASA에 로드되어 있고 실행 중인 컨피그레이션에 있음을 의미합니다. 이미지는 **enabled** 또는 **not enabled**일 수 있습니다. webvpn 컨피그레이션 모드로 전환해 **csd enable** 명령을 입력하여 CSD를 활성화할 수 있습니다.

"(Hostscan is currently installed and enabled via the CSD package)" 메시지는 CSD 패키지와 함께 제공된 Host Scan 패키지가 현재 사용 중임을 의미합니다.

- Secure Desktop version *n.n.n.n* is currently installed and enabled
  Hostscan version *n.n.n.n* is currently installed and enabled

  "Secure Desktop version *n.n.n.n* is currently installed and enabled Hostscan version *n.n.n.n* is currently installed and enabled" 메시지는 독립형 패키지 또는 AnyConnect 이미지의 일부로 제공된 CSD와 Host Scan 패키지가 둘 다 설치되어 있음을 의미합니다. Host Scan이 활성화되고 CSD와 Host Scan이 포함된 AnyConnect 이미지가 둘 다 설치 및 활성화되거나 독립형 Host Scan 패키지가 설치 및 활성화된 경우 독립형 패키지 또는 AnyConnect 이미지의 일부로 제공된 Host Scan 패키지가 CSD 패키지와 함께 제공된 Host Scan 패키지보다 우선합니다.

- Secure Desktop version *n.n.n.n* is currently installed but not enabled
  Hostscan version *n.n.n.n* is currently installed but not enabled

show webvpn csd image *filename* 명령을 사용해 파일을 테스트하여 CSD 배포 패키지가 유효한지 확인할 수 있습니다.

ciscoasa# **show webvpn csd image csd_n.n.n-k9.pkg**

이 명령을 입력한 경우 CLI는 다음 메시지 중 하나로 응답합니다.

- ERROR: This is not a valid Secure Desktop image file.

  파일 이름이 **csd_n.n.n_k9.pkg** 형식인지 확인합니다. CSD 패키지에 이 명명 규칙이 없는 경우 파일을 다음 웹사이트에서 가져온 파일로 대체합니다.

  http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

  그런 다음 **show webvpn csd image** 명령을 다시 입력합니다. 이미지가 유효한 경우 webvpn 컨피그레이션 모드에서 **csd image** 및 **csd enable** 명령을 사용하여 CSD를 설치하고 활성화합니다.

- This is a valid Cisco Secure Desktop image:
  Version : 3.6.172.0
  Hostscan Version : 3.6.172.0
  Built on : Wed Feb 23 15:46:44 MST 2011

  파일이 유효한 경우 CLI에서 버전 및 날짜 스탬프를 둘 다 제공합니다.

관련 명령

명령	설명
csd enable	관리 및 원격 사용자 액세스에 CSD를 사용합니다.
csd image	명령에 이름이 지정된 CSD 이미지를 경로에 지정된 플래시 드라이브에서 실행 중인 컨피그레이션으로 복사합니다.

show webvpn group-alias

특정 터널 그룹 또는 모든 터널 그룹에 대한 별칭을 표시하려면 특권 EXEC 모드에서 **group-alias** 명령을 사용합니다.

show webvpn group-alias [*tunnel-group*]

구문 설명

tunnel-group	(선택 사항) 그룹 별칭을 표시할 특정 터널 그룹을 지정합니다.

기본값

터널 그룹 이름을 입력하지 않으면 모든 터널 그룹에 대한 모든 별칭이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1	이 명령이 도입되었습니다.

사용 지침

show webvpn group-alias 명령을 입력하려면 WebVPN이 실행 중이어야 합니다.

각 터널 그룹에는 여러 별칭이 있을 수도 있고 별칭이 없을 수도 있습니다.

예

다음 예에서는 터널 그룹 “devtest”에 대한 별칭을 표시하는 **show webvpn group-alias** 명령과 해당 출력을 보여 줍니다.

```
ciscoasa# show webvpn group-alias devtest
QA
Fra-QA
```

관련 명령

명령	설명
group-alias	그룹의 URL을 하나 이상 지정합니다.
tunnel-group webvpn-attributes	WebVPN 터널 그룹 특성을 구성하는 config-webvpn 모드를 시작합니다.

show webvpn group-url

특정 터널 그룹 또는 모든 터널 그룹에 대한 URL을 표시하려면 특권 EXEC 모드에서 **group-url** 명령을 사용합니다.

show webvpn group-url [*tunnel-group*]

구문 설명

tunnel-group	(선택 사항) URL을 표시할 특정 터널 그룹을 지정합니다.

기본값

터널 그룹 이름을 입력하지 않으면 모든 터널 그룹에 대한 모든 URL이 표시됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

사용 지침

show webvpn group-url 명령을 입력하려면 WebVPN이 실행 중이어야 합니다. 각 그룹에는 여러 URL이 있을 수도 있고 URL이 없을 수도 있습니다.

예

다음 예에서는 터널 그룹 “frn-eng1”에 대한 URL을 표시하는 **show webvpn group-url** 명령과 해당 출력을 보여 줍니다.

```
ciscoasa# show webvpn group-url
http://www.cisco.com
https://fra1.example.com
https://fra2.example.com
```

관련 명령

명령	설명
group-url	그룹의 URL을 하나 이상 지정합니다.
tunnel-group webvpn-attributes	WebVPN 터널 그룹 특성을 구성하는 config-webvpn 모드를 시작합니다.

show webvpn kcd

webvpn 컨피그레이션 모드에서 **show webvpn kcd** 명령을 사용하여 ASA의 도메인 컨트롤러 정보 및 도메인 가입 상태를 표시할 수 있습니다.

show webvpn kcd

구문 설명

없음

기본값

이 명령에는 기본값이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

사용 지침

webvpn 컨피그레이션 모드의 **show webvpn kcd** 명령은 ASA의 도메인 컨트롤러 정보 및 도메인 가입 상태를 표시합니다.

예

다음 예에서는 **show webvpn kcd** 명령에 대한 중요한 정보 및 상태 메시지 해석을 표시합니다.

이 예에서는 등록이 진행 중이며 완료되지 않았음을 보여 줍니다.

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNAL
Domain Join: In-Progress
```

이 예에서는 등록이 완료되었으며 ASA가 도메인에 조인되었음을 표시합니다.

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNAL
Domain Join: Complete
```

관련 명령

명령	설명
clear aaa kerberos	ASA에서 캐시된 모든 Kerberos 티켓을 지웁니다.
kcd-server	ASA가 Active Directory 도메인에 가입할 수 있도록 합니다.
show aaa kerberos	ASA에서 캐시된 모든 Kerberos 티켓을 표시합니다.

show webvpn sso-server

Webvpn SSO(Single Sign On) 서버에 대한 작업 통계를 표시하려면 특권 EXEC 모드에서 **show webvpn sso-server** 명령을 사용합니다.

show webvpn sso-server [*name***]**

구문 설명

name	선택적으로 SSO 서버 이름을 지정합니다. 서버 이름은 4~31자여야 합니다.

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Config-webvpn-sso-saml	• 예	—	• 예	—	—
Config-webvpn-sso-siteminder	• 예	—	• 예	—	—
특권 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

사용 지침

SSO(WebVPN에만 제공) 지원을 통해 사용자가 사용자 이름 및 비밀번호를 단 한 번만 입력하여 여러 서버에서 다양한 보안 서비스에 액세스할 수 있습니다. **show webvpn sso-server** 명령은 보안 디바이스에 구성된 모든 SSO 서버에 대한 작업 통계를 표시합니다.

SSO 서버 이름 인수를 입력하지 않으면 모든 SSO 서버에 대한 통계가 표시됩니다.

예

특권 EXEC 모드에서 입력된 다음 예에서는 example이라는 SiteMinder-type SSO 서버에 대한 통계를 표시합니다.

```
ciscoasa# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:         0
Number of auth requests:            0
Number of retransmissions:          0
Number of accepts:                  0
Number of rejects:                  0
Number of timeouts:                 0
Number of unrecognized responses:   0
ciscoasa#
```

특정 SSO 서버 이름 없이 실행된 다음 명령 예에서는 ASA에 구성된 모든 SSO 서버에 대한 통계를 표시합니다.

```
ciscoasa#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:         0
Number of auth requests:            0
Number of retransmissions:          0
Number of accepts:                  0
Number of rejects:                  0
Number of timeouts:                 0
Number of unrecognized responses:   0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:         0
Number of auth requests:            0
Number of retransmissions:          0
Number of accepts:                  0
Number of rejects:                  0
Number of timeouts:                 0
Number of unrecognized responses:   0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:         0
Number of auth requests:            0
Number of retransmissions:          0
Number of accepts:                  0
Number of rejects:                  0
Number of timeouts:                 0
Number of unrecognized responses:   0
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
max-retry-attempts	ASA에서 SSO 인증을 재시도할 수 있는 횟수를 구성합니다.
policy-server-secret	SiteMinder-type SSO 서버에 대한 인증 요청을 암호화하는 데 사용되는 비밀 키를 생성합니다.
request-timeout	시간 초과로 인해 SSO 인증 시도가 실패하는 시간(초)을 지정합니다.
sso-server	SSO(Single Sign On) 서버를 생성합니다.
web-agent-url	ASA에서 SiteMinder SSO 인증 요청을 작성하는 SSO 서버 URL을 지정합니다.

show webvpn anyconnect

ASA에 설치되고 캐시 메모리에 로드된 SSL VPN 클라이언트 이미지에 대한 정보를 보거나, 파일을 테스트하여 유효한 클라이언트 이미지인지 알아보려면 특권 EXEC 모드에서 **show webvpn anyconnect** 명령을 사용합니다.

show webvpn anyconnect [**image** *filename*]

구문 설명

image *filename*	SSL VPN 클라이언트 이미지 파일로 테스트할 파일 이름을 지정합니다.

기본값

이 명령에는 기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.
8.4(1)	이 명령의 **show webvpn svc** 형식이 **show webvpn anyconnect**로 대체되었습니다.

사용 지침

show webvpn anyconnect 명령을 사용하여 캐시 메모리에 로드되고 원격 PC에 다운로드할 수 있는 SSL VPN 클라이언트 이미지에 대한 정보를 볼 수 있습니다. **image** *filename* 키워드 및 인수를 사용해 파일을 테스트하여 유효한 이미지인지 확인할 수 있습니다. 파일이 유효한 이미지가 아닌 경우 다음 메시지가 표시됩니다.

```
ERROR: This is not a valid SSL VPN Client image file.
```

예

다음 예에서는 현재 설치된 이미지에 대한 **show webvpn anyconnect** 명령의 출력을 보여 줍니다.

```
ciscoasa# show webvpn anyconnect
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

다음 예에서는 유효한 이미지에 대한 **show webvpn anyconnect image** *filename* 명령의 출력을 보여 줍니다.

```
ciscoasa(config-webvpn)# show webvpn anyconnect image sslclient-win-1.0.2.127.pkg

This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

관련 명령

명령	설명
anyconnect enable	ASA가 SSL VPN 클라이언트를 원격 PC에 다운로드할 수 있도록 합니다.
anyconnect image	보안 어플라이언스가 플래시 메모리에서 캐시 메모리로 SSL VPN 클라이언트 파일을 로드하도록 하고, 보안 어플라이언스가 클라이언트 이미지를 운영 체제와 일치시킬 대 클라이언트 이미지의 일부를 원격 PC에 다운로드하는 순서를 지정합니다.
vpn-tunnel-protocol	SSL VPN 클라이언트에서 사용하는 SSL을 포함하여 원격 VPN 사용자에 대한 특정 VPN 터널 프로토콜을 활성화합니다.

show xlate

NAT 세션(xlate)에 대한 정보를 표시하려면 특권 EXEC 모드에서 **show xlate** 명령을 사용합니다.

show xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]]
[**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**type** *type*]

show xlate count

구문 설명

count	변환 수를 표시합니다.
global *ip1*[**-***ip2*]	(선택 사항) 매핑된 IP 주소 또는 주소 범위별 활성 변환을 표시합니다.
gport *port1*[*-port2*]	매핑된 포트 또는 포트 범위별 활성 변환을 표시합니다.
interface *if_name*	(선택 사항) 인터페이스별 활성 변환을 표시합니다.
local *ip1*[**-***ip2*]	(선택 사항) 실제 IP 주소 또는 주소 범위별 활성 변환을 표시합니다.
lport *port1*[*-port2*]	실제 포트 또는 포트 범위별 활성 변환을 표시합니다.
netmask *mask*	(선택 사항) 매핑된 IP 주소 또는 실제 IP 주소를 정규화할 네트워크 마스크를 지정합니다.
type *type*	(선택 사항) 유형별 활성 변환을 표시합니다. 다음 유형 중 하나 이상을 입력할 수 있습니다. • **static** • **portmap** • **dynamic** • **twice-nat** 유형을 두 개 이상 지정할 경우 공백으로 구분합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.3(1)	새 NAT 구현을 지원하도록 명령이 수정되었습니다.
8.4(3)	확장 PAT 사용을 표시하도록 **e** 플래그가 추가되었습니다. 또한 xlate가 확장되는 목적지 주소가 표시됩니다.
9.0(1)	IPv6을 지원하도록 명령이 수정되었습니다.

사용 지침

show xlate 명령은 변환 슬롯의 내용을 표시합니다.

vpnclient 컨피그레이션이 활성화되고 내부 호스트에서 DNS 요청을 보내는 경우 **show xlate** 명령은 정적 변환에 대해 여러 xlate를 나열할 수 있습니다.

ASA 클러스터링 환경에서는 PAT 세션을 처리하기 위해 최대 3개의 xlate가 클러스터의 여러 노드에 복제될 수 있습니다. 하나는 연결을 소유한 디바이스에서 생성됩니다. 또 하나는 PAT 주소를 백업하기 위해 다른 디바이스에서 생성됩니다. 마지막 하나는 흐름을 복제하는 디렉터에 존재합니다. 백업 및 디렉터가 같은 디바이스인 경우 3개 대신 2개의 xlate가 생성될 수 있습니다.

예

다음은 **show xlate** 명령의 샘플 출력입니다.

```
ciscoasa# show xlate
5 in use, 5 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
NAT from any:10.90.67.2 to any:10.9.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.90.67.2 to any:10.86.94.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.9.0.9, 10.9.0.10/31, 10.9.0.12/30,
    10.9.0.16/28, 10.9.0.32/29, 10.9.0.40/30,
    10.9.0.44/31 to any:0.0.0.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:14 timeout 0:00:00
```

다음은 **e - extended** 플래그 사용 및 xlate가 확장되는 목적지 주소를 표시하는 **show xlate** 명령의 샘플 출력입니다.

```
ciscoasa# show xlate
1 in use, 1 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
ICMP PAT from inside:10.2.1.100/6000 to outside:172.16.2.200/6000(172.16.2.99)
    flags idle 0:00:06 timeout 0:00:30
TCP PAT from inside:10.2.1.99/5 to outside:172.16.2.200/5(172.16.2.90)
    flags idle 0:00:03 timeout 0:00:30
UDP PAT from inside:10.2.1.101/1025 to outside:172.16.2.200/1025(172.16.2.100)
    flags idle 0:00:10 timeout 0:00:30
```

다음은 IPv4에서 IPv6으로 변환을 표시하는 **show xlate** 명령의 샘플 출력입니다.

```
ciscoasa# show xlate
1 in use, 2 most used
NAT from outside:0.0.0.0/0 to in:2001::/96
flags sT idle 0:16:16 timeout 0:00:00
```

관련 명령

명령	설명
clear xlate	현재 변환 및 연결 정보를 지웁니다.
show conn	모든 활성 연결을 표시합니다.
show local-host	로컬 호스트 네트워크 정보를 표시합니다.
show uauth	현재 인증된 사용자를 표시합니다.

show zone

영역 ID, 상황, 보안 수준 및 멤버를 표시하려면 특권 EXEC 모드에서 **show zone** 명령을 사용합니다.

show zone [*name*]

구문 설명

name	(선택 사항) **zone** 명령으로 설정한 영역 이름을 식별합니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

영역 컨피그레이션을 보려면 **show running-config zone** 명령을 사용합니다.

예

show zone 명령에 대한 다음 출력을 참고하십시오.

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

관련 명령

명령	설명
clear configure zone	영역 컨피그레이션을 지웁니다.
clear conn zone	영역 연결을 지웁니다.
clear local-host zone	영역 호스트를 지웁니다.
show asp table routing	디버깅을 위해 가속화된 보안 경로 테이블을 표시하며, 각 경로와 연계된 영역을 표시합니다.
show asp table zone	디버깅을 위해 가속화된 보안 경로 테이블을 표시합니다.
show conn long	영역에 대한 연결 정보를 표시합니다.
show local-host zone	영역 내 로컬 호스트의 네트워크 상태를 표시합니다.
show nameif zone	인터페이스 이름 및 영역 이름을 표시합니다.
show route zone	영역 인터페이스에 대한 경로를 표시합니다.
show running-config zone	영역 컨피그레이션을 표시합니다.
zone	트래픽 영역을 구성합니다.
zone-member	트래픽 영역에 인터페이스를 할당합니다.

15 장

shun부터 snmp-server user-list까지의 명령

shun

공격 호스트의 연결을 차단하려면 특권 EXEC 모드에서 **shun** 명령을 사용합니다. shun을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

구문 설명

dest_port	(선택 사항) 소스 IP 주소에 shun을 적용할 때, 연결을 끊고자 하는 현재 연결의 목적지 포트를 지정합니다.
dest_ip	(선택 사항) 소스 IP 주소에 shun을 적용할 때, 연결을 끊고자 하는 현재 연결의 목적지 주소를 지정합니다.
protocol	(선택 사항) UDP 또는 TCP와 같은 소스 IP 주소에 shun을 적용할 때 연결을 끊고자 하는 현재 연결의 IP 프로토콜을 지정합니다. 기본적으로 프로토콜은 0입니다(모든 프로토콜).
source_ip	공격 호스트의 주소를 지정합니다. 소스 IP 주소만 지정할 경우, 향후 이 주소에서의 모든 연결은 끊어지나 현재 연결은 그대로 유지됩니다. 현재 연결을 끊고 shun을 적용하려면 연결의 추가 파라미터를 지정합니다. 대상 파라미터에 상관없이 향후 소스 IP 주소의 모든 연결에 대해 shun이 유지됩니다.
source_port	(선택 사항) 소스 IP 주소에 shun을 적용할 때 연결을 끊고자 하는 현재 연결의 소스 포트를 지정합니다.
vlan_id	(선택 사항) 소스 호스트가 상주하는 VLAN ID를 지정합니다.

기본값

기본 프로토콜은 0입니다(모든 프로토콜).

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

shun 명령을 사용하여 공격 호스트의 연결을 차단할 수 있습니다. 차단 기능을 수동으로 제거하거나 Cisco IPS 센서에서 제거할 때까지 향후 이 소스 IP 주소의 모든 연결은 끊어지고 기록됩니다. **shun** 명령의 차단 기능은 지정된 호스트 주소와의 연결이 현재 활성 상태인지의 여부에 상관없이 적용됩니다.

목적지 주소와 소스 및 목적지 포트, 프로토콜을 지정한 경우 일치하는 연결을 삭제할 수 있을 뿐만 아니라 향후 해당 소스 IP 주소의 모든 연결에 shun을 적용할 수 있습니다. 그러면 특정 연결 파라미터와 일치하는 연결뿐만 아니라 이후의 모든 연결에 shun이 적용됩니다.

소스 IP 주소당 하나의 **shun** 명령만 적용 가능합니다.

shun 명령은 공격을 동적으로 차단하는 데 사용되기 때문에 ASA 컨피그레이션에 표시되지 않습니다.

인터페이스 컨피그레이션이 제거될 때마다 해당 인터페이스에 연결된 모든 shun도 제거됩니다. 새 인터페이스를 추가하거나 동일한 인터페이스를 대체(동일한 이름 사용)하는 경우 IPS 센서가 해당 인터페이스를 모니터링할 수 있도록 하려면 그 인터페이스를 IPS 센서에 추가해야 합니다.

예

다음 예에서 공격 호스트(10.1.1.27)가 TCP를 통해 대상(10.2.2.89)에 연결하는 것을 볼 수 있습니다. ASA 연결 테이블의 연결은 다음과 같습니다.

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

다음 옵션을 사용하여 **shun** 명령을 적용합니다.

```
ciscoasa# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

이 명령은 특정 현재 연결을 ASA 연결 테이블에서 삭제하고, 향후 10.1.1.27의 모든 패킷이 ASA를 통해 이동하는 것을 방지합니다.

관련 명령

명령	설명
clear shun	현재 활성화된 모든 shun을 비활성화하고 shun 통계를 지웁니다.
show conn	모든 활성 연결을 표시합니다.
show shun	shun 정보를 표시합니다.

shutdown

인터페이스를 비활성화하려면 인터페이스 컨피그레이션 모드에서 **shutdown** 명령을 사용합니다. 인터페이스를 활성화하려면 이 명령의 **no** 형식을 사용합니다.

shutdown

no shutdown

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

모든 물리적 인터페이스는 기본적으로 종료됩니다. 보안 상황에 할당된 인터페이스는 컨피그레이션에서 종료되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령은 **interface** 명령 키워드에서 인터페이스 컨피그레이션 모드 명령으로 이동되었습니다.

사용 지침

인터페이스의 기본 상태는 유형 및 상황 모드에 따라 다릅니다.

다중 상황 모드에서는 인터페이스가 시스템 실행 공간에서 어떤 상태인지에 상관없이 할당된 모든 인터페이스가 기본적으로 활성화됩니다. 그러나 트래픽이 인터페이스를 통과하려면 시스템 실행 공간에서도 인터페이스가 활성화되어야 합니다. 시스템 실행 공간에서 인터페이스를 종료하면 해당 인터페이스를 공유하는 모든 상황에서 인터페이스가 중단됩니다.

단일 모드 또는 시스템 실행 공간에서 인터페이스의 기본 상태는 다음과 같습니다.

- 물리적 인터페이스 - 비활성화됨.
- 이중 인터페이스 - 활성화됨. 그러나 트래픽이 이중 인터페이스를 통과하려면 물리적 인터페이스 멤버도 활성화되어야 합니다.
- 하위 인터페이스 - 활성화됨 그러나 트래픽이 하위 인터페이스를 통과하려면 물리적 인터페이스도 활성화되어야 합니다.

참고 이 명령은 소프트웨어 인터페이스만 비활성화합니다. 물리적 링크는 가동 상태로 유지되며, 직접 연결된 디바이스는 해당 인터페이스가 **shutdown** 명령으로 구성된 경우에도 여전히 가동 중인 것으로 인식됩니다.

예

다음 예에서는 기본 인터페이스를 활성화합니다.

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

다음 예에서는 하위 인터페이스를 활성화합니다.

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

다음 예에서는 하위 인터페이스를 종료합니다.

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# shutdown
```

관련 명령

명령	설명
clear xlate	기존 연결의 모든 변환을 재설정하여 연결이 다시 설정되도록 합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.

shutdown(ca-server 모드)

로컬 CA(Certificate Authority) 서버를 비활성화하고 사용자가 등록 인터페이스에 액세스할 수 없도록 하려면 CA 서버 컨피그레이션 모드에서 **shutdown** 명령을 사용합니다. CA 서버를 활성화하려면 컨피그레이션을 변경하지 못하도록 하고, 등록 인터페이스 액세스를 허용하려면 이 명령의 **no** 형식을 사용합니다.

[**no**] **shutdown**

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

처음에는 기본적으로 CA 서버가 종료되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

CA 서버 모드의 이 명령은 인터페이스 모드의 **shutdown**과 유사합니다. 설정 시 로컬 CA 서버는 기본적으로 종료되며 **no shutdown** 명령을 사용하여 활성화해야 합니다. **no shutdown** 명령을 처음 사용할 때 CA 서버를 활성화하고 CA 서버 인증서 및 키 쌍을 생성하게 됩니다.

참고 CA 컨피그레이션을 잠그고 **no shutdown** 명령을 사용하여 CA 인증서를 발행한 후에는 CA 컨피그레이션을 변경할 수 없습니다.

CA 서버를 활성화하고 **no shutdown** 명령으로 현재 컨피그레이션을 잠그려면 7자로 된 비밀번호를 사용하여 CA 인증서 및 생성할 키 쌍이 있는 PKCS12 파일을 인코딩 및 아카이빙해야 합니다. 이 파일은 이전에 **database path** 명령을 통해 지정한 저장소에 저장됩니다.

예

다음 예에서는 로컬 CA 서버를 비활성화하고 등록 인터페이스 액세스를 차단합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# shutdown
ciscoasa(config-ca-server)#
```

다음 예에서는 로컬 CA 서버를 활성화하고 등록 인터페이스 액세스를 차단합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no shutdown
ciscoasa(config-ca-server)#

ciscoasa(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...

ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스할 수 있도록 합니다.
show crypto ca server	CA 컨피그레이션의 상태를 표시합니다.

sla monitor

SLA 작업을 생성하려면 글로벌 컨피그레이션 모드에서 **sla monitor** 명령을 사용합니다. SLA 작업을 제거하려면 이 명령의 **no** 형식을 사용합니다.

sla monitor *sla_id*

no sla monitor *sla_id*

구문 설명

sla_id	구성할 SLA의 ID를 지정합니다. SLA가 아직 없는 경우 새로 생성합니다. 유효한 값은 1~2147483647입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

sla monitor 명령은 SLA 작업을 생성하고 SLA 모니터 컨피그레이션 모드를 시작합니다. 이 명령을 입력하면 명령 프롬프트가 `ciscoasa(config-sla-monitor)#`으로 변경되어 SLA 모니터 컨피그레이션 모드 상태임을 나타냅니다. SLA 작업이 이미 있고 유형이 이미 정의된 경우에는 프롬프트가 `ciscoasa(config-sla-monitor-echo)#`으로 표시됩니다. 최대 2000개의 SLA 작업을 생성할 수 있으나, 어느 때든 32개의 SLA 작업만 디버깅할 수 있습니다.

no sla monitor 명령은 지정된 SLA 작업과 해당 작업을 구성하는 데 사용된 명령을 제거합니다.

SLA 작업을 구성한 후에는 **sla monitor schedule** 명령을 사용하여 작업을 예약해야 합니다. SLA 작업을 예약한 후에는 SLA 작업의 컨피그레이션을 수정할 수 없습니다. 예약된 SLA 작업의 컨피그레이션을 수정하려면 **no sla monitor** 명령을 사용하여 선택한 SLA 작업을 완전히 제거해야 합니다. SLA 작업을 제거하면 연관된 **sla monitor schedule** 명령도 제거됩니다. 그러면 SLA 작업 컨피그레이션을 다시 시작할 수 있습니다.

작업의 현재 컨피그레이션 설정을 표시하려면 **show sla monitor configuration** 명령을 사용합니다. SLA 작업의 작업 통계를 표시하려면 **show sla monitor operation-state command** 명령을 사용합니다. 컨피그레이션에서 SLA 명령을 확인하려면 **show running-config sla monitor** 명령을 사용합니다.

예

다음 예에서는 ID 123을 사용하여 SLA 작업을 구성하고 ID가 1인 추적 엔트리를 만들어 SLA 도달 가능성을 추적합니다.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

명령	설명
frequency	SLA 작업이 반복되는 빈도를 지정합니다.
show sla monitor configuration	SLA 컨피그레이션 설정을 표시합니다.
sla monitor schedule	SLA 작업을 예약합니다.
timeout	SLA 작업의 응답 대기 시간을 설정합니다.
track rtr	SLA를 폴링할 추적 항목을 생성합니다.

sla monitor schedule

SLA 작업을 예약하려면 글로벌 컨피그레이션 모드에서 **sla monitor schedule** 명령을 사용합니다. SLA 작업 일정을 제거하고 작업을 보류 중인 상태로 두려면 이 명령의 **no** 형식을 사용합니다.

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

구문 설명

after *hh*:*mm*:*ss*	명령을 입력한 후 지정된 기간(시간, 분, 초) 내에 작업이 시작됨을 나타냅니다.
ageout *seconds*	(선택 사항) 정보 수집이 능동적으로 이루어지지 않을 때 작업을 메모리에 유지할 기간(초)을 지정합니다. 타임아웃된 SLA 작업은 실행 중인 컨피그레이션에서 제거됩니다.
day	작업 시작 날짜를 입력합니다. 유효한 값은 1~31입니다. 날짜를 지정하지 않으면 현재 날짜가 사용됩니다. 날짜를 지정한 경우 달도 지정해야 합니다.
hh:*mm*[:*ss*]	24시간 표기법으로 절대 시작 시간을 지정합니다. 초는 선택 사항입니다. *month* 및 *day*를 지정하지 않은 경우, 다음 돌아오는 지정 시간에 바로 시작합니다..
life forever	(선택 사항) 작업이 무기한 실행되도록 예약합니다.
life *seconds*	(선택 사항) 작업에서 정보를 능동적으로 수집하는 기간(초)을 설정합니다.
month	(선택 사항) 작업을 시작할 달의 이름입니다. 달을 지정하지 않으면 현재의 달이 사용됩니다. 달을 지정한 경우 날짜도 지정해야 합니다. 해당 달의 영문을 그대로 표기하거나 영문의 첫 3자만 입력하면 됩니다.
now	명령을 입력하는 즉시 작업이 시작됨을 나타냅니다.
pending	수집되는 정보가 없음을 나타냅니다. 이것이 기본 상태입니다.
recurring	(선택 사항) 매일 지정된 시간에 지정된 기간 동안 작업이 자동으로 시작됨을 나타냅니다.
sla-id	예약할 SLA 작업의 ID입니다.
start-time	SLA 작업이 시작되는 시간을 설정합니다.

기본값

기본값은 다음과 같습니다.

- SLA 작업은 예약된 시간이 충족될 때까지 **pending** 상태로 유지됩니다. 이는 작업이 활성화되어 있지만 능동적으로 데이터를 수집하지 않음을 의미합니다.
- 기본 **ageout** 시간은 0초(타임아웃 없음)입니다.
- 기본 **life**는 3600초(1시간)입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

SLA 작업이 활성 상태인 경우 정보 수집이 즉시 시작됩니다. 다음 타임라인은 작업의 타임아웃 프로세스를 보여 줍니다.

```
W--------------------X--------------------Y--------------------Z
```

- W는 SLA 작업이 **sla monitor** 명령으로 구성된 시간입니다.
- X는 SLA 작업의 시작 시간입니다. 이는 작업이 "활성화"된 시간입니다.
- Y는 **sla monitor schedule** 명령으로 구성한 수명의 종료 시간입니다(**life** 초가 0으로 카운트다운됨).
- Z는 타임아웃입니다.

타임아웃 프로세스(사용된 경우)는 W에서 카운트다운이 시작되고, X와 Y 사이에서 일시 중지되었다가 구성된 사이즈로 재설정된 후 Y에서 다시 카운트다운을 시작합니다. SLA 작업이 타임아웃되면 실행 중인 컨피그레이션에서 SLA 작업 컨피그레이션이 제거됩니다. 작업을 실행하기도 전에 작업이 타임아웃될 수도 있습니다(즉, Z가 X 이전에 발생할 수 있음). 이러한 상황이 발생하지 않도록 하려면 작업 컨피그레이션 시간과 시작 시간(X와 W) 사이의 차이가 타임아웃 시간(초) 미만이어야 합니다.

recurring 키워드는 단일 SLA 작업 예약에만 지원됩니다. 단일 **sla monitor schedule** 명령을 사용하여 여러 SLA 작업을 예약할 수 없습니다. 반복 SLA 작업의 **life** 값은 1일보다 작아야 합니다. 반복 작업은 **ageout** 값이 “never”(값 0으로 지정됨)이거나 **life** 값과 **ageout** 값의 합계가 1일보다 커야 합니다. 반복 작업을 지정하지 않으면 기존 일반 일정 모드로 작업이 시작됩니다.

SLA 작업을 예약한 후에는 SLA 작업의 컨피그레이션을 수정할 수 없습니다. 예약된 SLA 작업의 컨피그레이션을 수정하려면 **no sla monitor** 명령을 사용하여 선택한 SLA 작업을 완전히 제거해야 합니다. SLA 작업을 제거하면 연관된 **sla monitor schedule** 명령도 제거됩니다. 그러면 SLA 작업 컨피그레이션을 다시 시작할 수 있습니다.

예

다음 예에서는 4월 5일 오후 3시에 능동적 데이터 수집을 위해 예약된 SLA 작업 25를 보여 줍니다. 이 작업은 비활성 상태가 12시간을 초과하면 타임아웃됩니다. 이 SLA 작업이 타임아웃되면 해당 SLA 작업에 대한 모든 컨피그레이션 정보가 실행 중인 컨피그레이션에서 제거됩니다.

```
ciscoasa(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

다음 예에서는 5분 지연 후 능동적 데이터 수집을 위해 예약된 SLA 작업 1을 보여 줍니다. 기본 1시간 수명이 적용됩니다.

```
ciscoasa(config)# sla monitor schedule 1 start after 00:05:00
```

다음 예에서는 즉시 데이터를 수집하고 무기한 실행되도록 예약된 SLA 작업 3을 보여 줍니다.

```
ciscoasa(config)# sla monitor schedule 3 life forever start-time now
```

다음 예에서는 매일 오전 1시 30분에 자동 데이터 수집을 위해 예약된 SLA 작업 15를 보여 줍니다.

```
ciscoasa(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

관련 명령

명령	설명
show sla monitor configuration	SLA 컨피그레이션 설정을 표시합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.

smart-tunnel auto-signon enable

클라이언트리스(브라우저 기반) SSL VPN 세션에서 스마트 터널 자동 로그온을 활성화하려면 group-policy webvpn 컨피그레이션 모드 또는 username webvpn 컨피그레이션 모드에서 **smart-tunnel auto-signon enable** 명령을 사용합니다.

그룹 정책 또는 사용자 이름에서 **smart-tunnel auto-signon enable** 명령을 제거하고 기본 그룹 정책에서 상속하려면 이 명령의 **no** 형식을 사용합니다.

no smart-tunnel auto-signon enable *list* [**domain** *domain*] [port *port*] [realm *realm string*]

구문 설명

domain *domain*	(선택 사항) 인증 과정에서 사용자 이름에 추가할 도메인 이름입니다. 도메인을 입력하는 경우 목록 엔트리에 **use-domain** 키워드를 입력합니다.
list	스마트 터널 자동 로그온 목록의 이름은 ASA webvpn 컨피그레이션에 이미 있습니다. SSL VPN 컨피그레이션에서 스마트 터널 자동 로그온 목록 항목을 보려면 특권 EXEC 모드에서 **show running-config webvpn smart-tunnel** 명령을 입력합니다.
port	자동 로그온을 수행할 포트를 지정합니다.
realm	인증할 영역을 구성합니다.

기본값

이 명령에는 기본값이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy webvpn 컨피그레이션	• 예	—	• 예	—	—
username webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.
8.4(1)	선택 사항인 *realm* 및 *port* 인수가 도입되었습니다.

사용 지침

스마트 터널 자동 로그온 기능은 Microsoft WININET 라이브러리를 사용하여 HTTP 및 HTTPS를 통신하는 애플리케이션만 지원합니다. 예를 들자면 Microsoft Internet Explorer는 WININET 동적 연결 라이브러리를 사용하여 웹 서버와 통신합니다.

먼저 **smart-tunnel auto-signon** *list* 명령을 사용하여 서버 목록을 생성해야 합니다. 그룹 정책 또는 사용자 이름 하나당 목록을 하나씩만 할당할 수 있습니다.

영역 문자열은 웹사이트의 보호 영역과 연결되어 있으며 인증과정 중 인증 프롬프트 또는 HTTP 헤더에서 브라우저로 다시 전달됩니다. 관리자가 해당 영역을 모르는 경우 로그온을 한 번 수행한 후 프롬프트 대화 상자에서 문자열을 가져와야 합니다.

이제 관리자는 선택적으로 해당 호스트에 대한 포트 번호를 지정할 수 있습니다. Firefox의 경우 포트 번호를 지정하지 않으면 HTTP 및 HTTPS에서 자동 로그온이 수행되며, 기본적으로 각각 포트 번호 80과 443을 통해 액세스됩니다.

예

다음 명령은 HR이라는 스마트 터널 자동 로그온 목록을 활성화합니다.

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR
ciscoasa(config-group-webvpn)
```

다음 명령은 인증과정 중 HR이라는 스마트 터널 자동 로그온 목록을 활성화하고 CISCO라는 도메인을 사용자 이름에 추가합니다.

```
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

다음 명령은 그룹 정책에서 HR이라는 스마트 터널 자동 로그온 목록을 제거하고 기본 그룹 정책에서 스마트 터널 자동 로그온 목록 명령을 상속합니다.

```
ciscoasa(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

관련 명령

명령	설명
smart-tunnel auto-signon *list*	스마트 터널 연결에서 자격 증명 제출을 자동화할 서버 목록을 생성합니다.
show running-config webvpn smart-tunnel	ASA의 스마트 터널 컨피그레이션을 표시합니다.
smart-tunnel auto-start	사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.
smart-tunnel disable	스마트 터널 액세스를 차단합니다.
smart-tunnel *list*	클라이언트리스 SSL VPN 세션을 사용하여 개인 사이트에 접속할 수 있는 애플리케이션 목록에 항목을 추가합니다.

smart-tunnel auto-signon list

스마트 터널 연결에서 자격 증명 제출을 자동화할 서버 목록을 만들려면 webvpn 컨피그레이션 모드에서 **smart-tunnel auto-signon list** 명령을 사용합니다. 목록에 추가할 각 서버에 이 명령을 사용해야합니다.

목록에서 항목을 제거하려면 ASA 컨피그레이션에 표시된 대로 목록과 IP 주소 또는 호스트 이름을 둘 다 지정하여 이 명령의 **no** 형식을 사용합니다.

no smart-tunnel auto-signon *list* [**use-domain**] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

스마트 터널 자동 로그온 목록 항목을 표시하려면 특권 EXEC 모드에서 **show running-config webvpn smart-tunnel** 명령을 입력합니다.

서버 목록 전체를 ASA 컨피그레이션에서 제거하려면 해당 목록만 지정하여 이 명령의 **no** 형식을 사용합니다.

no smart-tunnel auto-signon *list*

구문 설명

host	해당 호스트 이름 또는 와일드카드 마스크로 식별되는 서버입니다.
hostname-mask	자동 인증할 호스트 이름 또는 와일드카드 마스크입니다.
ip	해당 IP 주소와 넷마스크로 식별되는 서버입니다.
ip-address [*netmask*]	자동 인증할 호스트의 하위 네트워크입니다.
list	원격 서버 목록의 이름입니다. 공백이 포함된 경우 이름에 따옴표를 사용합니다. 문자열은 최대 64자까지 허용됩니다. 컨피그레이션에 목록이 없는 경우 ASA가 목록을 생성합니다. 컨피그레이션에 목록이 있으면 목록에 항목을 추가합니다.
use-domain	(선택 사항) 인증에 필요한 경우 사용자 이름에 Windows 도메인을 추가합니다. 이 키워드를 입력할 경우 하나 이상의 그룹 정책 또는 사용자 이름에 스마트 터널 목록을 할당할 때 도메인 이름을 지정해야 합니다.

기본값

이 명령에는 기본값이 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.

사용 지침

스마트 터널 자동 로그온 기능은 Microsoft WININET 라이브러리를 사용하여 HTTP 및 HTTPS를 통신하는 애플리케이션만 지원합니다. 예를 들자면 Microsoft Internet Explorer는 WININET 동적 연결 라이브러리를 사용하여 웹 서버와 통신합니다.

스마트 터널 자동 로그온 목록 작성 후, group policy webvpn 또는 username webvpn 모드에서 **smart-tunnel auto-signon enable** *list* 명령을 사용하여 목록을 할당합니다.

예

다음 명령은 서브넷의 모든 호스트를 추가하고 인증에 필요한 경우 사용자 이름에 Windows 도메인을 추가합니다.

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

다음 명령은 목록에서 해당 항목을 제거합니다.

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

위에 표시된 명령은 제거된 항목이 HR이라는 목록의 유일한 항목인 경우 그 목록도 제거합니다. 그렇지 않은 경우 다음 명령은 ASA 컨피그레이션에서 목록 전체를 제거합니다.

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR
```

다음 명령은 도메인의 모든 호스트를 intranet이라는 스마트 터널 자동 로그온 목록에 추가합니다.

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

다음 명령은 목록에서 해당 항목을 제거합니다.

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon intranet host *.exampledomain.com
```

관련 명령s

명령	설명
smart-tunnel auto-signon enable	명령 모드에 지정된 그룹 정책 또는 사용자 이름에 대해 스마트 터널 자동 로그온을 활성화합니다.
smart-tunnel auto-signon enable *list*	그룹 정책 또는 사용자 이름에 스마트 터널 자동 로그온 목록을 할당합니다.
show running-config webvpn smart-tunnel	스마트 터널 컨피그레이션을 표시합니다.
smart-tunnel auto-start	사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.
smart-tunnel enable	사용자 로그인 시 스마트 터널 액세스를 활성화합니다. 하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access > Start Smart Tunnels** 버튼을 사용하여 수동으로 스마트 터널 액세스를 시작해야 합니다.

smart-tunnel auto-start

클라이언트리스(브라우저 기반) SSL VPN 세션에서 사용자 로그인 시 스마트 터널 액세스를 자동으로 시작하려면 group-policy webvpn 컨피그레이션 모드 또는 username webvpn 컨피그레이션 모드에서 **smart-tunnel auto-start** 명령을 사용합니다.

smart-tunnel auto-start *list*

그룹 정책 또는 사용자 이름에서 **smart-tunnel** 명령을 제거하고 기본 그룹 정책에서 **[no] smart-tunnel** 명령을 상속하려면 이 명령의 **no** 형식을 사용합니다.

no smart-tunnel

구문 설명

list	*list*는 ASA webvpn 컨피그레이션의 기존 스마트 터널 목록의 이름입니다. SSL VPN 컨피그레이션의 기존 스마트 터널 목록 항목을 보려면 특권 EXEC 모드에서 **show running-config webvpn** 명령을 입력합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy webvpn 컨피그레이션 모드	• 예	—	• 예	—	—
username webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하려면 먼저 **smart-tunnel list** 명령을 사용하여 애플리케이션 목록을 만들어야 합니다.

사용자가 로그인 시 스마트 터널 액세스를 시작하는 이 옵션은 Windows에만 적용됩니다.

예

다음 명령은 apps1이라는 애플리케이션 목록에 대한 스마트 터널 액세스를 시작합니다.

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-start apps1
ciscoasa(config-group-webvpn)
```

다음 명령은 그룹 정책에서 apps1이라는 목록을 제거하고 기본 그룹 정책에서 스마트 터널 명령을 상속합니다.

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

관련 명령

명령	설명
show running-config webvpn	모든 스마트 터널 목록 항목을 포함하여 클라이언트리스 SSL VPN 컨피그레이션을 표시합니다.
smart-tunnel disable	스마트 터널 액세스를 차단합니다.
smart-tunnel enable	사용자 로그인 시 스마트 터널 액세스를 활성화합니다. 하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access > Start Smart Tunnels** 버튼을 사용하여 수동으로 스마트 터널 액세스를 시작해야 합니다.
smart-tunnel list	클라이언트리스 SSL VPN 세션을 사용하여 개인 사이트에 접속할 수 있는 애플리케이션 목록에 항목을 추가합니다.

smart-tunnel disable

스마트 터널이 클라이언트리스(브라우저 기반) SSL VPN 세션을 통해 액세스하지 못하도록 하려면 group-policy webvpn 컨피그레이션 모드 또는 username webvpn 컨피그레이션 모드에서 **smart-tunnel disable** 명령을 사용합니다.

smart-tunnel disable

그룹 정책 또는 사용자 이름에서 **smart-tunnel** 명령을 제거하고 기본 그룹 정책에서 **[no] smart-tunnel** 명령을 상속하려면 이 명령의 **no** 형식을 사용합니다.

no smart-tunnel

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy webvpn 컨피그레이션 모드	• 예	—	• 예	—	—
username webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

기본적으로 스마트 터널은 활성화되어 있지 않으므로 **smart-tunnel disable** 명령은 (기본) 그룹 정책 또는 사용자 이름 컨피그레이션에 해당 그룹 정책 또는 사용자 이름에 적용하지 않으려는 **smart-tunnel auto-start** 또는 **smart-tunnel enable** 명령이 포함된 경우에만 필요합니다.

예

다음 명령은 스마트 터널 액세스를 차단합니다.

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel disable
ciscoasa(config-group-webvpn)
```

관련 명령

명령	설명
smart-tunnel auto-start	사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.
smart-tunnel enable	사용자 로그인 시 스마트 터널 액세스를 활성화합니다. 하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access > Start Smart Tunnels** 버튼을 사용하여 수동으로 스마트 터널 액세스를 시작해야 합니다.
smart-tunnel list	클라이언트리스 SSL VPN 세션을 사용하여 개인 사이트에 접속할 수 있는 애플리케이션 목록에 항목을 추가합니다.

smart-tunnel enable

스마트 터널이 클라이언트리스(브라우저 기반) SSL VPN 세션을 통해 액세스할 수 있도록 하려면 group-policy webvpn 컨피그레이션 모드 또는 username webvpn 컨피그레이션 모드에서 **smart-tunnel enable** 명령을 사용합니다.

smart-tunnel enable *list*

그룹 정책 또는 사용자 이름에서 **smart-tunnel** 명령을 제거하고 기본 그룹 정책에서 **[no] smart-tunnel** 명령을 상속하려면 이 명령의 **no** 형식을 사용합니다.

no smart-tunnel

구문 설명

list	*list*는 ASA webvpn 컨피그레이션의 기존 스마트 터널 목록의 이름입니다. SSL VPN 컨피그레이션에서 스마트 터널 목록 항목을 보려면 특권 EXEC 모드에서 **show running-config webvpn** 명령을 입력합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy webvpn 컨피그레이션 모드	• 예	—	• 예	—	—
username webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

smart-tunnel enable 명령은 스마트 터널 액세스를 사용 가능한 애플리케이션 목록을 그룹 정책 또는 사용자 이름에 할당합니다. 이를 위해서는 사용자가 clientless-SSL-VPN 포털 페이지에서 **Application Access > Start Smart Tunnels** 버튼을 사용하여 스마트 터널 액세스를 수동으로 시작해야 합니다. 또는 **smart-tunnel auto-start** 명령을 사용하여 사용자 로그인 시 스마트 터널 액세스를 자동으로 시작할 수 있습니다.

두 명령 모두 먼저 **smart-tunnel list** 명령을 사용하여 애플리케이션 목록을 만들어야 합니다.

예

다음 명령은 apps1이라는 스마트 터널 목록을 활성화합니다.

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel enable apps1
ciscoasa(config-group-webvpn)
```

다음 명령은 그룹 정책에서 apps1이라는 목록을 제거하고 기본 그룹 정책에서 스마트 터널 목록을 상속합니다.

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

관련 명령

명령	설명
show running-config webvpn	모든 스마트 터널 목록 항목을 포함하여 클라이언트리스 SSL VPN 컨피그레이션을 표시합니다.
smart-tunnel auto-start	사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.
smart-tunnel disable	스마트 터널 액세스를 차단합니다.
smart-tunnel list	클라이언트리스 SSL VPN 세션을 사용하여 개인 사이트에 접속할 수 있는 애플리케이션 목록에 항목을 추가합니다.

smart-tunnel list

클라이언트리스(브라우저 기반) SSL VPN 세션을 사용하여 개인 사이트에 접속할 수 있는 애플리케이션 목록을 작성하려면 webvpn 컨피그레이션 모드에서 **smart-tunnel list** 명령을 사용합니다. 목록에서 애플리케이션을 제거하려면 항목을 지정하여 이 명령의 **no** 형식을 사용합니다. 전체 애플리케이션 목록을 ASA 컨피그레이션에서 제거하려면 목록만 지정하여 이 명령의 **no** 형식을 사용합니다.

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

no smart-tunnel list *list*

구문 설명

application	스마트 터널 액세스 권한을 부여할 애플리케이션의 이름입니다. 문자열은 최대 64자까지 허용됩니다.
hash	(선택 사항이며 Windows만 해당) 이 값을 얻으려면 SHA-1 알고리즘을 사용하여 해시를 계산하는 유틸리티에 애플리케이션 체크섬, 즉 실행 파일의 체크섬을 입력합니다. 이러한 유틸리티의 예로 Microsoft FCIV(File Checksum Integrity Verifier)가 있으며 http://support.microsoft.com/kb/841290/에서 얻을 수 있습니다. FCIV를 설치한 후에는 해시할 애플리케이션의 임시 사본을 공백 없는 경로(예: c:/fciv.exe)에 배치한 후 커맨드 라인에 **fciv.exe -sha1** *application*을 입력하여(예: **fciv.exe -sha1 c:\msimn.exe**) SHA-1 해시를 표시합니다. SHA-1 해시는 항상 16진수 40자입니다.
list	애플리케이션 또는 프로그램 목록의 이름입니다. 공백이 포함된 경우 이름에 따옴표를 사용합니다. 컨피그레이션에 목록이 없는 경우 CLI가 목록을 생성합니다. 컨피그레이션에 목록이 있으면 목록에 항목을 추가합니다.
path	Mac OS의 경우 애플리케이션의 전체 경로이고, Windows의 경우 애플리케이션의 파일 이름을 포함하는 애플리케이션의 전체 또는 일부 경로입니다. 문자열은 최대 128자까지 허용됩니다.
platform *OS*	(OS가 Microsoft Windows인 경우 선택 사항) **windows 또는 mac**을 입력하여 애플리케이션의 호스트를 지정합니다.

기본값

Windows가 기본 플랫폼입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
8.0(4)	Added **platform** *OS*.

사용 지침

ASA에서 둘 이상의 스마트 터널 액세스 목록을 구성할 수 있지만 어느 그룹 정책 또는 사용자 이름에도 둘 이상의 스마트 터널 목록을 할당할 수는 없습니다. 스마트 터널 목록을 작성하려면 각 애플리케이션에 한 번씩 **smart-tunnel list** 명령을 입력합니다. 이때 동일한 *list* 문자열을 입력하되, *application* 및 *path*는 OS에 고유하게 지정해야 합니다. 목록에서 지원할 각 *OS*에 대해 한 번씩 명령을 입력합니다.

OS가 항목에 지정된 것과 일치하지 않으면 세션에서 목록 항목이 무시됩니다. 또한 애플리케이션에 경로가 존재하지 않는 경우에도 항목이 무시됩니다.

SSL VPN 컨피그레이션에서 스마트 터널 목록 항목을 보려면 특권 EXEC 모드에서 **show running-config webvpn smart-tunnel** 명령을 입력합니다.

*path*는 컴퓨터의 경로와 일치해야 하지만 완전하지 않아도 됩니다. 예를 들어 *path*는 실행 파일과 해당 확장명으로만 구성될 수 있습니다.

스마트 터널에 대한 필요 조건은 다음과 같습니다.

- 스마트 터널 연결을 시작하는 원격 호스트는 32비트 버전의 Microsoft Windows Vista, Windows XP 또는 Windows 2000을 실행하거나 Mac OS 10.4 또는 10.5를 실행해야 합니다.
- 스마트 터널 또는 포트 포워딩을 사용하는 Microsoft Windows Vista 사용자는 신뢰할 수 있는 사이트 영역에 ASA의 URL을 추가해야 합니다. 신뢰할 수 있는 사이트 영역에 액세스하려면 Internet Explorer를 시작한 다음 도구 > 인터넷 옵션 > 보안 탭을 선택합니다. 또한 Vista 사용자는 스마트 터널 액세스를 용이하게 하기 위해 보호 모드를 비활성화할 수 있습니다. 그러나 이렇게 하면 컴퓨터가 공격에 더욱 취약해지므로 이 방법을 사용하지 않는 것이 좋습니다.
- 브라우저가 Java, Microsoft ActiveX 또는 둘 다에서 활성화되어 있어야 합니다.
- Mac OS에 대한 스마트 터널 지원에는 Safari 3.1.1 이상의 버전이 필요합니다.

Microsoft Windows에서는 TCP 기반 애플리케이션인 Winsock 2만 스마트 터널 액세스 대상입니다.

Mac OS에서는 SSL 라이브러리에 동적으로 연결된 TCP를 사용하는 애플리케이션이 스마트 터널에서 작동할 수 있습니다. 다음 애플리케이션 유형은 스마트 터널에서 작동하지 않습니다.

- dlopen 또는 dlsym을 사용하여 libsocket 호출을 찾는 애플리케이션
- libsocket 호출을 찾기 위해 정적으로 연결된 애플리케이션
- Mac OS 2단계 네임스페이스를 사용하는 애플리케이션
- Telnet, SSH, cURL 같은 콘솔 기반 Mac OS 애플리케이션
- PowerPC 유형 Mac OS 애플리케이션. Mac OS 애플리케이션 유형을 확인하려면 해당 아이콘을 마우스 오른쪽 버튼으로 클릭하고 Get Info(정보 가져오기)를 선택합니다.

Mac OS에서는 포털 페이지에서 시작된 응용 프로그램만 스마트 터널 세션을 설정할 수 있습니다. 이 필요 조건은 Firefox에 대한 스마트 터널 지원에도 적용됩니다. 스마트 터널을 처음 사용하는 동안 Firefox를 사용하여 Firefox의 또 다른 인스턴스를 시작하려면 csco_st라는 사용자 프로파일이 필요합니다. 이 사용자 프로파일이 없는 경우 새로 만들라는 메시지가 표시됩니다.

스마트 터널에는 다음 제한 사항이 적용됩니다.

- 원격 컴퓨터에서 ASA에 연결하는 데 프록시 서버가 필요한 경우 연결이 종료되는 쪽의 URL은 프록시 서비스에서 제외된 URL 목록에 있어야 합니다. 이 컨피그레이션에서는 스마트 터널이 기본 인증만 지원합니다.
- 스마트 터널 자동 로그온 기능은 Microsoft Windows OS에서 Microsoft WININET 라이브러리를 사용하여 HTTP 및 HTTPS를 통신하는 애플리케이션만 지원합니다. 예를 들자면 Microsoft Internet Explorer는 WININET 동적 연결 라이브러리를 사용하여 웹 서버와 통신합니다.
- 그룹 정책 또는 로컬 사용자 정책은 최대 하나의 스마트 터널 액세스 대상 애플리케이션 목록 및 하나의 스마트 터널 자동 로그온 서버 목록을 지원합니다.
- 상태 저장 대체작동은 스마트 터널 연결을 유지하지 않습니다. 사용자는 대체작동 후 다시 연결해야 합니다.

참고 스마트 터널 액세스에 갑자기 문제가 발생하는 경우는 애플리케이션 업그레이드로 인해 *path* 값이 더이상 유효하지 않다는 의미일 수도 있습니다. 예를 들어 애플리케이션 및 다음 업그레이드를 개발하는 회사가 인수되고 나면 일반적으로 애플리케이션의 기본 경로가 변경됩니다.

해시를 입력하면 *path*에 지정한 문자열과 일치하는 부적격 파일에 클라이언트리스 SSL VPN이 액세스 권한을 부여하지 않으므로 안심할 수 있습니다. 애플리케이션의 각 버전 또는 패치마다 체크섬이 다르기 때문에 입력하는 *hash*가 원격 호스트의 특정 버전 또는 특정 패치하고만 일치할 수도 있습니다. 여러 버전의 애플리케이션에 대한 *hash*를 지정하려면 각 버전에 대해 한 번씩 **smart-tunnel list** 명령을 입력합니다. 이때 동일한 *list* 문자열을 입력하되, 각 명령에서 고유한 *application* 문자열 및 고유한 *hash* 값을 지정해야 합니다.

참고 *hash* 값을 입력한 경우 스마트 터널 액세스 권한이 있는 애플리케이션의 이후 버전 또는 패치를 지원하려면 향후 스마트 터널 목록을 유지 관리해야 합니다. 스마트 터널 액세스에 갑자기 문제가 발생할 경우는 애플리케이션 업그레이드로 인해 *hash* 값이 더이상 유효하지 않다는 의미일 수도 있습니다. *hash*를 입력하지 않으면 이 문제를 피할 수 있습니다.

스마트 터널 목록의 컨피그레이션에 따라 **smart-tunnel auto-start** 또는 **smart-tunnel enable** 명령을 사용하여 그룹 정책 또는 사용자 이름에 목록을 할당합니다.

예

다음 명령은 Microsoft Windows 애플리케이션 Connect를 apps1이라는 스마트 터널 목록에 추가합니다.

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

다음 명령은 Windows 애플리케이션 msimn.exe를 추가합니다. 이를 위해서는 원격 호스트의 애플리케이션 해시가 스마트 터널 액세스 대상으로 지정하기 위해 입력한 마지막 문자열과 일치해야 합니다.

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

다음 명령은 Mac OS 브라우저 Safari에 대한 스마트 터널 지원을 제공합니다.

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

관련 명령

명령	설명
show running-config webvpn smart-tunnel	ASA의 스마트 터널 컨피그레이션을 표시합니다.
smart-tunnel auto-start	사용자 로그인 시 자동으로 스마트 터널 액세스를 시작합니다.
smart-tunnel disable	스마트 터널 액세스를 차단합니다.
smart-tunnel enable	사용자 로그인 시 스마트 터널 액세스를 활성화합니다. 하지만 사용자가 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access > Start Smart Tunnels** 버튼을 사용하여 수동으로 스마트 터널 액세스를 시작해야 합니다.

smart-tunnel network

스마트 터널 터널 정책 컨피그레이션에 사용할 호스트 목록을 만들려면 webvpn 컨피그레이션 모드에서 **smart-tunnel network** 명령을 사용합니다. 스마트 터널 정책을 위한 호스트 목록을 허용하지 않으려면 이 명령의 **no** 형식을 사용합니다.

smart-tunnel network

no smart-tunnel network

구문 설명

host *host mask*	*.cisco.com과 같은 호스트 이름 마스크입니다.
ip *ip address*	네트워크의 IP 주소입니다.
netmask	네트워크의 넷마스크입니다.
network name	터널 정책을 적용할 네트워크의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.

사용 지침

스마트 터널이 설정된 경우 네트워크(호스트 집합)를 구성하는 **smart-tunnel network** 명령 및 지정된 스마트 터널 네트워크를 사용하여 사용자에 대한 정책을 적용하는 **smart-tunnel tunnel-policy** 명령으로 터널 외부 트래픽을 허용할 수 있습니다.

예

다음은 **smart-tunnel network** 명령을 사용하는 방법에 대한 샘플입니다.

```
ciscoasa(config-webvpn)# smart-tunnel network testnet ip 192.168.0.0 255.255.255
```

관련 명령

명령	설명
smart-tunnel tunnel-policy	지정된 스마트 터널 네트워크를 사용하여 사용자에 대한 정책을 적용합니다.

smart-tunnel tunnel-policy

특정 그룹 또는 사용자 정책에 스마트 터널 터널 정책을 적용하려면 webvpn 컨피그레이션 모드에서 **smart-tunnel tunnel-policy** 명령을 사용합니다. 특정 그룹에 대한 스마트 터널 터널 정책 적용을 취소하려면 이 명령의 [no] 형식을 사용합니다.

smart-tunnel tunnel-policy

no smart-tunnel tunnel-policy

구문 설명

excludespecified	네트워크 이름에서 지정된 네트워크 외부의 네트워크만 터널링합니다.
network name	터널링할 네트워크를 나열합니다.
tunnelall	모든 항목을 터널링합니다.
tunnelspecified	네트워크 이름에서 지정된 네트워크만 터널링합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.3.1	이 명령이 도입되었습니다.

사용 지침

스마트 터널이 설정된 경우 네트워크(호스트 집합)를 구성하는 **smart-tunnel network** 명령 및 지정된 스마트 터널 네트워크를 사용하여 사용자에 대한 정책을 적용하는 **smart-tunnel tunnel-policy** 명령으로 터널 외부 트래픽을 허용할 수 있습니다.

예

다음은 **smart-tunnel tunnel-policy** 명령을 사용하는 방법에 대한 샘플입니다.

```
ciscoasa(config-username-webvpn)# smart-tunnel tunnel-policy tunnelspecified testnet
```

관련 명령

명령	설명
smart-tunnel network	스마트 터널 정책 컨피그레이션에 사용할 호스트 목록을 생성합니다.

smtp from-address

로컬 CA 서버에서 생성되는 모든 이메일의 E-mail From: 필드에 사용할 이메일 주소를 지정하려면(예: 일회용 비밀번호 배포) CA 서버 컨피그레이션 모드에서 **smtp from-address** 명령을 사용합니다. 이메일 주소를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

smtp from-address *e-mail_address*

no smtp from-address

구문 설명

e-mail_address	CA 서버에서 생성된 모든 이메일의 From: field 필드에 표시되는 이메일 주소를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

예

다음 예에서는 로컬 CA 서버에서 생성된 모든 이메일의 From: 필드에 ca-admin@asa1-ca.example.com이 포함되도록 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address ca-admin@asa1-ca.example.com
ciscoasa(config-ca-server)#
```

다음 예에서는 로컬 CA 서버에서 생성된 모든 이메일의 From: 필드를 기본 주소 admin@asa1-ca.example.com으로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address admin@asa1-ca.example.com
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA의 구성 및 관리를 허용하는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스를 부여합니다.
smtp subject	로컬 CA 서버에서 생성된 모든 이메일의 제목 필드에 표시할 텍스트를 사용자 지정합니다.

smtp subject

로컬 CA(Certificate Authority) 서버에서 생성된 모든 이메일의 제목 필드에 표시할 텍스트를 사용자 지정하려면(예: 일회용 비밀번호 배포) CA 서버 컨피그레이션 모드에서 **smtp subject** 명령을 사용합니다. 텍스트를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

smtp subject *subject-line*

no smtp subject

구문 설명

subject-line	CA 서버에서 전송되는 모든 이메일의 Subj: 필드에 표시될 텍스트를 지정합니다. 문자는 최대 127자까지 허용됩니다.

기본값

기본적으로 Subj: 필드의 텍스트는 “Certificate Enrollment Invitation”입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

예

다음 예에서는 CA 서버에서 생성되는 모든 이메일의 Subj: 필드에 *Action: Enroll for a certificate*라는 텍스트가 표시되도록 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp subject Action: Enroll for a certificate
ciscoasa(config-ca-server)#
```

다음 예에서는 CA 서버에서 생성되는 모든 이메일의 Subj: 필드를 기본 텍스트인 “Certificate Enrollment Invitation”으로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no smtp subject
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA의 구성 및 관리를 허용하는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스를 부여합니다.
smtp from-address	로컬 CA 서버에서 생성되는 모든 이메일의 E-mail From: 필드에 사용할 이메일 주소를 지정합니다.

smtps

SMTPS 컨피그레이션 모드를 시작하려면 글로벌 컨피그레이션 모드에서 **smtps** 명령을 사용합니다. SMTPS 명령 모드에서 입력한 모든 명령을 제거하려면 이 명령의 **no** 버전을 사용합니다. SMTPS는 SSL 연결을 통해 이메일을 보낼 수 있도록 하는 TCP/IP 프로토콜입니다.

smtps

no smtps

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 SMTPS 컨피그레이션 모드를 시작하는 방법을 보여 줍니다.

```
ciscoasa(config)# smtps
ciscoasa(config-smtps)#
```

관련 명령

명령	설명
clear configure smtps	SMTPS 컨피그레이션을 제거합니다.
show running-config smtps	SMTPS에 대한 실행 중인 컨피그레이션을 표시합니다.

smtp-server

SMTP 서버를 구성하려면 글로벌 컨피그레이션 모드에서 **smtp-server** 명령을 사용합니다. 컨피그레이션에서 이 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

구문 설명

backup_server	기본 SMTP 서버를 사용할 수 없는 경우 이벤트 메시지를 릴레이할 백업 SMTP 서버를 식별합니다. IP 주소 또는 호스트 이름(**name** 명령을 사용하여 구성)을 사용합니다.
primary_server	기본 SMTP 서버를 식별합니다. IP 주소 또는 호스트 이름(**name** 명령을 사용하여 구성)을 사용합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

ASA에는 특정 이벤트가 발생했음을 외부 엔터티에 알리기 위해 Event 시스템이 사용할 수 있는 내부 SMTP 클라이언트가 포함되어 있습니다. 이러한 이벤트 알림을 수신한 다음 지정된 이메일 주소로 전달하도록 SMTP 서버를 구성할 수 있습니다. SMTP 기능은 ASA에 대한 이메일 이벤트를 활성화한 경우에만 활성화됩니다.

예

다음 예에서는 SMTP 서버의 IP 주소를 10.1.1.24로 설정하고, 백업 SMTP 서버의 IP 주소를 10.1.1.34로 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp cpu threshold rising

높은 CPU 임계값에 대한 임계값 및 임계값 모니터링 기간을 구성하려면 글로벌 컨피그레이션 모드에서 **snmp cpu threshold rising** 명령을 사용합니다. 임계값 및 임계값 모니터링 기간을 구성하지 않으려면 이 명령의 **no** 형식을 사용합니다.

snmp cpu threshold rising *threshold_value monitoring_period*

no snmp cpu threshold rising *threshold_value monitoring_period*

구문 설명

monitoring_period	모니터링 기간(분)을 정의합니다.
threshold_value	임계값 수준을 백분율 단위의 CPU 사용량으로 정의합니다.

기본값

snmp cpu threshold rising 명령을 구성하지 않은 경우에는 높은 임계값 수준에 대한 기본값이 70%가 넘는 CPU 사용량으로 설정되며, 위험 임계값 수준에 대한 기본값이 95%가 넘는 CPU 사용량으로 설정됩니다. 기본 모니터링 기간은 1분으로 설정됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다. ASA 서비스 모듈에는 적용되지 않습니다.

사용 지침

항상 95%로 유지되는 위험 CPU 임계값 수준은 구성할 수 없습니다. 유효한 임계값 범위는 10~94%의 CPU 사용량입니다. 모니터링 기간에 대한 유효한 값은 1~60분입니다.

예

다음 예에서는 SNMP CPU 임계값 수준을 75%의 CPU 사용량으로 구성하고 모니터링 기간을 30분으로 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp cpu threshold 75% 30
```

관련 명령

명령	설명
snmp-server enable traps	SNMP 관련 트랩을 활성화합니다.
snmp link threshold	SNMP 인터페이스 임계값을 정의합니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.
snmp-server location	SNMP 서버 위치 문자열을 설정합니다.

snmp link threshold

SNMP 물리적 인터페이스에 대한 임계값 및 시스템 메모리 사용량에 대한 임계값을 구성하려면 글로벌 컨피그레이션 모드에서 **snmp link threshold** 명령을 사용합니다. SNMP 물리적 인터페이스에 대한 임계값 및 시스템 메모리 사용량에 대한 임계값을 지우려면 이 명령의 **no** 형식을 사용합니다.

snmp link threshold *threshold_value*

no snmp link threshold *threshold_value*

구문 설명

threshold_value	임계값을 백분율 단위의 CPU 사용량으로 정의합니다.

기본값

snmp link threshold 명령을 구성하지 않은 경우 기본 임계값은 70%의 CPU 사용량 및 시스템 메모리 사용량입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 도입되었습니다.

사용 지침

유효한 임계값 범위는 30~99%의 물리적 인터페이스입니다. **snmp link threshold** 명령은 관리 상황에서만 사용할 수 있습니다.

예

다음 예에서는 SNMP 인터페이스 임계값을 모든 물리적 인터페이스에 대해 75%로 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp link threshold 75%
```

관련 명령

명령	설명
snmp-server enable traps	SNMP 관련 트랩을 활성화합니다.
snmp cpu threshold rising	SNMP CPU 임계값을 정의합니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.
snmp-server location	SNMP 서버 위치 문자열을 설정합니다.

snmp-map

SNMP 검사 파라미터를 정의하는 데 사용할 특정 맵을 식별하려면 글로벌 컨피그레이션 모드에서 **snmp-map** 명령을 사용합니다. 맵을 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-map *map_name*

no snmp-map *map_name*

구문 설명

map_name	SNMP 맵의 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

snmp-map 명령을 사용하여 SNMP 검사 파라미터를 정의하는 데 사용할 특정 맵을 식별할 수 있습니다. 이 명령을 입력하면 시스템이 특정 맵을 정의하는 데 사용되는 여러 명령을 입력할 수 있는 SNMP 맵 컨피그레이션 모드로 전환됩니다. SNMP 맵을 정의한 후에는 **inspect snmp** 명령을 사용하여 맵을 활성화합니다. 그런 다음 **class-map**, **policy-map** 및 **service-policy** 명령을 사용하여 트래픽의 클래스를 정의하고, 해당 클래스에 **inspect** 명령을 적용하고, 하나 이상의 인터페이스에 정책을 적용합니다.

예

다음 예에서는 SNMP 트래픽을 식별하고, SNMP 맵을 정의하고, 정책을 정의하고, 외부 인터페이스에 정책을 적용하는 방법을 보여 줍니다.

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port
ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp
ciscoasa(config-pmap-c)#
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
deny version	특정 버전의 SNMP를 사용하는 트래픽을 허용하지 않습니다.
inspect snmp	SNMP 애플리케이션 검사를 활성화합니다.
policy-map	클래스 맵을 특정 보안 작업과 연계시킵니다.

snmp-server community

SNMP 커뮤니티 문자열을 설정하려면 글로벌 컨피그레이션 모드에서 **snmp-server community** 명령을 사용합니다. SNMP 커뮤니티 문자열을 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server community [*0* | *8*] *community-string*

no snmp-server community [*0* | *8*] *community-string*

구문 설명

0	(선택 사항) 암호화되지 않은(일반 텍스트) 커뮤니티 문자열이 뒤에 오도록 지정합니다.
8	암호화된 커뮤니티 문자열이 뒤에 오도록 지정합니다.
community-string	암호화되거나 암호화되지 않은(일반 텍스트) 형식의 비밀번호인 SNMP 커뮤니티 문자열을 설정합니다. 커뮤니티 문자열은 최대 32자까지 허용됩니다.

기본값

기본 커뮤니티 문자열은 "public"입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.2(1)	*text* 인수가 *community-string* 인수로 변경되었습니다.
8.3(1)	암호화된 비밀번호에 대한 지원이 추가되었습니다.

사용 지침

SNMP 커뮤니티 문자열은 SNMP 관리 스테이션 및 관리할 네트워크 노드 간에 공유되는 암호입니다. 관리 스테이션과 디바이스 간의 버전 1 및 2c 통신에만 사용됩니다. ASA에서는 키를 사용하여 들어오는 SNMP 요청이 유효한지의 여부를 확인합니다.

예를 들어 커뮤니티 문자열로 사이트를 지정한 다음 동일한 문자열로 라우터, ASA 및 관리 스테이션을 구성할 수 있습니다. ASA에서는 이 문자열을 사용하며, 잘못된 커뮤니티 문자열로 된 요청에는 응답하지 않습니다.

암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템(예: CLI, ASDM, CSM 등)에 표시됩니다. 일반 텍스트 비밀번호는 표시되지 않습니다.

암호화된 커뮤니티 문자열은 항상 ASA에서 생성됩니다. 대개 입력 형식은 일반 텍스트 형식입니다.

참고 버전 8.3(1)에서 하위 버전의 ASA 소프트웨어로 다운그레이드하고 암호화된 비밀번호를 구성한 경우에는 먼저 **no key config-key password encryption** 명령을 사용하여 암호화된 비밀번호를 일반 텍스트로 변환한 다음 결과를 저장해야 합니다.

예

다음 예에서는 커뮤니티 문자열을 "onceuponatime"으로 설정합니다.

```
ciscoasa(config)# snmp-server community onceuponatime
```

다음 예에서는 암호화된 커뮤니티 문자열을 설정합니다.

```
ciscoasa(config)# snmp-server community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

다음 예에서는 암호화되지 않은 커뮤니티 문자열을 설정합니다.

```
ciscoasa(config)# snmp-server community 0 cisco
```

관련 명령

명령	설명
clear configure snmp-server	SNMP 카운터를 지웁니다.
snmp-server contact	SNMP 연락처 이름을 설정합니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.
snmp-server location	SNMP 서버 위치 문자열을 설정합니다.

snmp-server contact

SNMP 서버 연락처 이름을 설정하려면 글로벌 컨피그레이션 모드에서 **snmp-server contact** 명령을 사용합니다. SNMP 연락처 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server contact *text*

no snmp-server contact [*text*]

구문 설명

text	담당자 또는 ASA 시스템 관리자의 이름을 지정합니다. 이름은 대/소문자를 구분하며, 최대 127자까지 허용됩니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 SNMP 서버 연락처를 EmployeeA로 설정합니다.

```
ciscoasa(config)# snmp-server contact EmployeeA
```

관련 명령

명령	설명
snmp-server community	SNMP 커뮤니티 문자열을 설정합니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server enable traps	SNMP 트랩을 활성화합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.
snmp-server location	SNMP 서버 위치 문자열을 설정합니다.

snmp-server enable

ASA에서 SNMP 서버를 활성화하려면 글로벌 컨피그레이션 모드에서 **snmp-server enable** 명령을 사용합니다. SNMP 서버를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server enable

no snmp-server enable

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

SNMP 서버는 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

SNMP 트랩 또는 기타 컨피그레이션을 구성 및 재구성하지 않고도 SNMP를 쉽게 활성화 및 비활성화할 수 있습니다.

예

다음 예에서는 SNMP를 활성화하고, SNMP 호스트 및 트랩을 구성하며, 트랩을 syslog 메시지로 전송합니다.

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

관련 명령

명령	설명
snmp-server community	SNMP 커뮤니티 문자열을 설정합니다.
snmp-server contact	SNMP 연락처 이름을 설정합니다.
snmp-server enable traps	SNMP 트랩을 활성화합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.
snmp-server location	SNMP 서버 위치 문자열을 설정합니다.

snmp-server enable traps

ASA에서 NMS에 트랩을 전송할 수 있도록 하려면 글로벌 컨피그레이션 모드에서 **snmp-server enable traps** 명령을 사용합니다. 트랩을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **config** | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **ikev2** [*trap*] [...] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **config** | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*] | **connection-limit-reached** | **cpu threshold rising** | **link-threshold** | **memory-threshold** | **nat** [*trap*]

구문 설명

all	모든 트랩을 활성화합니다.
config	컨피그레이션 트랩을 활성화합니다.
connection-limit-reached	연결 제한에 도달한 트랩을 활성화합니다.
cpu threshold rising	CPU 임계값 증가 트랩을 활성화합니다.
entity [*trap*]	엔터티 트랩을 활성화합니다. **entity** 트랩은 다음과 같습니다. • **accelerator-temperature** • **chassis-fan-failure** • **chassis-temperature** • **config-change** • **cpu-temperature** • **fan-failure** • **fru-insert** • **fru-remove** • **power-supply** • **power-supply-failure** • **power-supply-presence** • **power-supply-temperature**
ipsec [*trap*]	IPsec 트랩을 활성화합니다. **ipsec** 트랩은 다음과 같습니다. • **start** • **stop**
ikev2 [*trap*]	IKEv2 IPsec 트랩을 활성화합니다. **ikev2** 트랩은 다음과 같습니다. • **start** • **stop**
link-threshold	링크 임계값 도달 트랩을 활성화합니다.
memory-threshold	메모리 임계값 도달 트랩을 활성화합니다.
nat [*trap*]	NAT 관련 트랩을 활성화합니다. **nat** 트랩은 다음과 같습니다. • **packet-discard**

remote-access [*trap*]	원격 액세스 트랩을 활성화합니다. **remote-access** 트랩은 다음과 같습니다. • **session-threshold-exceeded**
snmp [*trap*]	SNMP 트랩을 활성화합니다. 기본적으로 모든 SNMP 트랩은 활성화되어 있습니다. **snmp** 트랩은 다음과 같습니다. • **authentication** • **linkup** • **linkdown** • **coldstart** • **warmstart**
syslog	syslog 메시지 트랩을 활성화합니다.

기본값

기본 컨피그레이션에서는 다음 **snmp** 트랩이 활성화되어 있습니다(**snmp-server는 traps snmp authentication linkup linkdown coldstart warmstart를 활성화함**). 이 명령을 입력하고 트랩 유형을 지정하지 않은 경우 기본값은 **syslog**입니다. 기본 **snmp** 트랩은 **syslog** 트랩과 함께 계속 활성화되어 있습니다. 다른 모든 트랩은 기본적으로 비활성화되어 있습니다.

snmp 키워드와 함께 이 명령의 **no** 형식을 사용하여 이러한 트랩을 비활성화할 수 잇습니다. **clear configure snmp-server** 명령은 SNMP 트랩의 기본 활성화를 복원합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.4(1)	**snmp warmstart**, **nat packet-discard**, **link-threshold**, **memory-threshold**, **entity power-supply**, **entity fan-failure**, **entity cpu-temperature**, **cpu threshold rising** 및 **connection-limit-reached** 트랩이 추가되었습니다. 이러한 트랩은 ASASM에 적용되지 않습니다.
8.6(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X를 지원하도록 **entity power-supply-failure**, **entity chassis-fan-failure**, **entity power-supply-presence**, **entity chassis-temperature** 및 **entity power-supply-temperature** 트랩이 추가되었습니다.
9.0(1)	IKEv2 및 IPsec에 대한 다중 상황 모드 지원이 추가되었습니다.
9.3(2)	**config** 및 **entity accelerator-temperature** 트랩에 대한 지원이 추가되었습니다.

사용 지침

개별 트랩 또는 트랩 집합을 활성화하려면 각 기능 유형에 대해 이 명령을 입력합니다. 모든 트랩을 활성화하려면 **all** 키워드를 입력합니다.

NMS로 트랩을 전송하려면 **logging history** 명령을 입력한 다음 **logging enable** 명령을 사용하여 기록을 활성화합니다.

관리 상황에서 생성되는 트랩은 다음 트랩뿐입니다.

- **connection-limit-reached**
- **entity**
- **memory-threshold**

시스템 상황에서 물리적으로 연결된 인터페이스에 대해 관리 상황을 통해 생성되는 트랩은 다음 트랩뿐입니다.

- **interface-threshold**

다른 모든 트랩은 관리 및 사용자 상황에서 사용할 수 있습니다.

accelerator-temperature 임계값 트랩은 ASA 5506-X 및 ASA 5508-X에만 적용됩니다.

chassis-fan-failure 트랩은 ASA 5506-X에 적용되지 않습니다.

config 트랩은 컨피그레이션 모드를 종료한 후에 생성되는 ciscoConfigManEvent 알림 및 ccmCLIRunningConfigChanged 알림을 활성화합니다.

다음 트랩은 ASA 5506-X 및 ASA 5508-X에 적용되지 않습니다.**fan-failure**, **fru-insert**, **fru-remove**, **power-supply**, **power-supply-failure**, **power-supply-presence**, **power-supply-temperature**

다중 상황 모드 지침

- 다중 상황 모드에서는 **fan-failure** 트랩, **power-supply-failure** 트랩 및 **cpu-temperature** 트랩이 관리 상황에서만 생성되고 사용자 상황에서는 생성되지 않습니다. 이러한 트랩은 ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X에만 적용되고 ASA 5505에는 적용되지 않습니다.
- **snmp-server enable traps remote-access session-threshold-exceeded** 명령은 다중 상황 모드에서 지원되지 않습니다.

CPU 사용량이 구성된 모니터링 기간의 임계값보다 큰 경우에는 **cpu threshold rising** 트랩이 생성됩니다.

사용된 시스템 메모리가 80%에 도달하면 **memory-threshold** 트랩이 생성됩니다.

참고 SNMP에서는 전압 센서를 모니터링하지 않습니다.

예

다음 예에서는 SNMP를 활성화하고, SNMP 호스트 및 트랩을 구성한 다음, 트랩을 syslog 메시지로 전송합니다.

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

관련 명령

명령	설명
snmp-server community	SNMP 커뮤니티 문자열을 설정합니다.
snmp-server contact	SNMP 연락처 이름을 설정합니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.
snmp-server location	SNMP 서버 위치 문자열을 설정합니다.

snmp-server group

새 SNMP 그룹을 구성하려면 글로벌 컨피그레이션 모드에서 **snmp-server group** 명령을 사용합니다. 지정된 SNMP 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

no snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

구문 설명

auth	암호화를 사용하지 않는 패킷 인증을 지정합니다.
group-name	그룹 이름을 지정합니다.
noauth	비패킷 인증을 지정합니다.
priv	암호화를 사용하는 패킷 인증을 지정합니다.
v3	그룹이 지원되는 보안 모델 중 가장 안전한 SNMP 버전 3 보안 모델을 사용하도록 지정합니다. 이 버전을 사용하면 인증 특성을 명시적으로 구성할 수 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.
8.3(1)	비밀번호 암호화 지원이 추가되었습니다.

사용 지침

버전 3 보안 모델을 사용하려면 먼저 SNMP 그룹을 구성하고 SNMP 사용자를 구성한 다음 SNMP 호스트를 구성해야 합니다. 또한 버전 3 및 보안 수준을 지정해야 합니다. 커뮤니티 문자열이 내부적으로 구성된 경우 이름이 "public"인 두 그룹이 자동으로 생성됩니다. 하나는 버전 1 보안 모델 그룹이고, 나머지 하나는 버전 2c 보안 모델 그룹입니다. 커뮤니티 문자열을 삭제하면 구성된 두 그룹 모두 자동으로 삭제됩니다.

참고 특정 그룹에 속하도록 구성된 사용자에게는 그룹과 동일한 보안 모델이 있어야 합니다.

ASA를 부팅하거나 업그레이드하는 과정에서 한 자리 비밀번호나 숫자로 시작하고 그 뒤에 공백이 있는 비밀번호는 더 이상 지원되지 않습니다. 예를 들어, 0 pass나 1은 유효하지 않은 비밀번호입니다.

참고 버전 8.3(1)에서 하위 버전의 ASA 소프트웨어로 다운그레이드하고 암호화된 비밀번호를 구성한 경우에는 먼저 **no key config-key password encryption** 명령을 사용하여 암호화된 비밀번호를 일반 텍스트로 변환한 다음 결과를 저장해야 합니다.

예

다음 예에서는 ASA가 그룹 생성, 사용자 생성 및 호스트 생성을 포함하는 SNMP 버전 3 보안 모델을 사용하여 어떻게 SNMP 요청을 받을 수 있는지를 보여 줍니다.

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

관련 명령

명령	설명
clear configure snmp-server	SNMP 컨피그레이션 카운터를 지웁니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.
snmp-server user	새 SNMP 사용자를 생성합니다.

snmp-server host

ASA에서 SNMP를 사용할 수 있는 NMS를 지정하려면 글로벌 컨피그레이션 모드에서 **snmp-server host** 명령을 사용합니다. NMS를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

no snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

구문 설명

0	(선택 사항) 암호화되지 않은(일반 텍스트) 커뮤니티 문자열이 뒤에 오도록 지정합니다.
8	암호화된 커뮤니티 문자열이 뒤에 오도록 지정합니다.
community	NMS의 요청 또는 NMS로 전송되는 트랩 생성 시 기본이 아닌 문자열이 필요하도록 지정합니다. SNMP 버전 1 또는 2c에만 사용할 수 있습니다.
community-string	알림과 함께 전송되거나 NMS의 요청 시 전송되는 비밀번호 같은 커뮤니티 문자열을 지정합니다. 커뮤니티 문자열은 최대 32자까지 허용됩니다. 암호화되거나 암호화되지 않은(일반 텍스트) 형식을 사용할 수 있습니다.
hostname	일반적으로 NMS 또는 SNMP 관리자인 SNMP 알림 호스트를 지정합니다.
interface	NMS가 ASA와 통신하는 데 사용되는 인터페이스 이름을 지정합니다.
ip_address	SNMP 트랩을 전송할 대상 NMS 또는 SNMP 요청을 보낼 NMS의 IP 주소를 지정합니다. IPv4 주소*만* 지원합니다.
poll	(선택 사항) 호스트에서 찾아볼(폴링) 수는 있지만, 트랩을 전송할 수는 없도록 지정합니다.
port	NMS 호스트의 UDP 포트 번호를 설정합니다.
trap	(선택 사항) 트랩을 전송할 수만 있고 이 호스트에서 찾아볼(폴링) 수는 없도록 지정합니다.
udp-port	(선택 사항) SNMP 트랩이 기본이 아닌 포트에서 NMS 호스트로 전송되도록 지정합니다.
username	호스트로 전송되는 트랩 PDU에 포함할 사용자 이름을 지정합니다. SNMP 버전 3에만 사용할 수 있습니다.
version {**1** | **2c** | **3**}	(선택 사항) SNMP 트랩 버전을 지정합니다. ASA에서는 SNMP 요청(폴링)을 기반으로 하는 필터링을 지원하지 않습니다.

기본값

기본 UDP 포트는 162입니다.

기본 버전은 1입니다.

SNMP 트랩은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
8.2(1)	• SNMP 버전 3이 지원됩니다. • *username* 인수가 도입되었습니다. • *text* 인수가 *community-string* 인수로 변경되었습니다. • *interface_name* 인수가 *interface* 인수로 변경되었습니다.
8.3(1)	암호화된 비밀번호에 대한 지원이 추가되었습니다.

사용 지침

현재 사용 중인 포트에서 **snmp-server host** 명령을 구성하는 경우 다음 메시지가 표시됩니다.

경고 **다른 기능에서 UDP 포트 *port*를 사용 중입니다. snmp-server listen-port 명령이 다른 포트를 사용하도록 구성될 때까지 해당 장비에 대한 SNMP 요청이 실패합니다.**

기존 SNMP 스레드는 포트를 사용할 수 있을 때까지 60초마다 계속 폴링하며, 포트를 여전히 사용 중인 경우 syslog 메시지 %ASA-1-212001을 생성합니다.

버전 3 보안 모델을 사용하려면 먼저 SNMP 그룹을 구성하고 SNMP 사용자를 구성한 다음 SNMP 호스트를 구성해야 합니다. 사용자 이름은 디바이스에 이미 구성되어 있어야 합니다. 디바이스가 대체작동 쌍의 대기 디바이스로 구성된 경우 SNMP 엔진 ID 및 사용자 컨피그레이션은 활성 디바이스에서 복제됩니다. 이 작업은 SNMP 버전 3 쿼리 관점에서 투명 모드한 전환을 허용합니다. NMS에서 컨피그레이션을 변경하지 않아도 전환 이벤트를 수용할 수 있습니다.

암호화된 커뮤니티 문자열을 사용한 후에는 암호화된 형식만 모든 시스템(예: CLI, ASDM, CSM 등)에 표시됩니다. 일반 텍스트 비밀번호는 표시되지 않습니다.

암호화된 커뮤니티 문자열은 항상 ASA에서 생성됩니다. 대개 입력 형식은 일반 텍스트 형식입니다.

ASA를 부팅하거나 업그레이드하는 과정에서 한 자리 비밀번호나 숫자로 시작하고 그 뒤에 공백이 있는 비밀번호는 더 이상 지원되지 않습니다. 예를 들어, 0 pass나 1은 유효하지 않은 비밀번호입니다.

참고 버전 8.3(1)에서 하위 버전의 ASA 소프트웨어로 다운그레이드하고 암호화된 비밀번호를 구성한 경우에는 먼저 **no key config-key password encryption** 명령을 사용하여 암호화된 비밀번호를 일반 텍스트로 변환한 다음 결과를 저장해야 합니다.

예

다음 예에서는 호스트를 내부 인터페이스에 연결되는 192.0.2.5로 설정합니다.

```
ciscoasa(config)# snmp-server host inside 192.0.2.5
ciscoasa(config)# snmp-server host inside 192.0.2.5 version 3 username user1 password
cisco123 mschap md5aes128 udp-port 190
```

다음 예에서는 ASA가 그룹 생성, 사용자 생성 및 호스트 생성을 포함하는 SNMP 버전 3 보안 모델을 사용하여 어떻게 SNMP 요청을 받을 수 있는지를 보여 줍니다.

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 username user1 password
cisco123 mschap priv admin
```

다음 예에서는 암호화된 커뮤니티 문자열을 사용하도록 호스트를 설정합니다.

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
username user1 password cisco123 mschap
```

다음 예에서는 암호화되지 않은 커뮤니티 문자열을 사용하도록 호스트를 설정합니다.

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 0 cisco username user1 password
cisco123 mschap
```

관련 명령

명령	설명
clear configure snmp-server	SNMP 컨피그레이션 카운터를 지웁니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server group	새 SNMP 그룹을 구성합니다.
snmp-server user	새 SNMP 사용자를 구성합니다.

snmp-server host-group

단일 사용자 또는 사용자 목록에 있는 사용자 그룹을 네트워크 개체와 연결하려면 글로벌 컨피그레이션 모드에서 **snmp-server host-group** 명령을 사용합니다. 연결을 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server host-group *interface-network-object-name* [**trap** | **poll**]
[**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}]
[**udp-port** *port*]

no snmp-server host-group *interface-network-object-name* [**trap** | **poll**]
[**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}]
[**udp-port** *port*]

구문 설명

community	NMS의 요청 또는 NMS로 전송되는 트랩 생성 시 기본이 아닌 문자열이 필요하도록 지정합니다. SNMP 버전 1 또는 2c에만 사용할 수 있습니다.
community-string	알림과 함께 전송되거나 NMS의 요청 시 전송되는 비밀번호 같은 커뮤니티 문자열을 지정합니다. 커뮤니티 문자열은 최대 32자까지 허용됩니다.
interface-network-object-name	사용자 또는 사용자 그룹을 연결할 인터페이스 네트워크 개체 이름을 지정합니다.
poll	(선택 사항) 호스트에서 찾아볼(폴링) 수는 있지만, 트랩을 전송할 수는 없도록 지정합니다.
udp-port *port*	(선택 사항) SNMP 트랩이 기본이 아닌 포트에서 NMS 호스트로 전송되도록 지정하고, NMS 호스트의 UDP 포트 번호를 설정합니다.
user-list *list_name*	사용자 목록의 이름을 지정합니다.
username	사용자의 이름을 지정합니다.
version {**1** | **2c** | **3**}	(선택 사항) 트랩 전송에 사용할 SNMP 알림 버전을 버전 1, 2c 또는 3으로 설정합니다.

기본값

기본 UDP 포트는 162입니다.

기본 버전은 1입니다.

SNMP 트랩은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

이제 호스트를 최대 4000개까지 추가할 수 있습니다. 지원되는 활성 폴링 대상 수는 128개입니다. 호스트 이름 또는 IP 주소 범위를 사용하여 호스트를 정의할 수 있습니다. 호스트 그룹으로 추가할 개별 호스트를 나타내는 네트워크 개체를 지정할 수 있습니다. 둘 이상의 사용자를 하나의 호스트와 연결할 수 있습니다.

SNMP 알림 버전 1 또는 2c를 사용하여 트랩을 전송하는 경우 단일 사용자를 네트워크 개체와 연결할 수 있습니다. SNMP 알림 버전 3을 사용하여 트랩을 전송하는 경우 단일 사용자 또는 사용자 그룹을 네트워크 개체와 연결할 수 있습니다. **snmp-server user-list** 명령을 사용하여 사용자 그룹을 생성할 수 있습니다. 사용자는 모든 그룹 컨피그레이션에 속할 수 있습니다.

SNMP 버전 3을 사용하는 경우 사용자 이름을 SNMP 호스트와 연결해야 합니다.

예

다음 예에서는 SNMP 알림 버전 1을 사용하여 단일 사용자를 네트워크 개체와 연결합니다.

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
```

다음 예에서는 SNMP 알림 버전 2c를 사용하여 단일 사용자를 네트워크 개체와 연결합니다.

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
```

다음 예에서는 SNMP 알림 버전 3을 사용하여 단일 사용자를 네트워크 개체와 연결합니다.

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
```

다음 예에서는 SNMP 알림 버전 3을 사용하여 사용자 목록을 네트워크 개체와 연결합니다.

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

관련 명령

명령	설명
clear configure snmp-server host-group	모든 SNMP 호스트 그룹 컨피그레이션을 지웁니다.
show running-config snmp-server host-group	SNMP 서버 호스트 그룹 컨피그레이션을 실행 중인 컨피그레이션에서 필터링합니다.

snmp-server listen-port

SNMP 요청의 수신 대기 포트를 설정하려면 글로벌 컨피그레이션 모드에서 **snmp-server listen-port** 명령을 사용합니다. 기본 포트를 복원하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

구문 설명

lport	들어오는 요청을 허용할 포트입니다[1].

1. **snmp-server listen-port** 명령은 관리 상황에서만 사용할 수 있으며, 시스템 상황에서는 사용할 수 없습니다.

기본값

기본 포트는 161입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

현재 사용 중인 포트에서 **snmp-server listen-port** 명령을 구성한 경우 다음 메시지가 표시됩니다.

경고 **다른 기능에서 UDP 포트 *port*를 사용 중입니다. snmp-server listen-port 명령이 다른 포트를 사용하도록 구성될 때까지 해당 장비에 대한 SNMP 요청이 실패합니다.**

기존 SNMP 스레드는 포트를 사용할 수 있을 때까지 60초마다 계속 폴링하며, 포트를 여전히 사용 중인 경우 syslog 메시지 %ASA-1-212001을 생성합니다.

예

다음 예에서는 수신 대기 포트를 192로 설정합니다.

```
ciscoasa(config)# snmp-server listen-port 192
```

관련 명령

명령	설명
snmp-server community	SNMP 커뮤니티 문자열을 설정합니다.
snmp-server contact	SNMP 연락처 이름을 설정합니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server enable traps	SNMP 트랩을 활성화합니다.
snmp-server location	SNMP 서버 위치 문자열을 설정합니다.

snmp-server location

SNMP에 대한 ASA 위치를 설정하려면 글로벌 컨피그레이션 모드에서 **snmp-server location** 명령을 사용합니다. 위치를 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server location *text*

no snmp-server location [*text*]

구문 설명

location *text*	보안 어플라이언스 위치를 지정합니다. **location** *text*는 대/소문자를 구분하며, 최대 127자까지 허용됩니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 SNMP에 대한 ASA 위치를 Building 42, Sector 54로 설정합니다.

```
ciscoasa(config)# snmp-server location Building 42, Sector 54
```

관련 명령

명령	설명
snmp-server community	SNMP 커뮤니티 문자열을 설정합니다.
snmp-server contact	SNMP 연락처 이름을 설정합니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server enable traps	SNMP 트랩을 활성화합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.

snmp-server user

새 SNMP 사용자를 구성하려면 글로벌 컨피그레이션 모드에서 **snmp-server user** 명령을 사용합니다. 지정된 SNMP 사용자를 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password*]} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password*]} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

구문 설명

128	(선택 사항) 암호화에 128비트 AES 알고리즘을 사용하도록 지정합니다.
192	(선택 사항) 암호화에 192비트 AES 알고리즘을 사용하도록 지정합니다.
256	(선택 사항) 암호화에 256비트 AES 알고리즘을 사용하도록 지정합니다.
3des	(선택 사항) 암호화에 168비트 3DES 알고리즘을 사용하도록 지정합니다.
aes	(선택 사항) 암호화에 AES 알고리즘을 사용하도록 지정합니다.
auth	(선택 사항) 사용할 인증 수준을 지정합니다.
auth-password	(선택 사항) 에이전트가 호스트로부터 패킷을 받을 수 있는 문자열을 지정합니다. 최소 길이는 1자입니다. 권장 길이는 8자 이상이며, 문자와 숫자를 포함해야 합니다. 최대 길이는 64자입니다. 일반 텍스트 비밀번호 또는 지역화된 MD5 다이제스트를 지정할 수 있습니다. 지역화된 MD5 또는 SHA 다이제스트가 있는 경우 일반 텍스트 비밀번호 대신 해당 문자열을 지정할 수 있습니다. 다이제스트는 aa:bb:cc:dd 형식이어야 합니다(여기서 aa, bb, cc는 16진수 값). 다이제스트는 정확히 16옥텟이어야 합니다.
des	(선택 사항) 암호화에 56비트 DES 알고리즘을 사용하도록 지정합니다.
encrypted	(선택 사항) 비밀번호가 암호화된 형식으로 표시되는지 여부를 지정합니다. 암호화된 비밀번호는 16진수 형식이어야 합니다.
group-name	사용자가 속한 그룹의 이름을 지정합니다.
md5	(선택 사항) HMAC-MD5-96 인증 수준을 지정합니다.
priv	암호화를 사용하는 패킷 인증을 지정합니다.
priv-password	(선택 사항) 개인정보 보호 사용자 비밀번호를 나타내는 문자열을 지정합니다. 최소 길이는 1자입니다. 권장 길이는 8자 이상이며, 문자와 숫자를 포함해야 합니다. 최대 길이는 64자입니다. 일반 텍스트 비밀번호 또는 지역화된 MD5 다이제스트를 지정할 수 있습니다. 지역화된 MD5 또는 SHA 다이제스트가 있는 경우 일반 텍스트 비밀번호 대신 해당 문자열을 지정할 수 있습니다. 다이제스트는 aa:bb:cc:dd 형식이어야 합니다(여기서 aa, bb, cc는 16진수 값). 다이제스트는 정확히 16옥텟이어야 합니다.
sha	(선택 사항) HMAC-SHA-96 인증 수준을 지정합니다.
username	에이전트에 연결된 호스트의 사용자 이름을 지정합니다.
v3	SNMP 버전 3 보안 모델을 사용하도록 지정합니다. **encrypted, priv** 또는 **auth** 키워드의 사용을 허용합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령이 도입되었습니다.

사용 지침

SNMP 사용자는 SNMP 그룹에 속해야 합니다. 버전 3 보안 모델을 사용하려면 먼저 SNMP 그룹을 구성하고 SNMP 사용자를 구성한 다음 SNMP 호스트를 구성해야 합니다.

참고 비밀번호를 잊어버린 경우에는 복구할 수 없으며 사용자를 다시 구성해야 합니다.

snmp-server user 컨피그레이션이 콘솔에 표시되거나 파일(예: startup-configuration 파일)로 작성된 경우 항상 일반 텍스트 비밀번호 대신 지역화된 인증 및 개인정보 보호 다이제스트가 표시됩니다. 이 사용은 RFC 3414, Section 11.2에 규정되어 있습니다.

참고 3DES 또는 AES 알고리즘으로 사용자를 구성하려면 3DES 또는 AES 기능 라이센스가 있어야 합니다.

ASA를 부팅하거나 업그레이드하는 과정에서 한 자리 비밀번호나 숫자로 시작하고 그 뒤에 공백이 있는 비밀번호는 더 이상 지원되지 않습니다. 예를 들어, 0 pass나 1은 유효하지 않은 비밀번호입니다.

클러스터링에서는 SNMPv3 사용자로 클러스터링된 각 ASA를 수동으로 업데이트해야 합니다. 마스터 디바이스에서 지역화되지 않은 해당 형식의 *priv-password* 옵션 및 *auth-password* 옵션과 함께 **snmp-server user** *username group-name* **v3** 명령을 입력하여 업데이트할 수 있습니다.

클러스터링 복제 또는 컨피그레이션 중에는 SNMPv3 사용자 명령이 복제되지 않음을 알리는 오류 메시지가 표시됩니다. 그런 다음 슬레이브 ASA에서 독립적으로 SNMPv3 사용자 및 그룹 명령을 구성할 수 있습니다. 이는 복제 중에 기존 SNMPv3 사용자 및 그룹이 지워지지 않으며, 클러스터의 모든 슬레이브에서 SNMPv3 사용자 및 그룹 명령을 입력할 수 있음도 의미합니다. 예를 들면 다음과 같습니다.

이미 지역화된 키와 함께 입력된 명령을 사용하는 마스터 장의 경우

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a priv aes 256
cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:f6:86:cf:18:c0:f0:47:d6:94:e5:
da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

클러스터 복제 중인 슬레이브 디바이스의 경우(**snmp-server user** 명령이 컨피그레이션에 있는 경우에만 표시됨)

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

예

다음 예에서는 ASA에서 SNMP 버전 3 보안 모델을 사용하는 SNMP 요청을 받을 수 있는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp-server group engineering v3 auth
ciscoasa(config)# snmp-server user engineering v3 auth sha mypassword
```

관련 명령

명령	설명
clear configure snmp-server	SNMP 서버 컨피그레이션을 지웁니다.
snmp-server enable	ASA에서 SNMP를 활성화합니다.
snmp-server group	새 SNMP 그룹을 생성합니다.
snmp-server host	SNMP 호스트 주소를 설정합니다.

snmp-server user-list

SNMP 사용자 목록을 해당 목록에 지정된 사용자 그룹으로 구성하려면 글로벌 컨피그레이션 모드에서 **snmp-server user-list** 명령을 사용합니다. 지정된 SNMP 사용자 목록을 제거하려면 이 명령의 **no** 형식을 사용합니다.

snmp-server user-list *list_name* **username** *user_name*

no snmp-server user-list *list_name* **username** *user_name*

구문 설명

list_name	사용자 목록의 이름을 지정합니다. 최대 33자까지 허용됩니다.
username *user_name*	사용자 목록에서 구성할 수 있는 사용자를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

snmp-server user *username* 명령을 사용하여 사용자 목록에서 사용자를 구성할 수 있습니다. 사용자 목록은 둘 이상의 사용자가 있어야 하며, 호스트 이름 또는 IP 주소 범위와 연결될 수 있습니다.

예

다음 예에서는 engineering이라는 사용자 목록에 대한 사용자 그룹을 만드는 방법을 보여 줍니다.

```
ciscoasa(config)# snmp-server user-list engineering username user1
ciscoasa(config)# snmp-server user-list engineering username user2
ciscoasa(config)# snmp-server user-list engineering username user3
ciscoasa(config)# snmp-server user-list engineering username user3
```

관련 명령

명령	설명
show running-config snmp-server user-list	실행 중인 컨피그레이션에서 SNMP 사용자 목록 컨피그레이션을 필터링합니다.
clear snmp-server user-list	SNMP 사용자 목록 컨피그레이션을 지웁니다.

16 장

software authenticity development through storage-objects 명령

software-version

서버 또는 엔드포인트의 소프트웨어 버전을 표시하는 Server 및 User-Agent 헤더 필드를 식별하려면 파라미터 컨피그레이션 모드에서 **software-version** 명령을 사용합니다. 파라미터 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

software-version action {mask | log} [log]

no software-version action {mask | log} [log]

구문 설명

log	위반 시 독립형 또는 추가 로그를 지정합니다.
mask	SIP 메시지에서 소프트웨어 버전을 마스킹합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
파라미터 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예에서는 SIP 검사 정책 맵에서 소프트웨어 버전을 식별하는 방법을 보여 줍니다.

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# software-version action log
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	계층 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

speed

구리(RJ-45) 이더넷 인터페이스의 속도를 설정하려면 인터페이스 컨피그레이션 모드에서 **speed** 명령을 사용합니다. 이 속도 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

no speed [**auto** | **10** | **100** | **1000** | **nonegotiate**]

구문 설명

10	속도를 10BASE-T로 설정합니다.
100	속도를 100BASE-T로 설정합니다.
1000	속도를 1000BASE-T로 설정합니다. 구리 기가비트 이더넷에만 해당됩니다.
auto	속도를 자동으로 감지합니다.
nonegotiate	파이버 인터페이스의 경우 속도를 1000Mbps로 설정하고 링크 파라미터를 협상하지 않습니다. 이 명령과 이 명령의 **no** 형식은 파이버 인터페이스에만 사용할 수 있는 설정입니다. 값을 **no speed nonegotiate**(기본값)로 설정하면 인터페이스에서 흐름 제어 파라미터 및 원격 장애 정보를 교환하는 링크 협상을 활성화합니다.

기본값

구리 인터페이스의 경우 기본값은 **speed auto**입니다.

파이버 인터페이스의 경우 기본값은 **no speed nonegotiate**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령은 **interface** 명령 키워드에서 인터페이스 컨피그레이션 모드 명령으로 이동되었습니다.

사용 지침

실제 인터페이스의 속도만 설정합니다.

네트워크에서 자동 감지를 지원하지 않는 경우 속도를 특정 값으로 설정합니다.

ASA 5500 Series RJ-45 인터페이스의 경우 기본 자동 협상 설정에 자동 MDI/MDIX 기능도 포함됩니다. 자동 MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 자동 MDI/MDIX를 사용하려면 속도 또는 이중을 자동 협상하도록 설정해야 합니다. 속도와 이중을 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 비활성화하면 자동 MDI/MDIX도 비활성화됩니다.

PoE 포트에서 속도를 **auto** 이외의 값으로 설정한 경우에는 IEEE 802.3af를 지원하지 않는 Cisco IP Phone 및 Cisco 무선 액세스 포인트가 감지되지 않고 전원이 공급되지 않습니다.

참고 파이버 인터페이스를 사용하는 ASA 5500x Series 또는 ASA 5585에 대해 **speed** 명령을 설정하지 마십시오. 이 명령을 설정하면 링크 장애가 발생합니다.

예

다음 예에서는 속도를 1000BASE-T로 설정합니다.

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

관련 명령

명령	설명
clear configure interface	인터페이스에 대한 모든 컨피그레이션을 지웁니다.
duplex	이중 모드를 설정합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show running-config interface	인터페이스 컨피그레이션을 표시합니다.

split-dns

스플릿 터널을 통해 확인할 도메인 목록을 입력하려면 group-policy 컨피그레이션 모드에서 **split-dns** 명령을 사용합니다. 목록을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

모든 스플릿 터널링 도메인 목록을 삭제하려면 인수 없이 **no split-dns** 명령을 사용합니다. 그러면 **split-dns none** 명령을 실행하여 만든 null 목록을 포함하여 구성된 모든 스플릿 터널링 도메인 목록이 삭제됩니다.

스플릿 터널링 도메인 목록이 없는 경우 사용자는 기본 그룹 정책에 있는 항목을 상속합니다. 사용자가 이러한 스플릿 터널링 도메인 목록을 상속하지 못하도록 하려면 **split-dns none** 명령을 사용합니다.

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

구문 설명

value *domain-name*	ASA가 스플릿 터널을 통해 확인하는 도메인 이름을 제공합니다.
none	스플릿 DNS 목록이 없음을 나타냅니다. 스플릿 DNS 목록을 null 값으로 설정하면 스플릿 DNS 목록이 허용되지 않습니다. 기본 또는 지정된 그룹 정책에서 스플릿 DNS 목록을 상속하지 못하도록 합니다.

기본값

스플릿 DNS가 비활성화됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

단일 공백을 사용하여 도메인 목록에서 각 항목을 구분합니다. 항목 수에 대한 제한은 없지만 전체 문자열이 255자를 초과할 수 없습니다. 영숫자 문자, 하이픈(-) 및 마침표(.)만 사용할 수 있습니다.

인수 없이 **no split-dns** 명령을 사용하면 **split-dns none** 명령을 통해 생성된 null 값을 포함하여 모든 현재 값이 삭제됩니다.

버전 3.0.4235부터 AnyConnect Secure Mobility Client는 Windows 플랫폼을 위한 진정한 스플릿 DNS 기능을 지원합니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 스플릿 터널링을 통해 확인할 도메인 Domain1, Domain2, Domain3 및 Domain4를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

관련 명령

명령	설명
default-domain	IPsec 클라이언트에서 도메인 필드를 생략하는 DNS 쿼리에 사용하는 기본 도메인 이름을 지정합니다.
split-dns	스플릿 터널을 통해 확인할 도메인 목록을 제공합니다.
split-tunnel-network-list	ASA에서 터널링이 필요한 네트워크를 구별하는 데 사용하는 액세스 목록을 식별합니다.
split-tunnel-policy	IPsec 클라이언트가 IPsec 터널을 통해 암호화된 형식으로 또는 네트워크 인터페이스에 일반 텍스트 형식으로 패킷을 조건부로 전달할 수 있도록 합니다.

split-horizon

EIGRP 스플릿 호라이즌을 재활성화하려면 인터페이스 컨피그레이션 모드에서 **split-horizon** 명령을 사용합니다. EIGRP 스플릿 호라이즌을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

split-horizon eigrp *as-number*

no split-horizon eigrp *as-number*

구문 설명

as-number	EIGRP 라우팅 프로세스의 자동 시스템 번호입니다.

기본값

split-horizon 명령이 활성화됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

X.25 패킷 교환 네트워크를 통한 링크가 포함된 네트워크의 경우 **neighbor** 명령을 사용하여 스플릿 호라이즌 기능을 해제할 수 있습니다. 또는 컨피그레이션에서 **no split-horizon eigrp** 명령을 명시적으로 지정할 수 있습니다. 그러나 이 경우 해당 네트워크의 모든 관련 멀티캐스트 그룹에 있는 모든 라우터 및 액세스 서버에 대해서도 스플릿 호라이즌을 비활성화해야 합니다.

일반적으로 경로를 올바르게 알리기 위해 애플리케이션에서 변경할 필요가 있다고 확신하는 경우 외에는 스플릿 호라이즌의 기본 상태를 변경하지 않는 것이 좋습니다. 스플릿 호라이즌이 직렬 인터페이스에서 비활성화되어 있고 해당 인터페이스가 패킷 교환 네트워크에 연결된 경우 해당 네트워크의 모든 관련 멀티캐스트 그룹에 있는 모든 라우터 및 액세스 서버에 대해 스플릿 호라이즌을 비활성화해야 합니다.

예

다음 예에서는 Ethernet0/0 인터페이스에서 EIGRP 스플릿 호라이즌을 비활성화합니다.

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# no split-horizon eigrp 100
```

관련 명령

명령	설명
router eigrp	EIGRP 라우팅 프로세스를 만들고 해당 프로세스에 대한 컨피그레이션 모드를 시작합니다.

split-tunnel-all-dns

AnyConnect Secure Mobility Client가 VPN 터널을 통해 모든 DNS 주소를 확인할 수 있도록 하려면 그룹 정책 컨피그레이션 모드에서 **split-tunnel-all-dns** 명령을 사용합니다.

실행 중인 컨피그레이션에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다. 그러면 다른 그룹 정책에서 값이 상속됩니다.

split-tunnel-all-dns {disable | enable}

no split-tunnel-all-dns [{disable | enable}]

구문 설명

disable(기본값)	AnyConnect 클라이언트는 스플릿 터널 정책(모든 네트워크 터널링, 네트워크 목록에 지정된 네트워크 터널링 또는 네트워크 목록에 지정된 네트워크 제외)에 따라 터널을 통해 DNS 쿼리를 보냅니다.
enable	AnyConnect 클라이언트가 VPN 터널을 통해 모든 DNS 주소를 확인합니다.

기본값

기본값은 비활성화입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.2(5)	이 명령이 도입되었습니다.

사용 지침

split-tunnel-all-dns enable 명령은 SSL 또는 IPsec/IKEv2 프로토콜을 사용하는 VPN 연결에 적용되며, AnyConnect 클라이언트에 VPN 터널을 통해 모든 DNS 주소를 확인하도록 지시합니다. DNS 확인이 실패하면 주소가 미확인 상태로 남아 있고 AnyConnect 클라이언트는 공용 DNS 서버를 통해 주소를 확인하지 않습니다.

기본적으로 이 기능은 비활성화됩니다. 클라이언트는 스플릿 터널 정책(모든 네트워크 터널링, 네트워크 목록에 지정된 네트워크 터널링 또는 네트워크 목록에 지정된 네트워크 제외)에 따라 터널을 통해 DNS 쿼리를 보냅니다.

예

다음 예에서는 AnyConnect 클라이언트가 VPN 터널을 통해 모든 DNS 쿼리를 확인할 수 있게 지원하도록 ASA를 구성합니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-all-dns enable
```

관련 명령

명령	설명
default-domain	레거시 IPsec(IKEv1) VPN 클라이언트 또는 AnyConnect VPN 클라이언트(SSL)가 도메인 필드가 생략된 DNS 쿼리에 사용하는 기본 도메인 이름을 지정합니다.
split-dns	스플릿 터널을 통해 확인할 도메인 목록을 제공합니다.
split-tunnel-network-list	ASA가 터널링이 필요한 네트워크와 터널링이 필요 없는 네트워크를 구별하는 데 사용하는 액세스 목록을 식별합니다.
split-tunnel-policy	레거시 IPsec(IKEv1) VPN 클라이언트 또는 AnyConnect VPN 클라이언트(SSL)가 터널을 통해 암호화된 형식으로 또는 네트워크 인터페이스에 일반 텍스트 형식으로 패킷을 조건부로 전달할 수 있도록 합니다.

split-tunnel-network-list

스플릿 터널링을 위한 네트워크 목록을 생성하려면 group-policy 컨피그레이션 모드에서 **split-tunnel-network-list** 명령을 사용합니다. 네트워크 목록을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

모든 스플릿 터널링 네트워크 목록을 삭제하려면 인수 없이 **no split-tunnel-network-list** 명령을 사용합니다. 그러면 **split-tunnel-network-list none** 명령을 실행하여 만든 null 목록을 포함하여 구성된 모든 네트워크 목록이 삭제됩니다.

스플릿 터널링 네트워크 목록이 없는 경우 사용자는 기본 또는 지정된 그룹 정책에 있는 네트워크 목록을 상속합니다. 사용자가 이러한 네트워크 목록을 상속하지 못하도록 하려면 **split-tunnel-network-list none** 명령을 사용합니다.

스플릿 터널링 네트워크 목록은 터널을 통해 트래픽을 전달해야 하는 네트워크와 터널링이 필요 없는 네트워크를 구별합니다.

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

구문 설명

none	스플릿 터널링을 위한 네트워크 목록이 없음을 나타냅니다. 이 경우 ASA에서 모든 트래픽을 터널링합니다. 따라서 스플릿 터널링을 허용하지 않도록 스플릿 터널링 네트워크 목록을 null 값으로 설정합니다. 기본 또는 지정된 그룹 정책에서 기본 스플릿 터널링 네트워크 목록을 상속하지 못하도록 합니다.
value *access-list name*	터널링하거나 터널링하지 않을 네트워크를 열거하는 액세스 목록을 식별합니다.

기본값

기본적으로 스플릿 터널링 네트워크 목록은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

ASA는 사설 네트워크의 주소 목록으로 구성된 표준 ACL인 네트워크 목록을 기반으로 스플릿 터널링을 결정합니다.

인수 없이 **no split-tunnel-network-list** 명령을 사용하면 **split-tunnel-network-list none** 명령을 통해 생성된 null 값을 포함하여 모든 현재 네트워크 값이 삭제됩니다.

참고 ASA 는 200 개의 스플릿 네트워크를 지원합니다 .

예

다음 예에서는 FirstGroup라는 그룹 정책에 대해 FirstList라는 네트워크 목록을 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-network-list FirstList
```

관련 명령

명령	설명
access-list	액세스 목록을 생성하거나 다운로드 가능한 액세스 목록을 사용합니다.
default-domain	IPsec 클라이언트에서 도메인 필드를 생략하는 DNS 쿼리에 사용하는 기본 도메인 이름을 지정합니다.
split-dns	스플릿 터널을 통해 확인할 도메인 목록을 제공합니다.
split-tunnel-policy	IPsec 클라이언트가 IPsec 터널을 통해 암호화된 형식으로 또는 네트워크 인터페이스에 일반 텍스트 형식으로 패킷을 조건부로 전달할 수 있도록 합니다.

split-tunnel-policy

스플릿 터널링 정책을 설정하려면 group-policy 컨피그레이션 모드에서 **split-tunnel-policy** 명령을 사용합니다. 실행 중인 컨피그레이션에서 split-tunnel-policy 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

구문 설명

excludespecified	트래픽이 암호화되지 않고 이동하는 네트워크 목록을 정의합니다. 이 기능은 프린터처럼 로컬 네트워크에 있지만 터널을 통해 회사 네트워크에 연결된 디바이스에 액세스하려는 원격 사용자에게 유용합니다.
split-tunnel-policy	터널링 트래픽에 대한 규칙을 설정함을 나타냅니다.
tunnelall	트래픽이 암호화되지 않고 이동할 수 없도록 또는 ASA 이외의 다른 대상으로 이동할 수 없도록 지정합니다. 원격 사용자는 회사 네트워크를 통해 인터넷 네트워크에 연결하며, 로컬 네트워크에 액세스할 권한은 없습니다.
tunnelspecified	지정된 네트워크로 들어오고 나가는 모든 트래픽을 터널링합니다. 이 옵션은 스플릿 터널링을 활성화합니다. 터널링할 주소의 네트워크 목록을 작성할 수 있습니다. 암호화되지 않은 상태로 그 외의 모든 다른 주소로 보내는 데이터는 원격 사용자의 인터넷 서비스 공급자를 통해 라우팅됩니다.

기본값

스플릿 터널링은 기본적으로 비활성화되어 있습니다(**tunnelall**).

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

스플릿 터널링은 주로 보안 기능이 아닌 트래픽 관리 기능입니다. 최적의 보안을 유지하기 위해 스플릿 터널링을 사용하지 않는 것이 좋습니다.

이렇게 하면 다른 그룹 정책에서 스플릿 터널링 값이 상속됩니다.

스플릿 터널링은 원격 액세스 VPN 클라이언트가 IPsec 또는 SSL 터널을 통해 암호화된 형식으로 또는 네트워크 인터페이스에 일반 텍스트 형식으로 패킷을 조건부로 전달할 수 있도록 합니다. 스플릿 터널링이 활성화된 경우 IPsec 또는 SSL VPN 터널 엔드포인트의 다른 쪽에 있는 대상에 바인딩되지 않은 패킷은 암호화하여 터널을 통해 전송한 다음 암호를 해독하고 최종 대상으로 라우팅할 필요가 없습니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 지정된 네트워크만 터널링하는 스플릿 터널링 정책을 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
```

관련 명령

명령	설명
default-domain	IPsec 클라이언트에서 도메인 필드를 생략하는 DNS 쿼리에 사용하는 기본 도메인 이름을 지정합니다.
split-dns	스플릿 터널을 통해 확인할 도메인 목록을 제공합니다.
split-tunnel-network-list none	스플릿 터널링에 대한 액세스 목록이 없음을 나타냅니다. 모든 트래픽이 터널을 통해 이동합니다.
split-tunnel-network-list value	ASA가 터널링이 필요한 네트워크와 터널링이 필요 없는 네트워크를 구별하는 데 사용하는 액세스 목록을 식별합니다.

spoof-server

HTTP 프로토콜 검사를 위해 서버 헤더 필드의 문자열로 대체하려면 파라미터 컨피그레이션 모드에서 **spoof-server** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

spoof-server *string*

no spoof-server *string*

구문 설명

string	서버 헤더 필드를 대체할 문자열입니다. 최대 82자입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
파라미터 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

WebVPN 스트림에는 **spoof-server** 명령이 적용되지 않습니다.

예

다음 예에서는 HTTP 검사 정책 맵의 서버 헤더 필드에 대한 문자열을 대체하는 방법을 보여 줍니다.

```
ciscoasa(config-pmap-p)# spoof-server string
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	계층 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

sq-period

NAC 프레임워크 세션에서 성공한 각 상태 검증과 호스트 상태 변경에 대한 다음 쿼리 간의 간격을 지정하려면 nac-policy-nac-framework 컨피그레이션 모드에서 **sq-period** 명령을 사용합니다. NAC 정책에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

sq-period *seconds*

no sq-period [*seconds*]

구문 설명

seconds	성공한 각 상태 검증 간의 시간 간격(초)입니다. 범위는 30~1800입니다.

기본값

기본값은 300입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
nac-policy-nac-framework 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.3(0)	명령 이름에서 “nac-”가 제거되었습니다. 명령이 group-policy 컨피그레이션 모드에서 nac-policy-nac-framework 컨피그레이션 모드로 이동되었습니다.
7.2(1)	이 명령이 도입되었습니다.

사용 지침

ASA에서는 상태 검증 및 상태 쿼리 응답에 성공할 때마다 상태 쿼리 타이머를 시작합니다. 이 타이머가 만료되면 호스트 상태 변경 쿼리가 트리거되며, 이를 *상태 쿼리*라고 합니다.

예

다음 예에서는 상태 쿼리 타이머 값을 1800초로 변경합니다.

```
ciscoasa(config-nac-policy-nac-framework)# sq-period 1800
ciscoasa(config-nac-policy-nac-framework)
```

다음 예에서는 NAC 프레임워크 정책에서 상태 쿼리 타이머를 제거합니다.

```
ciscoasa(config-nac-policy-nac-framework)# no sq-period
ciscoasa(config-nac-policy-nac-framework)
```

관련 명령

명령	설명
nac-policy	Cisco NAC 정책을 만들고 액세스하여 해당 유형을 지정합니다.
nac-settings	그룹 정책에 NAC 정책을 할당합니다.
eou timeout	NAC 프레임워크 컨피그레이션의 원격 호스트로 EAP over UDP 메시지를 보낸 후 대기할 시간(초)을 변경합니다.
reval-period	NAC 프레임워크 세션에서 성공한 각 상태 검증과 호스트 상태 변경에 대한 다음 쿼리 간의 간격을 지정합니다.
debug eap	NAC 프레임워크 메시징을 디버그하기 위해 EAP(Extensible Authentication Protocol: 확장 가능 인증 프로토콜) 이벤트 기록을 활성화합니다.

ssh

SSH 액세스를 ASA에 추가하려면 글로벌 컨피그레이션 모드에서 **ssh** 명령을 사용합니다. ASA에 대한 SSH 액세스를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

구문 설명

interface	SSH가 활성화된 ASA 인터페이스입니다. 지정하지 않으면 외부 인터페이스를 제외하고 모든 인터페이스에서 SSH가 활성화됩니다.
ip_address	ASA에 대한 SSH 연결을 시작할 수 있는 호스트 또는 네트워크의 IPv4 주소입니다. 호스트의 경우 호스트 이름을 입력할 수도 있습니다.
ipv6_address/*prefix*	ASA에 대한 SSH 연결을 시작할 수 있는 호스트 또는 네트워크의 IPv6 주소 및 접두사입니다.
mask	*ip_address*에 대한 네트워크 마스크입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 IPv4 및 IPv6 주소를 지원합니다. **ssh** *ip_address* 명령은 ASA에 대한 SSH 연결을 시작할 수 있는 호스트 또는 네트워크를 지정합니다. 컨피그레이션에서 여러 ssh 명령을 사용할 수 있습니다. 이 명령의 **no** 형식은 특정 SSH 명령을 컨피그레이션에서 제거합니다. 모든 SSH 명령을 제거하려면 **clear configure ssh** 명령을 사용합니다.

ASA에 대한 SSH 사용을 시작하려면 먼저 **crypto key generate rsa** 명령을 사용하여 기본 RSA 키를 생성해야 합니다.

ASA에서 지원되는 보안 알고리즘 및 암호는 다음과 같습니다.

- 3DES 및 AES 암호 - 데이터 암호화
- HMAC-SHA 및 HMAC-MD5 알고리즘 - 패킷 무결성
- RSA 공개 키 알고리즘 - 호스트 인증

다음 SSH 버전 2 기능은 ASA에서 지원되지 않습니다.

- X11 전달
- 포트 포워딩
- SFTP 지원
- Kerberos 및 AFS 티켓 전달
- 데이터 압축

예

다음 예에서는 IP 주소가 10.1.1.1인 관리 콘솔에서의 SSH 버전 2 연결을 허용하도록 내부 인터페이스를 구성하는 방법을 보여 줍니다. 유휴 세션 시간 제한은 60분으로 설정되어 있으며, SCP가 활성화되어 있습니다.

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh scopy enable
ciscoasa(config)# ssh timeout 60
```

관련 명령

명령	설명
clear configure ssh	실행 중인 컨피그레이션에서 모든 SSH 명령을 지웁니다.
crypto key generate rsa	ID 인증서에 대한 RSA 키 쌍을 생성합니다.
debug ssh	SSH 명령에 대한 디버깅 정보 및 오류 메시지를 표시합니다.
show running-config ssh	실행 중인 컨피그레이션의 현재 SSH 명령을 표시합니다.
ssh scopy enable	ASA에서 SCP(Secure Copy) 서버를 활성화합니다.
ssh version	SSH 버전 1 또는 SSH 버전 2를 사용하도록 ASA를 제한합니다.

ssh authentication

사용자 단위로 공개 키 인증을 활성화하려면 username 특성 모드에서 **ssh authentication** 명령을 사용합니다. 사용자 단위로 공개 키 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ssh authentication {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

no ssh authentication {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

구문 설명

hashed	각 바이트를 콜론으로 구분(구문 분석을 위해)하여 SHA-256 및 32바이트 길이로 해시되었습니다.
key	*key* 인수 값은 다음 중 하나일 수 있습니다. • *key* 인수를 제공하고 해시된 태그를 지정하지 않은 경우 키 값은 SSH-RSA 원시 키(즉, 인증서가 없음)를 생성할 수 있는 SSH 키 생성 소프트웨어에서 생성된 Base 64로 인코딩된 공개 키여야 합니다. Base 64로 인코딩된 공개 키를 전송하면 이 키는 SHA-256을 통해 해시되며, 해당 32바이트 해시가 모든 추가 비교에 사용됩니다. • *key* 인수를 제공하고 해시된 태그를 지정한 경우 키 값은 이전에 SHA-256으로 해시되고 길이가 32바이트이며, 각 바이트가 콜론으로 구분(구문 분석을 위해)되어 있습니다.
nointeractive	**nointeractive** 옵션은 SSH 공개 키 파일 형식의 키를 가져올 때 모든 프롬프트를 표시하지 않도록 설정합니다. 이 비대화형 데이터 입력 모드는 ASDM 전용으로 제공됩니다.
pkf	**pkf** 키의 경우 PKF 형식의 키에 붙여넣으라는 메시지가 표시됩니다(최대 4096비트). 너무 커서 Base64 형식으로 인라인으로 붙여넣을 수 없는 키에 이 형식을 사용합니다. 예를 들어 ssh keygen을 사용하여 4096비트를 생성하여 PKF로 변환한 다음 **pkf** 키워드를 사용하여 해당 키에 대한 메시지를 표시할 수 있습니다. **참고** 대체작동에서 **pkf** 옵션을 사용할 수 있지만 PKF 키가 대기 시스템에 자동으로 복제되지는 않습니다. **write standby** 명령을 입력하여 PKF 키를 동기화해야 합니다.
publickey	**publickey**의 경우 *key*는 Base64로 인코딩된 공개 키입니다. SSH-RSA 원시 키(즉, 인증서가 없음)를 생성할 수 있는 SSH 키 생성 소프트웨어(예: ssh keygen)를 사용하여 키를 생성할 수 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
username 특성	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.1(2)	이 명령이 도입되었습니다.

사용 지침

PKF(공개 키 파일) 형식의 키(**pkf** 키워드) 또는 Base64 키(**publickey** 키워드)를 지정할 수 있습니다.

key 필드와 **hashed** 키워드는 **publickey** 옵션에서만 사용할 수 있으며, **nointeractive** 키워드는 **pkf** 옵션에서만 사용할 수 있습니다.

컨피그레이션을 저장하면 해시된 키 값이 컨피그레이션에 저장되며 ASA가 재부팅될 때 사용됩니다.

show running-config username 명령을 사용하여 ASA에서 키를 확인하는 경우 키는 SHA-256 해시를 통해 암호화됩니다. 키를 **pkf**로 입력한 경우에도 ASA는 키를 해시하여 해시된 **publickey**로 표시합니다. **show** 출력에서 키를 복사해야 하는 경우 **hashed** 키워드를 사용하여 **publickey** 유형을 지정합니다.

예

다음 예에서는 PKF 형식의 키를 사용하여 인증하는 방법을 보여 줍니다.

```
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)
```

관련 명령

명령	설명
clear configure ssh	실행 중인 컨피그레이션에서 모든 SSH 명령을 지웁니다.
debug ssh	SSH 명령에 대한 디버깅 정보 및 오류 메시지를 표시합니다.
show running-config ssh	실행 중인 컨피그레이션의 현재 SSH 명령을 표시합니다.
ssh version	SSH 버전 1 또는 SSH 버전 2를 사용하도록 ASA를 제한합니다.

ssh disconnect

활성 SSH 세션의 연결을 해제하려면 특권 EXEC 모드에서 **ssh disconnect** 명령을 사용합니다.

ssh disconnect *session_id*

구문 설명

session_id	ID 번호로 지정된 SSH 세션의 연결을 해제합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

세션 ID를 지정해야 합니다. **show ssh sessions** 명령을 사용하여 연결을 해제할 SSH 세션의 ID를 가져올 수 있습니다.

예

다음 예에서는 SSH 세션의 연결을 해제하는 방법을 보여 줍니다.

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
ciscoasa# ssh disconnect 2
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

관련 명령

명령	설명
show ssh sessions	ASA의 활성 SSH 세션에 대한 정보를 표시합니다.
ssh timeout	유휴 SSH 세션에 대한 시간 제한 값을 설정합니다.

ssh key-exchange

Diffie-Hellman(DH) 그룹 1 또는 DH 그룹 14 키 교환 방법을 사용하여 키를 교환하려면 글로벌 컨피그레이션 모드에서 **ssh key-exchange** 명령을 사용합니다. DH 그룹 1 또는 DH 그룹 14 키 교환 방법을 사용한 키 교환을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ssh key-exchange group {**dh-group1** | **dh-group14**} **sha1**

no ssh key-exchange group {**dh-group1** | **dh-group14**} **sha1**

구문 설명

dh-group1	키를 교환할 때 DH 그룹 1 키 교환 방법을 따르고 사용해야 함을 나타냅니다. DH 그룹 2는 레거시 요인으로 인해 그룹 1이라고 합니다.
dh-group14	키를 교환할 때 DH 그룹 14 키 교환 방법을 따르고 사용해야 함을 나타냅니다.
group	키를 교환할 때 DH 그룹 1 키 교환 방법 또는 DH 그룹 14 키 교환 방법을 따르고 사용해야 함을 나타냅니다.
key-exchange	키를 교환할 때 DH 그룹 1 또는 DH 그룹 14 키 교환 방법을 따르고 사용하도록 지정합니다.
sha-1	SHA-1 암호화 알고리즘을 사용해야 하도록 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(4)	이 명령이 도입되었습니다.
9.1(2)	이 명령은 **ssh key-exchange group dh-group1-sha1**로 변경되었습니다.

사용 지침

ASA에 대한 SSH 사용을 시작하려면 먼저 **crypto key generate rsa** 명령을 사용하여 기본 RSA 키를 생성해야 합니다.

ASA에서는 DH 그룹 1 및 그룹 14 키 교환 방법이 키 교환에 모두 지원됩니다. DH 그룹 키 교환 방법을 지정하지 않으면 DH 그룹 1 키 교환 방법이 사용됩니다. DH 키 교환 방법 사용에 대한 자세한 내용은 RFC 4253을 참고하십시오.

참고 9.1(1) 또는 9.1.1(2) 릴리스에서는 이 명령을 사용할 수 없습니다.

예

다음 예에서는 DH 그룹 14 키 교환 방법을 사용하여 키를 교환하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssh key-exchange dh-group-1-sha1
```

관련 명령

명령	설명
clear configure ssh	실행 중인 컨피그레이션에서 모든 SSH 명령을 지웁니다.
crypto key generate rsa	ID 인증서에 대한 RSA 키 쌍을 생성합니다.
debug ssh	SSH 명령에 대한 디버깅 정보 및 오류 메시지를 표시합니다.
show running-config ssh	실행 중인 컨피그레이션의 현재 SSH 명령을 표시합니다.
ssh scopy enable	ASA에서 SCP(Secure Copy) 서버를 활성화합니다.
ssh version	SSH 버전 1 또는 SSH 버전 2를 사용하도록 ASA를 제한합니다.

ssh pubkey-chain

ASA 데이터베이스에서 온보드 SCP(Secure Copy) 클라이언트에 대한 SSH 서버 및 해당 키를 수동으로 추가하거나 삭제하려면 글로벌 컨피그레이션 모드에서 **ssh pubkey-chain** 명령을 사용합니다. 모든 호스트 키를 제거하려면 이 명령의 **no** 형식을 사용합니다. 단일 서버 키만 제거하려면 **server** 명령을 참고하십시오.

ssh pubkey-chain

no ssh pubkey-chain

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.1(5)	이 명령이 도입되었습니다.

사용 지침

온보드 SCP 클라이언트를 사용하여 ASA와 파일을 서로 복사할 수 있습니다. ASA는 연결한 각 SCP 서버에 대한 SSH 호스트 키를 저장합니다. 원하는 경우 서버와 해당 키를 ASA 데이터베이스에서 수동으로 추가하거나 삭제할 수 있습니다.

각 서버(**server** 명령 참고)에 대해 SSH 호스트의 **key-string**(공개 키) 또는 **key-hash**(해시 값)를 지정할 수 있습니다.

예

다음 예에서는 10.86.94.170에서 서버의 이미 해시된 호스트 키를 추가합니다.

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

다음 예에서는 10.7.8.9에서 서버의 호스트 문자열을 추가합니다.

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

관련 명령

명령	설명
copy	ASA와 파일을 서로 복사합니다.
key-hash	해시된 SSH 호스트 키를 입력합니다.
key-string	공개 SSH 호스트 키를 입력합니다.
server	ASA 데이터베이스에 SSH 서버 및 호스트 키를 추가합니다.
ssh stricthostkeycheck	온보드 SCP(Secure Copy) 클라이언트에 대한 SSH 호스트 키 확인을 활성화합니다.

ssh scopy enable

ASA에서 SCP(Secure Copy)를 활성화하려면 글로벌 컨피그레이션 모드에서 **ssh scopy enable** 명령을 사용합니다. SCP를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ssh scopy enable

no ssh scopy enable

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

SCP는 서버 전용 구현입니다. SCP에 대한 연결을 허용하고 종료할 수 있지만 시작할 수는 없습니다. ASA에는 다음과 같은 제한 사항이 있습니다.

- 이 SCP 구현에서는 디렉토리가 지원되지 않으므로 원격 클라이언트 액세스가 ASA 내부 파일로 제한됩니다.
- SCP를 사용할 때 배너가 지원되지 않습니다.
- SCP는 와일드카드를 지원하지 않습니다.
- SSH 버전 2 연결을 지원하려면 ASA 라이센스에 VPN-3DES-AES 기능이 있어야 합니다.

파일 전송을 시작하기 전에 ASA에서 사용 가능한 플래시 메모리를 확인합니다. 사용 가능한 공간이 부족한 경우 ASA는 SCP 연결을 종료합니다. 플래시 메모리의 파일을 덮어쓰는 경우 여전히 ASA에 파일을 복사할 여유 공간이 있어야 합니다. SCP 프로세스는 먼저 파일을 임시 파일에 복사한 다음 대체할 파일에 임시 파일을 복사합니다. 플래시의 공간이 부족해 파일 복사 및 파일 덮어쓰기를 지속할 수 없는 경우 ASA는 SCP 연결을 종료합니다.

예

다음 예에서는 IP 주소가 10.1.1.1인 관리 콘솔에서의 SSH 버전 2 연결을 허용하도록 내부 인터페이스를 구성하는 방법을 보여 줍니다. 유휴 세션 시간 제한은 60분으로 설정되어 있으며, SCP가 활성화되어 있습니다.

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh scopy enable
ciscoasa(config)# ssh timeout 60
```

관련 명령

명령	설명
clear configure ssh	실행 중인 컨피그레이션에서 모든 SSH 명령을 지웁니다.
debug ssh	SSH 명령에 대한 디버그 정보 및 오류 메시지를 표시합니다.
show running-config ssh	실행 중인 컨피그레이션의 현재 SSH 명령을 표시합니다.
ssh	ASA에 대한 지정된 클라이언트 또는 네트워크의 SSH 연결을 허용합니다.
ssh version	SSH 버전 1 또는 SSH 버전 2를 사용하도록 ASA를 제한합니다.

ssh stricthostkeycheck

온보드 SCP(Secure Copy) 클라이언트에 대한 SSH 호스트 키 확인을 활성화하려면 글로벌 컨피그레이션 모드에서 **ssh stricthostkeycheck** 명령을 사용합니다. 호스트 키 확인을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ssh stricthostkeycheck

no ssh stricthostkeycheck

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본적으로 이 명령은 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.1(5)	이 명령이 도입되었습니다.

사용 지침

온보드 SCP 클라이언트를 사용하여 ASA와 파일을 서로 복사할 수 있습니다. 이 옵션을 활성화하면 호스트 키를 허용할지 또는 거부할지 묻는 메시지가 표시됩니다(ASA에 이미 저장되지 않은 경우). 이 옵션을 비활성화하면 ASA에서 호스트 키를 자동으로 허용합니다(이전에 저장되지 않은 경우).

예

다음 예에서는 SSH 호스트 키 확인을 활성화합니다.

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

관련 명령

명령	설명
copy	ASA와 파일을 서로 복사합니다.
key-hash	해시된 SSH 호스트 키를 입력합니다.
key-string	공개 SSH 호스트 키를 입력합니다.
서버	ASA 데이터베이스에 SSH 서버 및 호스트 키를 추가합니다.
ssh pubkey-chain	서버와 해당 키를 ASA 데이터베이스에서 수동으로 추가하거나 삭제합니다.

ssh timeout

기본 SSH 세션 유휴 시간 제한 값을 변경하려면 글로벌 컨피그레이션 모드에서 **ssh timeout** 명령을 사용합니다. 기본 시간 제한 값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ssh timeout *number*

no ssh timeout

구문 설명

number	연결을 해제하기 전에 SSH 세션을 비활성 상태로 유지할 수 있는 기간(분)을 지정합니다. 유효한 값은 1~60분입니다.

기본값

기본 세션 시간 제한 값은 5분입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

ssh timeout 명령은 연결을 해제하기 전에 세션을 유휴 상태로 유지할 수 있는 기간(분)을 지정합니다. 기본 지속 시간은 5분입니다.

예

다음 예에서는 IP 주소가 10.1.1.1인 관리 콘솔에서의 SSH 버전 2 연결만 허용하도록 내부 인터페이스를 구성하는 방법을 보여 줍니다. 유휴 세션 시간 제한은 60분으로 설정되어 있으며, SCP가 활성화되어 있습니다.

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

관련 명령

명령	설명
clear configure ssh	실행 중인 컨피그레이션에서 모든 SSH 명령을 지웁니다.
show running-config ssh	실행 중인 컨피그레이션의 현재 SSH 명령을 표시합니다.
show ssh sessions	ASA의 활성 SSH 세션에 대한 정보를 표시합니다.
ssh disconnect	활성 SSH 세션의 연결을 해제합니다.

ssh version

ASA에서 허용하는 SSH 버전을 제한하려면 글로벌 컨피그레이션 모드에서 **ssh version** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다. 기본값은 ASA에 대한 SSH 버전 1 및 SSH 버전 2를 허용하는 것입니다.

ssh version {**1** | **2**}

no ssh version [**1** | **2**]

구문 설명

1	SSH 버전 1 연결만 지원되도록 지정합니다.
2	SSH 버전 2 연결만 지원되도록 지정합니다.

기본값

기본적으로 SSH 버전 1과 SSH 버전 2가 모두 지원됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

1과 2는 ASA에서 사용이 제한된 SSH 버전을 지정합니다. 이 명령의 **no** 형식은 ASA를 두 버전 모두 사용할 수 있는 호환 모드인 기본 상태로 되돌립니다.

예

다음 예에서는 IP 주소가 10.1.1.1인 관리 콘솔에서의 SSH 버전 2 연결을 허용하도록 내부 인터페이스를 구성하는 방법을 보여 줍니다. 유휴 세션 시간 제한은 60분으로 설정되어 있으며, SCP가 활성화되어 있습니다.

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

관련 명령

명령	설명
clear configure ssh	실행 중인 컨피그레이션에서 모든 SSH 명령을 지웁니다.
debug ssh	SSH 명령에 대한 디버그 정보 및 오류 메시지를 표시합니다.
show running-config ssh	실행 중인 컨피그레이션의 현재 SSH 명령을 표시합니다.
ssh	ASA에 대한 지정된 클라이언트 또는 네트워크의 SSH 연결을 허용합니다.

ssl certificate-authentication

이전 8.2(1) 버전과의 호환성을 위해 클라이언트 인증서 인증을 활성화하려면 글로벌 컨피그레이션 모드에서 **ssl certificate-authentication** 명령을 사용합니다. SSL 인증서 인증을 비활성화하려면 이 명령의 **no** 버전을 사용합니다.

ssl certificate-authentication interface *interface-name* **port** *port-number*

no ssl certificate-authentication interface *interface-name* **port** *port-numbe***r**

구문 설명

interface-name	선택한 인터페이스의 이름(예: inside, management 및 outside)입니다.
port-number	TCP 포트 번호(1~65535의 정수)입니다.

기본값

이 기능은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.0(3)	이 명령이 도입되었습니다.
8.2(1)	이 명령은 더 이상 필요 없지만 ASA에서는 이전 버전으로의 다운그레이드를 위해 이 명령을 유지합니다.

사용 지침

이 명령은 사용이 중단된 **http authentication-certificate** 명령을 대체합니다.

예

다음 예에서는 SSL 인증서 인증 기능을 사용하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl certificate-authentication interface inside port 330
```

관련 명령

명령	설명
show running-config ssl	현재 구성된 SSL 명령 집합을 표시합니다.

ssl cipher

SSL, DTLS 및 TLS 프로토콜에 대한 암호화 알고리즘을 지정하려면 글로벌 컨피그레이션 모드에서 **ssl cipher** 명령을 사용합니다. 전체 암호화 알고리즘 집합인 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

ssl cipher *version* [*level* | **custom** "*string*"]

no ssl cipher *version* [*level* | **custom** "*string*"]

구문 설명

custom *string*	OpenSSL 암호 정의 문자열을 사용하여 암호 그룹에 대한 모든 권한을 허용합니다.
level	암호의 강도를 지정하고 지원되는 최소 암호 수준을 나타냅니다. 증가하는 강도 순서의 유효한 값은 다음과 같습니다. • **all** - NULL-SHA를 비롯한 모든 암호를 포함합니다. • **low** - NULL-SHA를 제외한 모든 암호를 포함합니다. • **medium** - NULL-SHA, DES-CBC-SHA 및 RC4-MD5를 제외한 모든 암호를 포함합니다. • **fips** - 모든 FIPS 호환 암호(NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA 및 DES-CBC3-SHA 제외)를 포함합니다. • **high**(TLSv1.2에만 적용됨) - SHA-2 암호를 사용하는 AES-256만 포함합니다.
version	SSL, DTLS 또는 TLS 프로토콜 버전을 지정합니다. 지원되는 버전은 다음과 같습니다. • **default** - 아웃바운드 연결을 위한 암호 집합입니다. • **dtlsv1** - DTLSv1 인바운드 연결을 위한 암호입니다. • **sslv3** - SSLv3 인바운드 연결을 위한 암호입니다. • **tlsv1** - TLSv1 인바운드 연결을 위한 암호입니다. • **tlsv1.1** - TLSv1.1 인바운드 연결을 위한 암호입니다. • **tlsv1.2** - TLSv1.2 인바운드 연결을 위한 암호입니다.

기본값

기본값은 모든 프로토콜 버전에 대해 **medium**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

이 명령은 ASA 버전 9.3(2)부터 **ssl encryption** 명령을 대체합니다.

권장 설정은 **medium**입니다. **high**를 사용하면 연결이 제한될 수 있습니다. **custom**을 사용하면 소수의 암호만 구성된 경우 기능이 제한될 수 있습니다. 기본 사용자 지정 값을 제한하면 클러스터링을 포함하여 아웃바운드 연결이 제한됩니다.

OpenSSL을 사용하는 암호에 대한 자세한 내용은 https://www.openssl.org/docs/apps/ciphers.html을 참고하십시오.

show ssl ciphers all 명령을 사용하여 각 버전을 지원하는 암호 목록을 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
These are the ciphers for the given cipher level; not all ciphers are supported by all
versions of SSL/TLS.
These names can be used to create a custom cipher list:
  DHE-RSA-AES256-SHA256(tlsv1.2)
  AES256-SHA256(tlsv1.2)
  DHE-RSA-AES128-SHA256(tlsv1.2)
  AES128-SHA256(tlsv1.2)
  DHE-RSA-AES256-SHA(tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA(sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA(tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA(sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA(sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA(sslv3, tlsv1)
  RC4-MD5(sslv3, tlsv1)
  DES-CBC-SHA(sslv3, tlsv1)
  NULL-SHA(sslv3, tlsv1)
```

ASA에서는 지원되는 암호화에 대한 우선 순위를 다음과 같이 지정합니다.

TLSv1.2에서 지원되는 암호(1~9)

1. DHE-RSA-AES256-SHA256
2. AES256-SHA256
3. DHE-RSA-AES128-SHA256
4. AES128-SHA256
5. DHE-RSA-AES256-SHA
6. AES256-SHA
7. DHE-RSA-AES128-SHA
8. AES128-SHA
9. DES-CBC3-SHA

TLSv1.1 또는 TLSv1.2에서 지원되지 않는 암호화(10~13)

10. RC4-SHA
11. RC4-MD5
12. DES-CBC-SHA
13. NULL-SHA

예

다음 예에서는 TLSv1.1 FIPS 호환 암호를 사용하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl cipher tlsv1.1 fips
```

다음 예에서는 SSLv3 사용자 지정 암호를 사용하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl cipher sslv3 custom "RC4:ALL:!DH"
```

다음 예에서는 TLSv1 사용자 지정 암호를 사용하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl cipher tlsv1 custom "RC4-SHA:ALL"
```

관련 명령

명령	설명
show running-config ssl	현재 구성된 SSL 명령 집합을 표시합니다.
show ssl ciphers	지원되는 암호 목록을 표시합니다.

ssl client-version

ASA가 클라이언트로 작동할 때 사용하는 SSL/TLS 프로토콜 버전을 지정하려면 글로벌 컨피그레이션 모드에서 **ssl client-version** 명령을 사용합니다. 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

ssl client-version [**any** | **sslv3-only** | **tlsv1-only** | **sslv3** | **tlsv1** | **tlsv1.1** | **tlsv1.2**]

no ssl client-version

구문 설명

any	SSLv3 클라이언트 Hello를 전송하고 SSLv3 이상을 협상합니다.
sslv3	SSLv3 클라이언트 Hello를 전송하고 SSLv3 이상을 협상합니다.
sslv3-only	SSLv3 클라이언트 Hello를 전송하고 SSLv3 이상을 협상합니다. **참고** 이 옵션은 버전 9.3(2)부터 사용이 중단되었습니다.
tlsv1	TLSv1 클라이언트 Hello를 전송하고 TLSv1 이상을 협상합니다.
tlsv1.1	TLSv1.1 클라이언트 Hello를 전송하고 TLSv1.1 이상을 협상합니다.
tlsv1.2	TLSv1.2 클라이언트 Hello를 전송하고 TLSv1.2 이상을 협상합니다.
tlsv1-only	TLSv1 클라이언트 Hello를 전송하고 TLSv1 이상을 협상합니다. **참고** 이 옵션은 버전 9.3(2)부터 사용이 중단되었습니다.

기본값

기본값은 **tlsv1**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.3(2)	SSLv3의 사용이 중단되었습니다. 이제 기본값은 **any** 대신 **tlsv1**입니다. **any** 키워드는 더 이상 사용되지 않습니다.

사용 지침

any, **sslv3** 또는 **sslv3-only** 키워드를 사용하는 경우 다음 경고와 함께 명령이 허용됩니다.

```
WARNING: SSLv3 is deprecated. Use of TLSv1 or greater is recommended.
```

다음 주요 ASA 릴리스에서 이 키워드는 ASA에서 제거됩니다.

예

다음 예에서는 SSL 클라이언트로 작동할 때 SSLv3 프로토콜 버전을 지정하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl client-version any
```

관련 명령

명령	설명
clear config ssl	컨피그레이션에서 모든 SSL 명령을 제거하고 기본값으로 되돌립니다.
ssl encryption	SSL/TLS 프로토콜에서 사용하는 암호화 알고리즘을 지정합니다.
show running-config ssl	현재 구성된 SSL 명령 집합을 표시합니다.
ssl server-version	ASA가 SSL/TLS 연결을 협상할 최소 프로토콜 버전을 지정합니다.
ssl trust-point	인터페이스에 대한 SSL 인증서를 나타내는 인증서 신뢰 지점을 지정합니다.

ssl dh-group

TLS에서 사용되는 DHE-RSA 암호와 함께 사용할 Diffie-Hellmann(DH) 그룹을 지정하려면 글로벌 컨피그레이션 모드에서 **ssl dh-group** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

no ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

구문 설명

group1	DH 그룹 1(768비트 모듈러스)을 구성합니다.
group2	DH 그룹 2(1024비트 모듈러스)을 구성합니다.
group5	DH 그룹 5(1536비트 모듈러스)을 구성합니다.
group14	DH 그룹 14(2048비트 모듈러스, 224비트 소수 위수 하위 그룹)을 구성합니다.
group24	DH 그룹 24(2048비트 모듈러스, 256비트 소수 위수 하위 그룹)을 구성합니다.

기본값

기본값은 DH 그룹 2입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령이 도입되었습니다.

사용 지침

그룹 1 및 2는 Java 7 이하 버전과 호환됩니다. 그룹 5, 14 및 24는 Java 7과 호환되지 않습니다. 모든 그룹은 Java 8과 호환됩니다. 그룹 14 및 24는 FIPS와 호환됩니다.

예

다음 예에서는 특정 DH 그룹을 사용하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl dh-group group14
```

관련 명령

명령	설명
show running-config ssl	현재 구성된 SSL 명령 집합을 표시합니다.

ssl encryption (Deprecated)

참고 마지막으로 이 명령을 지원하는 릴리스는 버전 9.3(1)이었습니다.

SSL, DTLS 및 TLS 프로토콜에 대한 암호화 알고리즘을 지정하려면 글로벌 컨피그레이션 모드에서 **ssl encryption** 명령을 사용합니다**.** 전체 암호화 알고리즘 집합인 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

ssl encryption [**3des-sha1**] [**aes128-sha1**] [**aes256-sha1**] [**des-sha1**] [**null-sha1**] [**rc4-md5**] [**rc4-sha1**] [**dhe-aes256-sha1**] [**dhe-aes128-sha1**]

no ssl encryption

구문 설명

3des-sha1	Secure Hash Algorithm 1(FIPS 호환)을 사용하는 3중 DES 168비트 암호화를 지정합니다.
aes128-sha1	Secure Hash Algorithm 1(FIPS 호환)을 사용하는 3중 AES 128비트 암호화를 지정합니다.
aes256-sha1	Secure Hash Algorithm 1(FIPS 호환)을 사용하는 3중 AES 256비트 암호화를 지정합니다.
dhe-aes128-sha1	TLS(전송 계층 보안)(FIPS 호환)에 대한 AES 128비트 암호화 암호 그룹을 지정합니다.
dhe-aes256-sha1	TLS(전송 계층 보안)(FIPS 호환)에 대한 AES 256비트 암호화 암호 그룹을 지정합니다.
des-sha1	Secure Hash Algorithm 1을 사용하는 DES 56비트 암호화를 지정합니다.
sha1 null	Secure Hash Algorithm 1을 사용하는 null 암호화를 지정합니다. 이 설정은 기밀성 없이 메시지 무결성을 적용합니다. 주의 **null sha1**을 지정한 경우에는 데이터가 암호화되지 않습니다.
rc4-md5	MD5 해시 기능을 사용하는 RC4 128비트 암호화를 지정합니다.
rc4-sha1	Secure Hash Algorithm 1을 사용하는 RC4 128비트 암호화를 지정합니다.

기본값

기본적으로 ASA의 SSL 암호화 목록에는 다음 알고리즘이 순서대로 포함되어 있습니다.

1. RC4-SHA1
2. AES128-SHA1(FIPS 호환)
3. AES256-SHA1(FIPS 호환)
4. 3DES-SHA1(FIPS 호환)
5. DHE-AES256-SHA1(FIPS 호환)
6. DHE-AES128-SHA1(FIPS 호환)

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.1(2)	DHE-AES128-SHA1 및 DHE-AES256-SHA1 알고리즘을 사용하는 SSL 암호화에 대한 지원이 추가되었습니다.
9.3(2)	이 명령은 사용이 중단되었으며, **ssl cipher** 명령으로 대체되었습니다.

사용 지침

명령을 다시 실행하면 이전 설정을 덮어씁니다. ASDM License(ASDM 라이센스) 탭에는 구성한 값이 아니라 라이센스에서 지원하는 최대 암호화가 반영됩니다.

알고리즘 순서에 따라 해당 사용에 대한 환경 설정이 결정됩니다. 사용자 환경의 요구에 맞게 알고리즘을 추가하거나 제거할 수 있습니다.

FIPS 호환 AnyConnect 클라이언트 SSL 연결의 경우 FIPS 호환 암호가 SSL 암호화 목록에 지정된 첫 번째 암호여야 합니다.

일부 애플리케이션은 DHE를 지원하지 않으므로 하나 이상의 다른 SSL 암호화 방법을 포함하여 암호 그룹이 둘 다에 공통적으로 사용되도록 해야 합니다.

암호화 작업에서는 http://en.wikipedia.org/wiki/Symmetric-key_algorithm에 언급된 대로 대칭 키 알고리즘을 사용합니다.

예

다음 예에서는 3des-sha1 및 des-sha1 암호화 알고리즘을 사용하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl encryption 3des-sha1 des-sha1
```

Starting with ASA version 9.3(2)

다음 예에서는 이 명령이 사용 중단되고 **ssl cipher** 명령으로 대체되었음을 보여 줍니다.

```
ciscoasa(config)# ssl encryption ?

configure mode commands/options:
This command is DEPRECATED, use 'ssl cipher' instead.

  3des-sha1         Indicate use of 3des-sha1 for ssl encryption
  aes128-sha1       Indicate use of aes128-sha1 for ssl encryption
  aes256-sha1       Indicate use of aes256-sha1 for ssl encryption
  des-sha1          Indicate use of des-sha1 for ssl encryption
  dhe-aes128-sha1   Indicate use of dhe-aes128-sha1 for ssl encryption
  dhe-aes256-sha1   Indicate use of dhe-aes256-sha1 for ssl encryption
  null-sha1         Indicate use of null-sha1 for ssl encryption (NOTE: Data is
                    NOT encrypted if this cipher is chosen)
  rc4-md5           Indicate use of rc4-md5 for ssl encryption
  rc4-sha1          Indicate use of rc4-sha1 for ssl encryption
```

```
ciscoasa(config)# ssl encryption rc4-sha1 aes256-sha1 aes128-sha1
WARNING: This command has been deprecated; use 'ssl cipher' instead.
INFO: Converting to: ssl cipher default custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher sslv3 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher tlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher dtlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
```

관련 명령

명령	설명
clear config ssl	컨피그레이션에서 모든 SSL 명령을 제거하고 기본값으로 되돌립니다.
show running-config ssl	현재 구성된 SSL 명령 집합을 표시합니다.
ssl client-version	ASA가 클라이언트로 작동할 때 사용하는 SSL/TLS 프로토콜 버전을 지정합니다.
ssl server-version	ASA가 SSL/TLS 연결을 협상할 최소 프로토콜 버전을 지정합니다.
ssl trust-point	인터페이스에 대한 SSL 인증서를 나타내는 인증서 신뢰 지점을 지정합니다.
ssl cipher	SSL, DTLS 및 TLS 프로토콜에 대한 암호화 알고리즘을 지정합니다. **참고** 9.3(2) 릴리스부터 사용할 수 있습니다.

ssl server-version

ASA가 SSL/TLS 연결을 협상할 최소 프로토콜 버전을 설정하려면 글로벌 컨피그레이션 모드에서 **ssl server-version** 명령을 사용합니다. 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

ssl server-version [**any** | **sslv3-only** | **tlsv1-only** | **sslv3** | **tlsv1** | **tlsv1.1** | **tlsv1.2**]

no ssl server-version

구문 설명

any	SSLv2 클라이언트 Hello를 수락하고 가장 높은 일반 버전을 협상합니다.
sslv3	SSLv2 클라이언트 Hello를 수락하고 SSLv3 이상을 협상합니다.
sslv3-only	SSLv2 클라이언트 Hello를 수락하고 SSLv3 이상을 협상합니다. **참고** 이 옵션은 버전 9.3(2)부터 사용이 중단되었습니다.
tlsv1	SSLv2 클라이언트 Hello를 수락하고 TLSv1 이상을 협상합니다.
tlsv1.1	SSLv2 클라이언트 Hello를 수락하고 TLSv1.1 이상을 협상합니다.
tlsv1.2	SSLv2 클라이언트 Hello를 수락하고 TLSv1.2 이상을 협상합니다.
tlsv1-only	SSLv2 클라이언트 Hello를 수락하고 TLSv1 이상을 협상합니다. **참고** 이 옵션은 버전 9.3(2)부터 사용이 중단되었습니다.

기본값

기본값은 **tlsv1**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.3(2)	SSLv3의 사용이 중단되었습니다. 이제 기본값은 **any** 대신 **tlsv1**입니다. **any** 키워드는 더 이상 사용되지 않습니다.

사용 지침

any, **sslv3** 또는 **sslv3-only** 키워드를 사용하는 경우 다음 경고와 함께 명령이 허용됩니다.

```
WARNING: SSLv3 is deprecated. Use of TLSv1 or greater is recommended.
```

다음 주요 ASA 릴리스에서 이 키워드는 ASA에서 제거됩니다.

예

다음 예에서는 SSL/TLS 연결을 협상하도록 ASA를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl server-version tlsv1
```

관련 명령

명령	설명
clear config ssl	컨피그레이션에서 모든 SSL 명령을 제거하고 기본값으로 되돌립니다.
show running-config ssl	현재 구성된 SSL 명령 집합을 표시합니다.
ssl client-version	ASA가 클라이언트로 작동할 때 사용하는 SSL/TLS 프로토콜 버전을 지정합니다.
ssl encryption	SSL/TLS 프로토콜에서 사용하는 암호화 알고리즘을 지정합니다.
ssl trust-point	인터페이스에 대한 SSL 인증서를 나타내는 인증서 신뢰 지점을 지정합니다.

ssl trust-point

인터페이스에 대한 SSL 인증서를 나타내는 인증서 신뢰 지점을 지정하려면 글로벌 컨피그레이션 모드에서 *interface* 인수와 함께 **ssl trust-point** 명령을 사용합니다. 인터페이스를 지원하지 않는 SSL 신뢰 지점을 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다. 인터페이스를 지원하지 않는 항목을 제거하려면 이 명령의 **no ssl trust-point** *name* [*interface*] 형식을 사용합니다.

ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** *domain-name*]

no ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** *domain-name*]

구문 설명

domain *domain-name*	이 신뢰 지점을 이 인터페이스에 액세스하는 데 사용되는 특정 도메인 이름(예 :www.cisco.com)과 연결합니다.
interface	신뢰 지점이 적용되는 인터페이스의 이름을 지정합니다. **nameif** 명령은 인터페이스의 이름을 정의합니다.
name	**crypto ca trustpoint** *name* 명령에 구성된 대로 CA 신뢰 지점의 이름을 지정합니다.
IP vpnlb	이 신뢰 지점을 이 인터페이스의 VPN 부하 균형 클러스터 IP 주소와 연결합니다. 인터페이스에만 적용됩니다.

기본값

기본값은 신뢰 지점 연계가 없는 것입니다. ASA에서는 기본 자체 생성 RSA 키 쌍 인증서를 사용합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.3(2)	**domain** *domain-name* 키워드-인수 쌍이 추가되었습니다.

사용 지침

인터페이스 또는 도메인을 지정하지 않은 경우 이 항목은 자체 신뢰 지점에 연결되지 않은 모든 인터페이스에서 사용되는 대체 신뢰 지점을 나타냅니다.

ssl trustpoint ? 명령을 입력한 경우 사용 가능한 구성된 신뢰 지점이 표시됩니다. **ssl trust-point** *name* **?** 명령(예: **ssl trust-point mysslcert ?**)을 입력한 경우 신뢰 지점-SSL 인증서 연계에 사용 가능한 구성된 인터페이스가 표시됩니다.

인터페이스당 최대 16개의 신뢰 지점을 구성할 수 있습니다.

이 명령을 사용할 때 다음 지침을 따르십시오.

- *trustpoint* 값은 **crypto ca trustpoint** *name* 명령에 구성된 CA 신뢰 지점의 이름이어야 합니다.
- *interface*는 이전에 구성된 인터페이스의 *nameif* 이름이어야 합니다.
- 신뢰 지점을 제거하면 해당 신뢰 지점을 참조하는 모든 **ssl trust-point** 항목도 제거됩니다.
- 인터페이스당 하나의 **ssl trust-point** 항목과 인터페이스 없음을 지정하는 항목을 유지할 수 있습니다.
- **domain** 키워드로 구성된 신뢰 지점은 연결 방법에 따라 여러 인터페이스에 적용될 수 있습니다.
- *domain-name* 값당 하나의 **ssl trust-point**만 유지할 수 있습니다.
- 여러 항목에 동일한 신뢰 지점을 다시 사용할 수 있습니다.
- 이 명령을 입력한 후 다음 오류가 표시되는 경우

  ```
  error:0B080074:x509 certificate routines:X509_check_private_key:key values
  mismatch@x509_cmp.c:339
  ```

  사용자가 이전에 구성된 인증서를 대체할 새 인증서를 구성했음을 의미합니다. 추가 작업은 필요하지 않습니다.
- 인증서가 다음 순서대로 선택됩니다.
  - 연결이 **domain** 키워드 값과 일치하지 않는 경우 해당 인증서가 먼저 선택됩니다. (**ssl trust-point** *name* **domain** *domain-name* 명령)
  - 부하 균형 주소로 연결이 설정된 경우 vpnlb-ip 인증서가 선택됩니다. (**ssl trust-point** *name* **interface vpnlb-ip** 명령)
  - 인터페이스에 대해 구성된 인증서 (**ssl trust-point** *name* **interface** 명령)
  - 인터페이스와 연결되지 않은 기본 인증서 (**ssl trust-point** *name* 명령)
  - ASA의 자체 서명 및 자체 생성된 인증서

예

다음 예에서는 내부 인터페이스에 대한 FirstTrust라는 SSL 신뢰 지점 및 연결된 인터페이스가 없는 DefaultTrust라는 신뢰 지점을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl trust-point FirstTrust inside
ciscoasa(config)# ssl trust-point DefaultTrust
```

다음 예에서는 이 명령의 **no** 형식을 사용하여 연결된 인터페이스가 없는 신뢰 지점을 삭제하는 방법을 보여 줍니다.

```
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

다음 예에서는 연결된 인터페이스가 있는 신뢰 지점을 삭제하는 방법을 보여 줍니다.

```
ciscoasa(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point FirstTrust inside
ciscoasa(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

다음 예에서는 구성된 신뢰 지점에 특정 도메인 이름을 할당하는 방법을 보여 줍니다.

```
ciscoasa(config)# ssl trust-point www-cert domain www.example.com
```

관련 명령

명령	설명
clear config ssl	컨피그레이션에서 모든 SSL 명령을 제거하고 기본값으로 되돌립니다.
show running-config ssl	현재 구성된 SSL 명령 집합을 표시합니다.
ssl client-version	ASA가 클라이언트로 작동할 때 사용하는 SSL/TLS 프로토콜 버전을 지정합니다.
ssl encryption	SSL/TLS 프로토콜에서 사용하는 암호화 알고리즘을 지정합니다.
ssl server-version	ASA가 SSL/TLS 연결을 협상할 최소 프로토콜 버전을 지정합니다.
show ssl	SSL 컨피그레이션 통계를 표시합니다.

sso-server

ASA 사용자 인증을 위한 SSO(Single Sign On: 단일 로그인) 서버를 생성하려면 webvpn 컨피그레이션 모드에서 **sso-server** 명령을 사용합니다. 이 명령을 사용하는 경우 SSO 서버 유형을 지정해야 합니다.

SSO 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

sso-server *name* **type** [*siteminder* | *saml-v1.1-post*]

no sso-server *name*

참고 이 명령은 SSO 인증에 필요합니다.

구문 설명

name	SSO 서버 이름을 지정합니다. 4~31자여야 합니다.
saml-v1.1-post	구성할 ASA SSO 서버가 POST 유형의 SAML, 버전 1.1, SSO 서버임을 지정합니다.
siteminder	구성할 ASA SSO 서버가 Computer Associates SiteMinder SSO 서버임을 지정합니다.
type	SSO 서버 유형을 지정합니다. Site Minder 및 SAML-V1.1-POST만 사용할 수 있습니다.

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

사용 지침

SSO(WebVPN에만 제공) 지원을 통해 사용자가 사용자 이름 및 비밀번호를 단 한 번만 입력하여 여러 서버에서 다양한 보안 서비스에 액세스할 수 있습니다. **sso-server** 명령을 사용하여 SSO 서버를 생성할 수 있습니다.

인증에서 ASA는 SSO 서버의 WebVPN 사용자를 위한 프록시 역할을 합니다. ASA는 현재 SiteMinder SSO 서버(이전의 Netegrity SiteMinder) 및 SAML POST 유형 SSO 서버를 지원합니다. 현재 유형 옵션에 사용 가능한 인수는 *siteminder* 또는 *saml-V1.1-post*로 제한됩니다.

예

webvpn 컨피그레이션 모드에서 입력된 다음 예에서는 “example1”이라는 SiteMinder 유형의 SSO 서버를 생성합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example1 type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
```

webvpn 컨피그레이션 모드에서 입력된 다음 예에서는 “example2”라는 SAML, 버전 1.1, POST 유형의 SSO 서버를 생성합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example2 type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml)#
```

관련 명령

명령	설명
assertion-consumer-url	SAML 유형 SSO 어설션 고객 서비스에 대한 URL을 식별합니다.
issuer	SAML 유형 SSO 서버의 보안 디바이스 이름을 지정합니다.
max-retry-attempts	ASA에서 SSO 인증을 재시도할 수 있는 횟수를 구성합니다.
policy-server-secret	SiteMinder SSO 서버에 대한 인증 요청을 암호화하는 데 사용되는 비밀 키를 생성합니다.
request-timeout	시간 초과로 인해 SSO 인증 시도가 실패하는 시간(초)을 지정합니다.
show webvpn sso-server	SSO 서버에 대한 운영 통계를 표시합니다.
test sso-server	평가판 인증 요청으로 SSO 서버를 테스트합니다.
trustpoint	SAML 유형 브라우저 어설션을 서명하는 데 사용할 인증서가 포함된 신뢰 지점 이름을 지정합니다.
web-agent-url	ASA에서 SiteMinder SSO 인증 요청을 작성하는 SSO 서버 URL을 지정합니다.

sso-server value (group-policy webvpn)

그룹 정책에 SSO 서버를 할당하려면 group-policy 컨피그레이션 모드에서 사용 할 수 있는 webvpn 컨피그레이션 모드에서 **sso-server value** 명령을 사용합니다.

할당을 제거하고 기본 정책을 사용하려면 이 명령의 **no** 형식을 사용합니다.

기본 정책을 상속하지 못하도록 하려면 **sso-server none** 명령을 사용합니다.

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

구문 설명

name	그룹 정책에 할당할 SSO 서버의 이름을 지정합니다.

기본값

그룹에 할당되는 기본 정책은 DfltGrpPolicy입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

사용 지침

group-policy webvpn 모드에서 입력된 **sso-server value** 명령을 통해 그룹 정책에 SSO 서버를 할당할 수 있습니다.

SSO(WebVPN에만 제공) 지원을 통해 사용자가 사용자 이름 및 비밀번호를 단 한 번만 입력하여 여러 서버에서 다양한 보안 서비스에 액세스할 수 있습니다. ASA는 현재 SiteMinder 유형 SSO 서버 및 SAML POST 유형 SSO 서버를 지원합니다.

이 명령은 두 유형의 SSO 서버 모두에 적용됩니다.

참고 사용자 정책에 SSO 서버를 할당하려면 동일한 명령 **sso-server value**를 username-webvpn 컨피그레이션 모드에서 입력합니다.

예

다음 예제 명령에서는 그룹 정책 my-sso-grp-pol을 만들어 example이라는 SSO 서버에 할당합니다.

```
ciscoasa(config)# group-policy my-sso-grp-pol internal
ciscoasa(config)# group-policy my-sso-grp-pol attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# sso-server value example
ciscoasa(config-group-webvpn)#
```

관련 명령

명령	설명
policy-server-secret	SiteMinder SSO 서버에 대한 인증 요청을 암호화하는 데 사용되는 비밀 키를 생성합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso-server	SSO(Single Sign On) 서버를 생성합니다.
sso-server value (username webvpn)	SSO 서버를 사용자 정책에 할당합니다.
web-agent-url	ASA에서 SiteMinder-type SSO 인증 요청을 작성하는 SSO 서버 URL을 지정합니다.

sso-server value (username webvpn)

사용자 정책에 SSO 서버를 할당하려면 group-policy 컨피그레이션 모드에서 사용 할 수 있는 webvpn 컨피그레이션 모드에서 **sso-server value** 명령을 사용합니다.

사용자에 대한 SSO 서버 할당을 제거하려면 이 명령의 **no** 형식을 사용합니다.

사용자 정책이 그룹 정책에서 불필요한 SSO 서버 할당을 상속하는 경우 **sso-server none** 명령을 사용하여 할당을 제거합니다.

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

구문 설명

name	사용자 정책에 할당할 SSO 서버의 이름을 지정합니다.

기본값

기본값은 사용자 정책에서 그룹 정책에 있는 SSO 서버 할당을 사용하는 것입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
username webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

사용 지침

SSO(WebVPN에만 제공) 지원을 통해 사용자가 사용자 이름 및 비밀번호를 단 한 번만 입력하여 여러 서버에서 다양한 보안 서비스에 액세스할 수 있습니다. ASA는 현재 SiteMinder 유형 SSO 서버 및 SAML POST 유형 SSO 서버를 지원합니다.

이 명령은 두 유형의 SSO 서버 모두에 적용됩니다.

sso-server value 명령을 사용하여 사용자 정책에 SSO 서버를 할당할 수 있습니다.

참고 그룹 정책에 SSO 서버를 할당하려면 동일한 명령 **sso-server value**를 group-webvpn 컨피그레이션 모드에서 입력합니다.

예

다음 예제 명령은 Anyuser라는 WebVPN 사용자의 사용자 정책에 my-sso-server라는 SSO 서버를 할당합니다.

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# sso-server value my-sso-server
ciscoasa(config-username-webvpn)#
```

관련 명령

명령	설명
policy-server-secret	SiteMinder SSO 서버에 대한 인증 요청을 암호화하는 데 사용되는 비밀 키를 생성합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso-server	SSO(Single Sign On) 서버를 생성합니다.
sso-server value (config-group-webvpn)	SSO 서버를 그룹 정책에 할당합니다.
web-agent-url	ASA에서 SiteMinder SSO 인증 요청을 작성하는 SSO 서버 URL을 지정합니다.

start-url

선택적 사전 로그인 쿠키를 검색할 URL을 입력하려면 aaa-server-host 컨피그레이션 모드에서 **start-url** 명령을 사용합니다. 이는 HTTP 양식을 사용하는 SSO 명령입니다.

start-url *string*

참고 HTTP 프로토콜로 SSO를 올바르게 설정하려면 인증 및 HTTP 프로토콜 교환에 대해 완벽한 지식을 갖추어야 합니다.

구문 설명

string	SSO 서버에 대한 URL입니다. 최대 URL 길이는 1024자입니다.

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
aaa-server-host 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령이 도입되었습니다.

사용 지침

ASA의 WebVPN 서버는 HTTP POST 요청을 사용하여 인증 웹 서버에 SSO(Single Sign On) 인증 요청을 제출할 수 있습니다. 인증 웹 서버에서 로그인 페이지 콘텐츠와 함께 헤더를 보내서 Set-Cookie 사전 로그인 시퀀스를 수행할 수도 있습니다. 브라우저로 인증 웹 서버의 로그인 페이지에 바로 연결하면 이를 확인할 수 있습니다. 로그인 페이지가 로드될 때 웹 서버에서 쿠키를 설정하고 이 쿠키가 다음 로그인 세션과 관련된 경우 **start-url** 명령을 사용하여 쿠키를 검색할 URL을 입력해야 합니다. 실제 로그인 시퀀스는 인증 웹 서버에 양식을 제출하고 사전 로그인 쿠키 시퀀스 후에 시작됩니다.

참고 사전 로그인 쿠키 교환이 있을 때에만 **start-url** 명령이 필요합니다.

예

aaa-server host 컨피그레이션 모드에서 입력한 다음 예는 https://example.com/east/Area.do?Page-Grp1의 사전 로그인 쿠키를 검색할 URL을 지정합니다.

```
ciscoasa(config)# aaa-server testgrp1 (inside) host example.com
ciscoasa(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
action-uri	SSO(Single Sign On) 인증에 필요한 사용자 이름 및 비밀번호를 받을 웹 서버 URI를 지정합니다.
auth-cookie-name	인증 쿠키 이름을 지정합니다.
hidden-parameter	인증 웹 서버와 교환할 숨겨진 파라미터를 생성합니다.
password-parameter	SSO 인증을 위해 사용자 비밀번호를 제출해야 하는 HTTP POST 요청 파라미터의 이름을 지정합니다.
user-parameter	SSO 인증을 위해 사용자 이름을 전송해야 하는 HTTP POST 요청 파라미터의 이름을 지정 합니다.

state-checking

H.323의 상태를 확인하려면 파라미터 컨피그레이션 모드에서 **state-checking** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

state-checking [h225 | ras]

no state-checking [h225 | ras]

구문 설명

h225	H.225의 상태를 검사합니다.
ras	RAS의 상태를 검사합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
파라미터 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예는 H.323 호출 시 RAS 상태를 검사하는 방법을 보여 줍니다.

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# state-checking ras
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	계층 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

strict-header-validation

RFC 3261에 따라 SIP 메시지의 헤더 필드를 엄격하게 검사하려면 파라미터 컨피그레이션 모드에서 **strict-header-validation** 명령을 사용합니다. 파라미터 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

strict-header-validation action {drop | drop-connection | reset | log} [log]

no strict-header-validation action {drop | drop-connection | reset | log} [log]

구문 설명

drop	유효성 검사가 발생하면 패킷을 차단합니다.
drop-connection	위반이 발생한 연결을 차단합니다.
reset	위반이 발생한 연결을 다시 설정합니다.
log	위반 시 독립형 또는 추가 로그를 지정합니다. 모든 작업에 연결할 수 있습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
파라미터 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

예

다음 예는 SIP 검사 정책 맵의 SIP 헤더 필드를 엄격하게 검사하는 방법을 보여 줍니다.

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-header-validation action log
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	계층 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

strict-http

규정을 따르지 않는 HTTP 트래픽을 전달하도록 허용하려면 HTTP 맵 컨피그레이션 모드에서 **strict-http** 명령을 사용합니다. HTTP 맵 컨피그레이션 모드는 **http-map** 명령을 사용하여 액세스할 수 있습니다. 이 기능을 기본 동작으로 다시 설정하려면 명령의 **no** 형식을 사용합니다.

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

구문 설명

action	메시지가 이 명령 검사에 실패하면 수행할 작업입니다.
allow	메시지를 허용합니다.
drop	연결을 닫습니다.
log	(선택 사항) syslog를 생성합니다.
reset	TCP 재설정 메시지와 함께 클라이언트 및 서버의 연결을 닫습니다.

기본값

이 명령은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
HTTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

엄격한 HTTP 검사를 비활성화할 수는 없지만 **strict-http action allow** 명령을 사용하면 ASA에서 규정을 따르지 않는 HTTP 트래픽 전달을 허용합니다. 이 명령은 기본 동작을 재정의합니다. 규정을 따르지 않는 HTTP 트래픽 전달을 거부하는 것이 기본 동작입니다.

예

다음 예는 규정을 따르지 않는 HTTP 트래픽 전달을 허용합니다.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# strict-http allow
ciscoasa(config-http-map)#
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
debug appfw	향상된 HTTP 검사와 연결된 트래픽에 대한 구체적인 정보를 표시합니다.
http-map	향상된 HTTP 검사 컨피그레이션에 대한 HTTP 맵을 정의합니다.
inspect http	애플리케이션 검사에 사용할 특정 HTTP 맵을 적용합니다.
policy-map	클래스 맵을 특정 보안 작업과 연계시킵니다.

strip-group

이 명령은 user@realm 형식으로 받은 사용자 이름에만 적용됩니다. 영역은 "@" 구분 기호가 붙은 사용자 이름(예: juser@abc)에 추가된 관리 도메인입니다.

스트립-그룹 처리를 활성화 또는 비활성화하려면 tunnel-group general-attributes 모드에서 **strip-group** 명령을 사용합니다. ASA는 VPN 클라이언트에서 제공한 사용자 이름에서 그룹 이름을 가져와서 IPsec 연결에 사용할 터널 그룹을 선택합니다. 스트립-그룹 처리가 활성화되면 ASA에서는 권한 부여/인증을 위해 사용자 이름의 사용자 부분만 보냅니다. 비활성화되면 ASA에서는 영역을 포함한 전체 사용자 이름을 보냅니다.

스트립-그룹 처리를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

strip-group

no strip-group

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령에 대한 기본 설정은 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tunnel-group general attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

IPsec 원격 액세스 터널 유형에만 이 특성을 적용할 수 있습니다.

참고 MSCHAPv2 의 제한 때문에 MSCHAPv2 가 PPP 인증에 사용되고 있으면 터널 그룹 전환을 수행할 수 없습니다 . MSCHAPv2 동안 해시 계산이 사용자 이름 문자열에 바인딩됩니다 (예 : 사용자 + 구분 기호 + 그룹).

예

다음 예는 IPsec 원격 액세스 유형에 대한 “remotegrp”라는 원격 액세스 터널 그룹을 구성한 후 일반 컨피그레이션 모드로 진입하여 기본 그룹 정책으로 “remotegrp”라는 터널 그룹을 설정하고, 해당 터널 그룹에 대해 스트립 그룹을 활성화합니다.

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-group
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
group-delimiter	그룹-이름 구문 분석을 활성화하고, 터널이 협상될 때 받은 사용자 이름의 그룹 이름을 구문 분석할 때 사용할 구분 기호를 지정합니다.
show running-config tunnel group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group general-attributes	명명된 tunnel-group의 일반 특성을 지정합니다.

strip-realm

스트립-영역 처리를 활성화 또는 비활성화하려면 tunnel-group general-attributes 모드에서 **strip-realm** 명령을 사용합니다. 스트립-영역 처리는 인증 또는 권한 부여 서버로 사용자 이름을 보낼 때 사용자 이름에서 영역을 제거합니다. 영역은 @ 구분 기호가 붙은 사용자 이름(username@realm)에 추가된 관리 도메인입니다. 명령이 활성화되면 ASA에서는 권한 부여/인증을 위해 사용자 이름의 사용자 부분만 보냅니다. 비활성화되면 ASA에서는 전체 사용자 이름을 보냅니다.

스트립-영역 처리를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

strip-realm

no strip-realm

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령에 대한 기본 설정은 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tunnel-group general attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0.1	이 명령이 도입되었습니다.

사용 지침

IPsec 원격 액세스 터널 유형에만 이 특성을 적용할 수 있습니다.

예

다음 예는 IPsec 원격 액세스 유형에 대한 “remotegrp”라는 원격 액세스 터널 그룹을 구성한 후 일반 컨피그레이션 모드로 진입하여 기본 그룹 정책으로 “remotegrp”라는 터널 그룹을 설정하고, 해당 터널 그룹에 대해 스트립 영역을 활성화합니다.

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-real
```

storage-key

세션 사이에 저장된 데이터를 보호할 스토리지 키를 지정하려면 group-policy webvpn 컨피그레이션 모드에서 **storage-key** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

storage- key {**none** | **value** *string*}

no storage-key

구문 설명

string	저장소 키 값으로 사용할 문자열을 지정합니다. 이 문자열은 최대 64자까지 허용됩니다.

기본값

기본값은 **none**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

공백을 제외한 모든 문자를 스토리지 키 값에 사용할 수 있지만 일반적인 영숫자 문자(0~9 및 a~z)를 사용할 것을 권장합니다.

예

다음 예는 스토리지 키 값을 abc123으로 설정합니다.

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# storage-key value abc123
```

관련 명령

명령	설명
storage-objects	세션 간에 저장되는 데이터의 스토리지 개체를 구성합니다.

storage-objects

세션 사이에 저장된 데이터에 어떤 스토리지 개체를 사용할 것인지 지정하려면 group-policy webvpn 컨피그레이션 모드에서 **storage-objects** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

storage- objects {**none** | **value** *string*}

no storage-objects

구문 설명

string	저장소 개체의 이름을 지정합니다. 이 문자열은 최대 64자까지 허용됩니다.

기본값

기본값은 **none**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
group-policy webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

공백과 쉼표를 제외한 모든 문자를 스토리지 개체 이름에 사용할 수 있지만 일반적인 영숫자 문자(0~9 및 a~z)를 사용할 것을 권장합니다. 문자열에서 스토리지 개체의 이름을 구분할 때에는 공백 없이 쉼표를 사용합니다.

예

다음 예는 스토리지 개체 이름을 cookies 및 xyz456으로 설정합니다.

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# storage-object value cookies,xyz456
```

관련 명령

명령	설명
storage-key	세션 간에 저장된 데이터에 사용할 저장소 키를 구성합니다.
user-storage	세션 간에 사용자 데이터를 저장할 위치를 구성합니다.

subject-name through sysopt radius ignore-secret 명령

subject-name (crypto ca certificate map)

규칙 항목이 IPsec 피어 인증서의 주체 DN에 적용됨을 나타내려면 crypto ca certificate map 컨피그레이션 모드에서 **subject-name** 명령을 사용합니다. 주체 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다.

subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

no subject-name [**attr** *tag* **eq | ne |co | nc** *string*]

구문 설명

attr *tag*	인증서 DN에서 지정된 특성 값만 규칙 항목 문자열과 비교됨을 나타냅니다. 태그 값은 다음과 같습니다. DNQ = DN 한정자 GENQ = 세대 한정자 I = 이니셜 GN = 이름 N = 이름 SN = 성 IP = IP 주소 SER = 일련 번호 UNAME = 구조화되지 않은 이름 EA = 이메일 주소 T = 직함 O = 조직 이름 L = 구/군/시 SP = 주/도 C = 국가 OU = 조직 구성 단위 CN = 공통 이름
co	규칙 항목 문자열이 DN 문자열의 하위 문자열 또는 지정된 특성이어야 하도록 지정합니다.
eq	DN 문자열 또는 지정된 특성이 전체 규칙 문자열과 일치해야 하도록 지정합니다.
nc	규칙 항목 문자열이 DN 문자열의 하위 문자열 또는 지정된 특성이 아니어야 하도록 지정합니다.
ne	DN 문자열 또는 지정된 특성이 전체 규칙 문자열과 일치하지 않아야 하도록 지정합니다.
string	일치시킬 값을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
crypto ca certificate map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 certificate map 1에 대한 ca certificate map 컨피그레이션 모드를 시작하고 인증서 주체 이름의 Organization 특성이 Central과 같아야 함을 나타내는 규칙 항목을 생성합니다.

```
ciscoasa(config)# crypto ca certificate map 1
ciscoasa(ca-certificate-map)# subject-name attr o eq central
ciscoasa(ca-certificate-map)# exit
```

관련 명령

명령	설명
crypto ca certificate map	ca certificate map 컨피그레이션 모드를 시작합니다.
issuer-name	CA 인증서에서 규칙 항목 문자열과 비교할 DN을 식별합니다.
tunnel-group-map	**crypto ca certificate map** 명령을 사용하여 생성된 인증서 맵 항목을 터널 그룹과 연결합니다.

subject-name (crypto ca trustpoint)

등록하는 동안 지정된 주체 DN을 인증서에 포함하려면 crypto ca trustpoint 컨피그레이션 모드에서 **subject-name** 명령을 사용합니다. 이는 인증서를 사용하는 사람 또는 시스템입니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

subject-name *X.500_name*

no subject-name

구문 설명

X.500_name	X.500 고유 이름을 정의합니다. 특성-값 쌍을 구분하려면 쉼표를 사용합니다. 쉼표 또는 공백이 포함된 값은 따옴표로 묶습니다. 예를 들면 **cn=crl,ou=certs,o="cisco systems, inc.",c=US**와 같습니다. 최대 길이는 500자입니다.

기본값

기본 설정은 주체 이름을 포함하지 않는 것입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

예

다음 예에서는 신뢰 지점 central에 대한 crypto ca trustpoint 컨피그레이션 모드를 시작하고, URL https//:frog.example.com에서 자동 등록을 설정하며, 신뢰 지점 central에 대한 등록 요청에 주체 DN OU 인증서를 포함합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url http://frog.example.com/
ciscoasa(ca-trustpoint)# subject-name ou=certs
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.
default enrollment	등록 파라미터를 해당 기본값으로 되돌립니다.
enrollment url	CA에 등록하기 위한 URL을 지정합니다.

subject-name-default

로컬 CA 서버에서 발급된 모든 사용자 인증서에 일반 주체 이름 DN(고유 이름)을 추가하도록 지정하려면 CA 서버 컨피그레이션 모드에서 **subject-name-default** 명령을 사용합니다. 주체 이름 DN을 기본값으로 다시 설정하려면 이 명령의 **no** 형식을 사용합니다.

subject-name-default *dn*

no subject-name-default

구문 설명

dn	로컬 CA 서버에서 발급된 모든 사용자 인증서에서 사용자 이름에 포함된 일반 주체 이름 DN을 지정합니다. 지원되는 DN 특성은 cn(공통 이름), ou(조직 구성 단위), ol(조직 구/군/시), st(주/도), ea(이메일 주소), c(회사), t(직함) 및 sn(성)입니다. 특성-값 쌍을 구분하려면 쉼표를 사용합니다. 쉼표가 포함된 값은 따옴표로 묶습니다. *dn*은 최대 500자까지 허용됩니다.

기본값

이 명령은 기본 컨피그레이션의 일부가 아닙니다. 이 명령은 인증서의 기본 DN을 지정합니다. ASA에서는 사용자 항목에 DN이 있는 경우 이 명령을 무시합니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.

사용 지침

subject-name-default 명령은 사용자 이름과 함께 사용되어 발급된 인증서의 주체 이름을 구성하는 공용 일반 DN을 지정합니다. *dn* 값 cn=username만 있으면 이 목적을 충족합니다. 특별히 각 사용자에 대한 주체 이름 DN을 정의할 필요가 없습니다. DN 필드는 **crypto ca server user-db add** dn *dn* 명령을 사용하여 사용자가 추가된 경우의 선택 사항입니다.

ASA에서는 사용자 항목에 DN이 지정되지 않은 경우 인증서를 발급할 때만 이 명령을 사용합니다.

예

다음 예에서는 DN을 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc."
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA의 구성 및 관리를 허용하는 CA 서버 컨피그레이션 모드 CLI 명령 집합에 액세스를 부여합니다.
issuer-name	인증서 인증 기관의 주체 이름 DN을 지정합니다.
keysize	사용자 인증서 등록 시 생성되는 공개 및 개인 키의 크기를 지정합니다.
lifetime	CA 인증서, 발급된 인증서 또는 CRL의 수명을 지정합니다.

subnet

네트워크 개체에 대한 네트워크를 구성하려면 개체 컨피그레이션 모드에서 **subnet** 명령을 사용합니다. 컨피그레이션에서 개체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

subnet {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*}

no subnet {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*}

구문 설명

IPv4_address IPv4_mask	공백으로 구분된 IPv4 네트워크 주소와 서브넷 마스크를 지정합니다.
IPv6_address/IPv6_prefix	공백 없이 / 문자로 구분된 IPv6 네트워크 주소와 접두사 길이를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
개체 네트워크 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령이 도입되었습니다.

사용 지침

다른 IP 주소를 사용하여 기존 네트워크 개체를 구성한 경우 새 컨피그레이션이 기존 컨피그레이션을 대체합니다.

예

다음 예에서는 서브넷 네트워크 개체를 만드는 방법을 보여 줍니다.

```
ciscoasa (config)# object network OBJECT_SUBNET
ciscoasa (config-network-object)# subnet 10.1.1.0 255.255.255.0
```

관련 명령

명령	설명
clear configure object	생성된 모든 개체를 지웁니다.
description	네트워크 개체에 대한 설명을 추가합니다.
fqdn	FQDN(정규화된 도메인 이름) 네트워크 개체를 지정합니다.
host	호스트 네트워크 개체를 지정합니다.
nat	네트워크 개체에 대한 NAT를 활성화합니다.
object network	네트워크 개체를 생성합니다.
object-group network	네트워크 개체 그룹을 생성합니다.
range	네트워크 개체에 대한 주소 범위를 지정합니다.
show running-config object network	네트워크 개체 컨피그레이션을 표시합니다.

summary-address (EIGRP)

특정 인터페이스의 EIGRP에 대한 요약을 구성하려면 인터페이스 컨피그레이션 모드에서 **summary-address** 명령을 사용합니다. 요약 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

summary-address *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

구문 설명

as-number	자동 시스템 번호입니다. EIGRP 라우팅 프로세스의 자동 시스템 번호와 같아야 합니다.
addr	요약 IP 주소입니다.
mask	IP 주소에 적용할 서브넷 마스크입니다.
admin-distance	(선택 사항) 요약 경로의 관리 영역입니다. 유효한 값은 0~255입니다. 지정하지 않을 경우 기본값은 5입니다.

기본값

기본값은 다음과 같습니다.

- EIGRP는 단일 호스트 경로에 대해서도 경로를 네트워크 수준으로 자동으로 요약합니다.
- EIGRP 요약 경로의 관리 영역은 5입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

기본적으로 EIGRP는 서브넷 경로를 네트워크 수준으로 요약합니다. **no auto-summary** 명령을 사용하여 자동 경로 요약을 비활성화할 수 있습니다. **summary-address** 명령을 사용하여 서브넷 경로 요약을 인터페이스별로 수동으로 정의할 수 있습니다.

예

다음 예에서는 **tag**를 3으로 설정하여 경로 요약을 구성합니다.

```
ciscoasa(config-router)# summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

다음 예에서는 기본값으로 다시 설정하는 옵션과 함께 **summary-address** 명령의 **no** 형식을 사용하는 방법을 보여 줍니다. 이 예에서는 이전 예에서3으로 설정된 **tag** 값이 **summary-address** 명령에서 제거되었습니다.

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

다음 예에서는 컨피그레이션에서 **summary-address** 명령을 제거합니다.

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

관련 명령

명령	설명
auto-summary	EIGRP 라우팅 프로세스에 대한 요약 주소를 자동으로 생성합니다.

summary-address (OSPFv2)

OSPF에 대한 집계 주소를 생성하려면 라우터 컨피그레이션 모드에서 **summary-address** 명령을 사용합니다. 요약 주소 또는 특정 요약 주소 옵션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

구문 설명

addr	주소 범위에 대해 지정된 요약 주소 값입니다.
mask	요약 경로에 사용되는 IP 서브넷 마스크입니다.
not-advertise	(선택 사항) 지정된 접두사/마스크 쌍과 일치하는 경로를 무시합니다.
tag *tag_value*	(선택 사항) 각 외부 경로에 연결되는 32비트 10진수 값입니다. 이 값은 OSPF 자체에서 사용되지 않습니다. ASBR 간에 정보를 전달하는 데 사용될 수 있습니다. none을 지정하면 BGP 및 EGP에서의 경로에 원격 자동 시스템 번호가 사용되고, 다른 프로토콜에는 0(영)이 사용됩니다. 유효한 값의 범위는 0~4294967295입니다.

기본값

기본값은 다음과 같습니다.

- *tag_value*는 0입니다.
- 지정된 접두사/마스크 쌍과 일치하는 경로가 무시되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드가 지원됩니다.

사용 지침

다른 라우팅 프로토콜에서 학습된 경로를 요약할 수 있습니다. OSPF에 이 명령을 사용하면 OSPF ASBR(자동 시스템 경계 라우터)이 하나의 외부 경로를 해당 주소가 적용되는 모든 재배포된 경로의 집계로 전달합니다. 이 명령은 OSPF로 재배포되는 다른 라우팅 프로토콜의 경로만 요약합니다. OSPF 영역 간의 경로 요약에는 **area range** 명령을 사용합니다.

컨피그레이션에서 **summary-address** 명령을 제거하려면 선택적 키워드 또는 인수를 지정하지 않고 이 명령의 no 형식을 사용합니다. 컨피그레이션의 요약 명령에서 옵션을 제거하려면 제거할 옵션과 함께 이 명령의 **no** 형식을 사용합니다. 자세한 내용은 "예제" 섹션을 참고하십시오.

예

다음 예에서는 **tag**를 3으로 설정하여 경로 요약을 구성합니다.

```
ciscoasa(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

다음 예에서는 기본값으로 다시 설정하는 옵션과 함께 **summary-address** 명령의 **no** 형식을 사용하는 방법을 보여 줍니다. 이 예에서는 이전 예에서3으로 설정된 **tag** 값이 **summary-address** 명령에서 제거되었습니다.

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

다음 예에서는 컨피그레이션에서 **summary-address** 명령을 제거합니다.

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

관련 명령

명령	설명
area range	영역 경계에서 경로를 통합하고 요약합니다.
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show ospf summary-address	각 OSPF 라우팅 프로세스에 대한 요약 주소 설정을 표시합니다.

summary-prefix (OSPFv3)

IPv6 요약 접두사를 구성하려면 IPv6 라우터 컨피그레이션 모드에서 **summary-prefix** 명령을 사용하려면 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

no summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

구문 설명

not-advertise	(선택 사항) 지정된 접두사/마스크 쌍과 일치하는 경로를 무시합니다. 이 키워드는 OSPFv3에만 적용됩니다.
prefix	대상의 IPv6 접두사를 지정합니다.
tag *tag_value*	(선택 사항) 경로 맵을 통한 재배포를 제어하는 일치 값으로 사용할 수 있는 태그 값을 지정합니다. 이 키워드는 OSPFv3에만 적용됩니다.

기본값

기본값은 다음과 같습니다.

- *tag_value*는 0입니다.
- 지정된 접두사/마스크 쌍과 일치하는 경로가 무시되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
IPv6 라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령이 도입되었습니다.

사용 지침

이 명령을 사용하여 IPv6 요약 접두사를 구성할 수 있습니다.

예

다음 예에서는 요약 접두사 FECO::/24에 FECO::/1~FECO::/24 주소가 포함되어 있습니다. FECO::/24 주소만 외부 LSA에서 전달됩니다.

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 172.16.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

관련 명령

명령	설명
ipv6 router ospf	OSPFv3에 대한 라우터 컨피그레이션 모드를 시작합니다.
redistribute	OSPFv3 라우팅 도메인 간에 IPv6 경로를 재배포합니다.

sunrpc-server

SunRPC 서비스 테이블의 항목을 생성하려면 글로벌 컨피그레이션 모드에서 **sunrpc-server** 명령을 사용합니다. SunRPC 서비스 테이블 항목을 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol [tcp | udp] port** *port* **[-** *port* **] timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol [tcp | udp] port** *port* [*- port*] **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

구문 설명

ifc_name	Server interface name.
ip_addr	SunRPC 서버 IP 주소입니다.
mask	네트워크 마스크입니다.
port *port* [- *port*]	SunRPC 프로토콜 포트 범위를 지정합니다.
port- *port*	(선택 사항) SunRPC 프로토콜 포트 범위를 지정합니다.
protocol tcp	SunRPC 전송 프로토콜을 지정합니다.
protocol udp	SunRPC 전송 프로토콜을 지정합니다.
service	서비스를 지정합니다.
service_type	**sunrpcinfo** 명령에 지정된 대로 SunRPC 서비스 프로그램 번호를 설정합니다.
timeout *hh:mm:ss*	SunRPC 서비스 트래픽에 대한 액세스가 닫히는 유휴 시간 제한을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

SunRPC 서비스 테이블은 시간 제한에 지정된 기간 동안 설정된 SunRPC 세션을 기반으로 SunRPC 트래픽이 ASA를 통과하도록 허용하는 데 사용됩니다.

예

다음 예에서는 SunRPC 서비스 테이블을 생성하는 방법을 보여 줍니다.

```
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

관련 명령

명령	설명
clear configure sunrpc-server	ASA에서 Sun 원격 프로세서 호출 서비스를 지웁니다.
show running-config sunrpc-server	SunRPC 서비스 컨피그레이션에 대한 정보를 표시합니다.

support-user-cert-validation

현재 신뢰 지점이 원격 인증서를 발급한 CA에 인증된 경우 이 신뢰 지점을 기반으로 원격 사용자 인증서를 확인하려면 crypto ca trustpoint 컨피그레이션 모드에서 **support-user-cert-validation** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

support-user-cert-validation

no support-user-cert-validation

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 설정은 사용자 인증서 검증을 지원하는 것입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

ASA에는 CA가 동일한 두 개의 신뢰 지점이 있을 수 있으며, 이 경우 동일한 CA에서 두 개의 ID 인증서가 생성됩니다. 신뢰 지점이 이 기능을 활성화한 다른 신뢰 지점에 이미 연결된 CA에 인증된 경우에는 이 옵션이 자동으로 비활성화됩니다. 따라서 경로 검증 파라미터의 선택 시 모호함이 방지됩니다. 사용자가 이 기능을 활성화한 다른 신뢰 지점에 이미 연결된 CA에 인증된 신뢰 지점에서 이 기능을 활성화하려고 하면 작업이 허용되지 않습니다. 두 개의 신뢰 지점에서 이 설정을 활성화하고 동일한 CA에 인증할 수 없습니다.

예

다음 예에서는 신뢰 지점 central에 대한 crypto ca trustpoint 컨피그레이션 모드를 시작하고 신뢰 지점 central에서 사용자 검증을 허용하도록 합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# support-user-cert-validation
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.
default enrollment	등록 파라미터를 해당 기본값으로 되돌립니다.

sw-module module password-reset

소프트웨어 모듈의 비밀번호를 기본값으로 다시 설정하려면 특권 EXEC 모드에서 **sw-module module password-reset** 명령을 사용합니다.

sw-module module *id* **password-reset**

구문 설명

id	모듈 ID(**cxsc** 또는 **ips**)를 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

명령 모드	방화벽 모드		보안 상황		
				다중 모드	
	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.
9.1(1)	**cxsc** 키워드가 추가되어 ASA CX 소프트웨어 모듈에 대한 지원이 추가되었습니다.

사용 지침

비밀번호를 다시 설정한 후에는 모듈 애플리케이션을 사용하여 고유한 값으로 변경해야 합니다. 모듈 비밀번호를 다시 설정하면 모듈이 재부팅됩니다. 모듈이 재부팅되는 동안에는 서비스를 사용할 수 없으며, 몇 분 정도 걸릴 수 있습니다. **show module** 명령을 실행하여 모듈 상태를 모니터링할 수 있습니다.

이 명령은 항상 확인 프롬프트를 표시합니다. 명령이 성공하면 다른 출력이 표시되지 않습니다. 명령이 실패하면 오류가 발생한 원인을 설명하는 오류 메시지가 표시됩니다.

이 명령은 모듈이 Up 상태인 경우에만 사용할 수 있습니다.

기본 비밀번호는 모듈에 따라 다릅니다.

- ASA IPS - 사용자 cisco에 대한 기본 비밀번호는 **cisco**입니다.
- ASA CX - 사용자 admin에 대한 기본 비밀번호는 **Admin123**입니다.

예

다음 예에서는 IPS 모듈의 비밀번호를 다시 설정합니다.

```
ciscoasa# sw-module module ips password-reset
Reset the password on module ips? [confirm] y
```

관련 명령

명령	설명
sw-module module recover	디스크에서 복구 이미지를 로드하여 모듈을 복구합니다.
sw-module module reload	모듈 소프트웨어를 다시 로드합니다.
sw-module module reset	모듈을 종료하고 다시 로드합니다.
sw-module module shutdown	컨피그레이션 데이터의 손실 없이 전원을 끄려고 준비 중인 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

sw-module module recover

디스크에서 소프트웨어 모듈에 대한 복구 소프트웨어 이미지를 로드하려면 특권 EXEC 모드에서 **sw-module module recover** 명령을 사용합니다. 예를 들어 모듈이 현재 이미지를 로드할 수 없는 경우 이 명령을 사용하여 모듈을 복구해야 할 수 있습니다.

sw-module module *id* **recover** {**boot | stop | configure image** *path*}

구문 설명

id	모듈 ID를 다음 중 하나로 지정합니다. • **sfr** - ASA FirePOWER 모듈 • **ips** - IPS 모듈 • **cxsc** - ASA CX 모듈
boot	이 모듈의 복구를 시작하고 **configure** 설정에 따라 복구 이미지를 다운로드합니다. 그러면 새 이미지에서 모듈이 재부팅됩니다.
configure image *path*	로컬 디스크에서 새 이미지 위치(예: disk0:image2)를 구성합니다.
stop	복구 작업을 중지합니다. 모듈이 원래 이미지에서 부팅됩니다. **sw-module module** *id* **recover boot** 명령을 사용하여 복구를 시작한 후 30초 이내에 이 명령을 입력해야 합니다. 이 기간이 지난 후 **stop** 명령을 실행하면 모듈이 응답하지 않는 등 예상치 못한 결과가 발생할 수 있습니다. 그러나 모듈이 이미 응답하지 않는 경우에는 모듈을 중지해야 재부팅하거나 새 이미지를 적용할 수 있습니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.
9.1(1)	**cxsc** 키워드가 추가되어 ASA CX 소프트웨어 모듈에 대한 지원이 추가되었습니다.
9.2(1)	**sfr** 키워드를 추가하여 ASA FirePOWER 모듈에 대한 지원이 추가되었습니다.

사용 지침

이 명령을 사용하여 소프트웨어 모듈을 설치할 수 있습니다. 이는 디바이스에 아직 구성되지 않은 새 모듈이거나, 장애가 발생하여 다시 설치해야 하는 기존 모듈일 수 있습니다.

이미지를 설치할 때 다음 명령 시퀀스를 사용합니다.

- **sw-module module** *id* **configure image** *path* - disk0에서 소프트웨어 모듈 이미지의 위치를 식별합니다.
- **sw-module module** *id* **boot** - 해당 이미지를 부팅합니다.

모듈이 Up, Down, Unresponsive 또는 Recovery 상태인 경우에만 이미지를 부팅할 수 있습니다. 상태 정보는 **show module** 명령을 참고하십시오. 모듈이 Up 상태가 아닌 경우에는 ASA에서 모듈을 강제로 종료합니다. 강제 종료는 컨피그레이션을 포함하여 이전 모듈 디스크 이미지를 삭제하므로 재해 복구 메커니즘으로만 사용해야 합니다.

show module *id* **recover** 명령을 사용하여 복구 컨피그레이션을 볼 수 있습니다.

참고 IPS 모듈의 경우 모듈 내에서 **upgrade** 명령을 사용하여 이미지를 설치하지 마십시오. 모듈 설치 및 초기 컨피그레이션을 완료하는 방법은 CLI 컨피그레이션 가이드에서 각 소프트웨어 모듈에 대한 장을 참고하십시오.

예

다음 예에서는 disk0:image2에서 이미지를 다운로드하도록 모듈을 설정합니다.

```
ciscoasa# sw-module module ips recover configure image disk0:image2
```

다음 예에서는 모듈을 복구합니다.

```
ciscoasa# sw-module module ips recover boot
The module in slot ips will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot ips? [confirm]
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버그 메시지를 표시합니다.
sw-module module reset	모듈을 종료하고 재설정을 수행합니다.
sw-module module reload	모듈 소프트웨어를 다시 로드합니다.
sw-module module shutdown	컨피그레이션 데이터의 손실 없이 전원을 끄려고 준비 중인 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

sw-module module reload

소프트웨어 모듈에 대한 모듈 소프트웨어를 다시 로드하려면 특권 EXEC 모드에서 **sw-module module reload** 명령을 사용합니다.

sw-module module *id* **reload**

구문 설명

id	모듈 ID를 다음 중 하나로 지정합니다. • **sfr** - ASA FirePOWER 모듈 • **ips** - IPS 모듈 • **cxsc** - ASA CX 모듈

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.
9.1(1)	**cxsc** 키워드가 추가되어 ASA CX 소프트웨어 모듈에 대한 지원이 추가되었습니다.
9.2(1)	**sfr** 키워드를 추가하여 ASA FirePOWER 모듈에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 모듈을 다시 로드하기 전에도 재설정을 수행한다는 점에서 **sw-module module reset** 명령과 다릅니다.

이 명령은 모듈이 Up 상태인 경우에만 사용할 수 있습니다. 상태 정보는 **show module** 명령을 참고하십시오.

예

다음 예에서는 IPS 모듈을 다시 로드합니다.

```
ciscoasa# sw-module module ips reload
Reload module in slot ips? [confirm] y
Reload issued for module in slot ips
%XXX-5-505002: Module in slot ips is reloading.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버그 메시지를 표시합니다.
sw-module module recover	디스크에서 복구 이미지를 로드하여 모듈을 복구합니다.
sw-module module reset	모듈을 종료하고 재설정을 수행합니다.
sw-module module shutdown	컨피그레이션 데이터의 손실 없이 전원을 끄려고 준비 중인 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

sw-module module reset

모듈을 재설정한 다음 모듈 소프트웨어를 다시 로드하려면 특권 EXEC 모드에서 **sw-module module reset** 명령을 사용합니다.

sw-module module *id* **reset**

구문 설명

id	모듈 ID를 다음 중 하나로 지정합니다. • **sfr** - ASA FirePOWER 모듈 • **ips** - IPS 모듈 • **cxsc** - ASA CX 모듈

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.
9.1(1)	**cxsc** 키워드가 추가되어 ASA CX 소프트웨어 모듈에 대한 지원이 추가되었습니다.
9.2(1)	**sfr** 키워드를 추가하여 ASA FirePOWER 모듈에 대한 지원이 추가되었습니다.

사용 지침

모듈이 Up 상태인 경우 **sw-module module reset** 명령은 재설정하기 전에 소프트웨어를 종료하라는 프롬프트를 표시합니다.

sw-module module recover 명령을 사용하여 모듈을 복구할 수 있습니다. 모듈이 Recover 상태에 있는 동안 **sw-module module reset** 명령을 입력한 경우에는 모듈이 복구 프로세스를 중단하지 않습니다. **sw-module module reset** 명령은 모듈의 재설정을 수행하며, 재설정 후 모듈 복구가 계속됩니다. 복구 중에 모듈이 중단된 경우 모듈을 재설정할 수 있습니다. 그러면 문제가 해결될 수도 있습니다.

이 명령은 소프트웨어를 다시 로드하기만 하고 재설정을 수행하지 않는다는 점에서 **sw-module module reload** 명령과 다릅니다.

이 명령은 모듈이 Up, Down, Unresponsive 또는 Recover 상태인 경우에만 사용할 수 있습니다. 상태 정보는 **show module** 명령을 참고하십시오.

예

다음 예에서는 Up 상태의 IPS 모듈을 다시 설정합니다.

```
ciscoasa# sw-module module ips reset
The module in slot ips should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot ips? [confirm] y
Reset issued for module in slot ips
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
%XXX-5-505003: Module in slot ips is resetting.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버그 메시지를 표시합니다.
sw-module module recover	디스크에서 복구 이미지를 로드하여 모듈을 복구합니다.
sw-module module reload	모듈 소프트웨어를 다시 로드합니다.
sw-module module shutdown	컨피그레이션 데이터의 손실 없이 전원을 끄려고 준비 중인 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

sw-module module shutdown

모듈 소프트웨어를 종료하려면 특권 EXEC 모드에서 **sw-module module shutdown** 명령을 사용합니다.

sw-module module *id* **shutdown**

구문 설명

id	모듈 ID를 다음 중 하나로 지정합니다. • **sfr** - ASA FirePOWER 모듈 • **ips** - IPS 모듈 • **cxsc** - ASA CX 모듈

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.
9.1(1)	**cxsc** 키워드가 추가되어 ASA CX 소프트웨어 모듈에 대한 지원이 추가되었습니다.
9.2(1)	**sfr** 키워드를 추가하여 ASA FirePOWER 모듈에 대한 지원이 추가되었습니다.

사용 지침

모듈 소프트웨어를 종료하면 컨피그레이션 데이터 손실 없이 모듈의 전원을 안전하게 끌 수 있도록 준비됩니다.

이 명령은 모듈이 Up 또는 Unresponsive 상태인 경우에만 사용할 수 있습니다. 상태 정보는 **show module** 명령을 참고하십시오.

예

다음 예에서는 IPS 모듈을 종료합니다.

```
ciscoasa# sw-module module ips shutdown
Shutdown module in slot ips? [confirm] y
Shutdown issued for module in slot ips
ciscoasa#
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버깅 메시지를 표시합니다.
sw-module module recover	디스크에서 복구 이미지를 로드하여 모듈을 복구합니다.
sw-module module reload	모듈 소프트웨어를 다시 로드합니다.
sw-module module reset	모듈을 종료하고 재설정을 수행합니다.
show module	모듈 정보를 표시합니다.

sw-module module uninstall

소프트웨어 모듈 이미지 및 관련 컨피그레이션을 제거하려면 특권 EXEC 모드에서 **sw-module module uninstall** 명령을 사용합니다.

sw-module module *id* **uninstall**

구문 설명

id	모듈 ID를 다음 중 하나로 지정합니다. • **sfr** - ASA FirePOWER 모듈 • **ips** - IPS 모듈 • **cxsc** - ASA CX 모듈

명령 기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
특권 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.6(1)	이 명령이 도입되었습니다.
9.1(1)	**cxsc** 키워드가 추가되어 ASA CX 소프트웨어 모듈에 대한 지원이 추가되었습니다.
9.2(1)	**sfr** 키워드를 추가하여 ASA FirePOWER 모듈에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 소프트웨어 모듈 이미지 및 관련 컨피그레이션을 영구적으로 제거합니다.

예

다음 예에서는 IPS 모듈 이미지 및 컨피그레이션을 제거합니다.

```
ciscoasa# sw-module module ips uninstall
Module ips will be uninstalled. This will completely remove the
disk image associated with the sw-module including any configuration
that existed within it.

Uninstall module <id>? [confirm]
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버깅 메시지를 표시합니다.
sw-module module recover	디스크에서 복구 이미지를 로드하여 모듈을 복구합니다.
sw-module module reload	모듈 소프트웨어를 다시 로드합니다.
sw-module module reset	모듈을 종료하고 재설정을 수행합니다.
show module	모듈 정보를 표시합니다.

switchport access vlan

내장형 스위치가 있는 모델(예: ASA 5505 Adaptive Security Appliance)의 경우 VLAN에 스위치 포트를 할당하려면 인터페이스 컨피그레이션 모드에서 **switchport access vlan** 명령을 사용합니다.

switchport access vlan *number*

no switchport access vlan *number*

구문 설명

vlan *number*	이 스위치 포트를 할당할 VLAN ID를 지정합니다. VLAN ID는 1~4090입니다.

기본값

기본적으로 모든 스위치 포트는 VLAN 1에 할당됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

투명 방화벽 모드에서는 ASA 5505 Adaptive Security Appliance Base 라이센스의 경우 2개의 활성 VLAN을 구성하고, Security Plus 라이센스의 경우 3개의 활성 VLAN을 구성할 수 있으며, 그 중 하나는 대체작동용이어야 합니다.

라우팅 모드에서는 ASA 5505 Adaptive Security Appliance Base 라이센스의 경우 최대 3개의 활성 VLAN을 구성하고, Security Plus 라이센스의 경우 최대 20개의 활성 VLAN을 구성할 수 있습니다.

활성 VLAN은 **nameif** 명령이 구성된 VLAN입니다.

switchport access vlan 명령을 사용하여 각 VLAN에 하나 이상의 물리적 인터페이스를 할당할 수 있습니다. 기본적으로 인터페이스의 VLAN 모드는 액세스 포트(인터페이스에 하나의 VLAN이 연결됨)입니다. 인터페이스에서 여러 VLAN을 전달하기 위해 트렁크 포트를 생성하려면 **switchport mode access trunk** 명령을 사용하여 모드를 트렁크 모드로 변경한 다음 **switchport trunk allowed vlan** 명령을 사용합니다.

예

다음 예에서는 3개의 VLAN 인터페이스에 5개의 물리적 인터페이스를 할당합니다.

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

...
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show running-config interface	실행 중인 컨피그레이션에서 인터페이스 컨피그레이션을 표시합니다.
switchport mode	VLAN 모드를 액세스 또는 트렁크로 설정합니다.
switchport protected	보안을 강화하기 위해 스위치 포트가 동일한 VLAN의 다른 스위치 포트와 통신하지 못하도록 합니다.
switchport trunk allowed vlan	트렁크 포트에 VLAN을 할당합니다.

switchport mode

내장형 스위치가 있는 모델(예: ASA 5505 Adaptive Security Appliance)의 경우 VLAN 모드를 액세스(기본값) 또는 트렁크로 설정하려면 인터페이스 컨피그레이션 모드에서 **switchport mode** 명령을 사용합니다.

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

구문 설명

access	스위치 포트를 액세스 모드로 설정합니다. 이 모드에서는 스위치 포트가 하나의 VLAN에 대해서만 트래픽만 트래픽을 전달할 수 있습니다. 패킷은 802.1Q VLAN 태그가 없는 스위치 포트를 나갑니다. 패킷이 태그가 있는 스위치 포트로 들어가면 해당 패킷이 삭제됩니다.
trunk	스위치 포트를 트렁크 모드로 설정합니다. 이 모드에서는 여러 VLAN에 대해 트래픽을 전달할 수 있습니다. 패킷은 802.1Q VLAN 태그가 있는 스위치 포트를 나갑니다. 패킷이 태그가 없는 스위치 포트로 들어가면 해당 패킷이 삭제됩니다.

기본값

기본적으로 모드는 access입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.
7.2(2)	이제 하나의 트렁크로 제한되지 않고 여러 트렁크 포트를 구성할 수 있습니다.

사용 지침

기본적으로 스위치 포트의 VLAN 모드는 액세스 포트(스위치 포트에 하나의 VLAN이 연결됨)입니다. 액세스 모드에서는 **switchport access vlan** 명령을 사용하여 VLAN에 스위치 포트를 할당합니다. 스위치 포트에서 여러 VLAN을 전달하기 위해 트렁크 포트를 생성하려면 **switchport trunk allowed vlan** 명령을 사용하여 여러 VLAN을 트렁크에 할당합니다. 모드를 트렁크 모드로 설정하고 **switchport trunk allowed vlan** 명령을 아직 구성하지 않은 경우에는 스위치 포트가 "line protocol down" 상태로 그대로 유지되고 트래픽 전달에 참가할 수 없습니다. 트렁크 모드는 Security Plus 라이센스에서만 사용할 수 있습니다.

switchport vlan access 명령은 모드가 액세스 모드로 설정된 경우에만 적용됩니다. **switchport trunk allowed vlan** 명령은 모드가 트렁크 모드로 설정된 경우에만 적용됩니다.

예

다음 예에서는 VLAN 100에 할당된 액세스 모드 스위치 포트와 VLAN 200 및 300에 할당된 트렁크 모드 스위치 포트를 구성합니다.

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200,300
ciscoasa(config-if)# no shutdown

...
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show running-config interface	실행 중인 컨피그레이션에서 인터페이스 컨피그레이션을 표시합니다.
switchport access vlan	VLAN에 스위치 포트를 할당합니다.
switchport protected	보안을 강화하기 위해 스위치 포트가 동일한 VLAN의 다른 스위치 포트와 통신하지 못하도록 합니다.
switchport trunk allowed vlan	트렁크 포트에 VLAN을 할당합니다.

switchport monitor

내장형 스위치가 있는 모델(예: ASA 5505 Adaptive Security Appliance)의 경우 SPAN(스위치 포트 모니터링이라고도 함)을 활성화하려면 인터페이스 컨피그레이션 모드에서 **switchport monitor** 명령을 사용합니다. 이 명령을 입력한 포트(대상 포트라고도 함)는 지정된 소스 포트에서 전송되거나 수신되는 모든 패킷의 사본을 받습니다. SPAN 기능을 사용하면 트래픽을 모니터링할 수 있도록 대상 포트에 스니퍼를 연결할 수 있습니다. 이 명령을 여러 번 입력하여 여러 소스 포트를 지정할 수 있습니다. 하나의 대상 포트에 대해서만 SPAN을 활성화할 수 있습니다. 소스 포트의 모니터링을 비활성화하려면 이 명령의 **no** 양식을 사용합니다.

switchport monitor *source_port* [**tx** | **rx** | **both**]

no switchport monitor *source_port* [**tx** | **rx** | **both**]

구문 설명

both	(선택 사항) 전송된 트래픽과 수신된 트래픽을 모두 모니터링하도록 지정합니다. **both**가 기본값입니다.
rx	(선택 사항) 수신된 트래픽만 모니터링하도록 지정합니다.
source_port	모니터링할 포트를 지정합니다. 이더넷 포트뿐 아니라 VLAN 인터페이스 간에 트래픽을 전달하는 Internal-Data0/1 백플레인 포트도 지정할 수 있습니다. Internal-Data0/1 포트는 기가비트 이더넷 포트이므로 고속 이더넷 대상 포트를 트래픽으로 오버로드할 수도 있습니다. 따라서 Internal-Data0/1 포트를 신중하게 모니터링해야 합니다.
tx	(선택 사항) 전송된 트래픽만 모니터링하도록 지정합니다.

기본값

모니터링할 트래픽의 기본 유형은 **both**입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

SPAN를 활성화하지 않은 경우 스위치 포트 중 하나에 스니퍼를 연결하면 해당 포트에서 들어오거나 나가는 트래픽만 캡처됩니다. 여러 포트에서 들어오거나 나가는 트래픽을 캡처하려면 SPAN을 활성화하고 모니터링할 포트를 식별해야 합니다.

SPAN 대상 포트를 다른 포트에 연결하는 동안 네트워크 루프가 발생할 수 있으므로 주의해야 합니다.

예

다음 예에서는 Ethernet 0/1 포트를 Ethernet 0/0 및 Ethernet 0/2 포트를 모니터링하는 대상 포트로 구성합니다.

```
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport monitor ethernet 0/0
ciscoasa(config-if)# switchport monitor ethernet 0/2
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show running-config interface	실행 중인 컨피그레이션에서 인터페이스 컨피그레이션을 표시합니다.
switchport access vlan	VLAN에 스위치 포트를 할당합니다.
switchport protected	보안을 강화하기 위해 스위치 포트가 동일한 VLAN의 다른 스위치 포트와 통신하지 못하도록 합니다.

switchport protected

내장형 스위치가 있는 모델(예: ASA 5505 Adaptive Security Appliance)의 경우 스위치 포트가 동일한 VLAN의 보호된 다른 스위치 포트와 통신하지 못하도록 하려면 인터페이스 컨피그레이션 모드에서 **switchport protected** 명령을 사용합니다. 이 기능은 하나의 스위치 포트가 손상된 경우 VLAN의 다른 스위치 포트에 대한 보안을 강화합니다.

switchport protected

no switchport protected

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 인터페이스는 보호되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.

사용 지침

스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되는 경우 VLAN 간 액세스를 허용하지 않고 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하기 위해 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우 **switchport protected** 명령을 각 스위치 포트에 적용하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버 모두와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.

보호되지 않는 포트와의 통신은 이 명령으로 제한되지 않습니다.

예

다음 예에서는 7개의 스위치 포트를 구성합니다. Ethernet 0/4, 0/5 및 0/6이 DMZ 네트워크에 할당되고 서로 보호됩니다.

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
```

```
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/5
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/6
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown

...
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show running-config interface	실행 중인 컨피그레이션에서 인터페이스 컨피그레이션을 표시합니다.
switchport access vlan	VLAN에 스위치 포트를 할당합니다.
switchport mode	VLAN 모드를 액세스 또는 트렁크로 설정합니다.
switchport trunk allowed vlan	트렁크 포트에 VLAN을 할당합니다.

switchport trunk

내장형 스위치가 있는 모델(예: ASA 5505 Adaptive Security Appliance)의 경우 VLAN을 트렁크 포트에 할당하려면 인터페이스 컨피그레이션 모드에서 **switchport trunk** 명령을 사용합니다. 트렁크에서 VLAN을 제거하려면 이 명령의 **no** 형식을 사용합니다.

switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

구문 설명

allowed vlans *vlan_range*	트렁크 포트에 할당할 수 있는 하나 이상의 VLAN을 식별합니다. VLAN ID는 1~4090입니다. *vlan_range*는 다음 방법 중 하나로 식별될 수 있습니다. • 단일 번호(n) • 범위(n-x) 쉼표로 구분된 번호와 범위(예: 5,7-10,13,45-100) 쉼표 대신 공백을 입력할 수 있지만 이 명령은 쉼표 컨피그레이션에 저장됩니다. 이 명령에 네이티브 VLAN을 포함할 수 있지만 이는 선택 사항입니다. 네이티브 VLAN은 이 명령에 포함되었는지 여부에 상관없이 전달됩니다.
native vlan *vlan*	트렁크에 네이티브 VLAN을 할당합니다. 네이티브 VLAN의 패킷은 트렁크를 통해 전송될 때 수정되지 않습니다. 예를 들어 포트에 VLAN 2, 3 및 4가 할당된 경우 VLAN 2가 네이티브 VLAN이면 포트를 이그레스하는 VLAN 2의 패킷이 802.1Q 헤더로 수정되지 않습니다. 이 포트로 인그레스(진입)하고 802.1Q 헤더가 없는 프레임은 VLAN 2에 배치됩니다. 각 포트에는 하나의 VLAN만 있을 수 있지만 모든 포트의 네이티브 VLAN이 같거나 다를 수 있습니다.

기본값

기본적으로 VLAN은 트렁크에 할당되지 않습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령이 도입되었습니다.
7.2(2)	스위치 포트당 3개 이상의 VLAN을 허용하도록 이 명령이 수정되었습니다. 이제 하나로만 제한되지 않고 여러 트렁크 포트를 구성할 수도 있습니다. 또한 이 명령에서는 공백 대신 쉼표를 사용하여 VLAN ID를 구분합니다.
7.2(4)/8.0(4)	**native vlan** 키워드와 함께 네이티브 VLAN 지원이 도입되었습니다.

사용 지침

스위치 포트에서 여러 VLAN을 전달하기 위해 트렁크 포트를 생성하려면 **switchport mode trunk** 명령을 사용하여 모드를 트렁크 모드로 설정한 다음 **switchport trunk** 명령을 사용하여 트렁크에 VLAN을 할당합니다. 이 스위치 포트는 하나 이상의 VLAN을 할당해야 트래픽을 전달할 수 있습니다. 모드를 트렁크 모드로 설정하고 **switchport trunk allowed vlan** 명령을 아직 구성하지 않은 경우에는 스위치 포트가 "line protocol down" 상태로 그대로 유지되고 트래픽 전달에 참가할 수 없습니다. 트렁크 모드는 Security Plus 라이센스에서만 사용할 수 있습니다. **switchport trunk** 명령은 **switchport mode trunk** 명령을 사용하여 모드를 트렁크 모드로 설정해야 적용됩니다.

참고 이 명령은 버전 7.2(1)로 다운그레이드할 수 없습니다. VLAN을 구분하는 쉼표는 7.2(1)에서 인식되지 않습니다. 다운그레이드할 경우 VLAN을 공백으로 구분하고 3개의 VLAN 제한을 초과하지 않아야 합니다.

예

다음 예에서는 **failover lan** 명령을 사용하여 구성된 대체작동 인터페이스를 포함하여 7개의 VLAN 인터페이스를 구성합니다. VLANs 200, 201 및 202는 Ethernet 0/1에서 트렁크됩니다.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 201
ciscoasa(config-if)# nameif dept1
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 202
ciscoasa(config-if)# nameif dept2
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.3.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200-202
ciscoasa(config-if)# switchport trunk native vlan 5
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show running-config interface	실행 중인 컨피그레이션에서 인터페이스 컨피그레이션을 표시합니다.
switchport access vlan	VLAN에 스위치 포트를 할당합니다.
switchport mode	VLAN 모드를 액세스 또는 트렁크로 설정합니다.
switchport protected	보안을 강화하기 위해 스위치 포트가 동일한 VLAN의 다른 스위치 포트와 통신하지 못하도록 합니다.

synack-data

데이터가 포함된 TCP SYNACK 패킷에 대한 작업을 설정하려면 tcp-map 컨피그레이션 모드에서 **synack-data** 명령을 사용합니다. 이 값을 다시 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 **set connection advanced-options** 명령을 사용하여 활성화된 TCP 정규화 정책의 일부입니다.

synack-data {**allow** | **drop**}

no synack-data

구문 설명

allow	데이터가 포함된 TCP SYNACK 패킷을 허용합니다.
drop	데이터가 포함된 TCP SYNACK 패킷을 삭제합니다.

기본값

기본 동작은 데이터가 포함된 TCP SYNACK 패킷을 삭제하는 것입니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(4)/8.0(4)	이 명령이 도입되었습니다.

사용 지침

TCP 정규화를 활성화하려면 MPF(Modular Policy Framework)를 사용합니다.

1. **tcp-map** - TCP 정규화 작업을 식별합니다.
   a. **synack-data** - tcp-map 컨피그레이션 모드에서 **synack-data** 명령 및 기타 여러 명령을 입력할 수 있습니다.
2. **class-map** - TCP 정규화를 수행할 트래픽을 식별합니다.
3. **policy-map** - 각 클래스 맵과 연계된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **set connection advanced-options** - 생성한 tcp-map을 식별합니다.
4. **service-policy** - 하나의 인터페이스 또는 전역적으로 정책 맵을 할당합니다.

예

다음 예에서는 데이터가 포함된 TCP SYNACK 패킷을 허용하도록 ASA를 설정합니다.

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# synack-data allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

관련 명령

명령	설명
class-map	서비스 정책의 트래픽을 식별합니다.
policy-map	서비스 정책의 트래픽에 적용할 작업을 식별합니다.
set connection advanced-options	TCP 정규화를 활성화합니다.
service-policy	인터페이스에 서비스 정책을 적용합니다.
show running-config tcp-map	TCP 맵 컨피그레이션을 표시합니다.
tcp-map	TCP 맵을 만들고 tcp-map 컨피그레이션 모드에 대한 액세스를 허용합니다.

synchronization

BGP 및 IGP(내부 게이트웨이 프로토콜) 시스템 간의 동기화를 활성화하려면 주소 패밀리 컨피그레이션 모드에서 **synchronization** 명령을 사용합니다. Cisco IOS 소프트웨어에서 IGP를 기다리지 않고 네트워크 경로를 전달할 수 있도록 하려면 이 명령의 **no** 형식을 사용합니다.

synchronization

no synchronization

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
address-family 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령이 도입되었습니다.

사용 지침

일반적으로 BGP 스피커는 경로가 로컬이거나 IGP에 존재하지 않는 한 외부 네이버에 경로를 전달하지 않습니다. 기본적으로 BGP와 IGP 간의 동기화는 Cisco IOS 소프트웨어가 IGP의 경로 검증을 기다리지 않고 네트워크 경로를 전달할 수 있도록 해제되어 있습니다. 이 기능을 사용하면 자동 시스템 내의 라우터 및 액세스 서버가 BGP에서 다른 자동 시스템에 사용할 수 있도록 지정하기 전에 경로를 가질 수 있습니다.

자동 시스템의 라우터가 BGP를 전달하지 않는 경우 **synchronization** 명령을 사용합니다.

예

다음 예에서는 주소 패밀리 컨피그레이션 모드에서 동기화를 활성화하는 방법을 보여 줍니다. 라우터는 경로를 외부에 전달하기 전에 해당 IGP에서 네트워크 경로를 확인합니다.

```
ciscoasa(config)# router bgp 65120
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# synchronization
```

syn-data

데이터가 있는 SYN 패킷을 허용하거나 거부하려면 tcp-map 컨피그레이션 모드에서 **syn-data** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

구문 설명

allow	데이터가 포함된 SYN 패킷을 허용합니다.
drop	데이터가 포함된 SYN 패킷을 삭제합니다.

기본값

SYN 데이터가 있는 패킷은 기본적으로 허용됩니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

tcp map 명령은 MPF(Modular Policy Framework) 인프라와 함께 사용됩니다. **class-map** 명령을 사용하여 트래픽의 클래스를 정의하고, **tcp-map** 명령을 사용하여 TCP 검사를 사용자 지정합니다. 새 TCP 맵은 **policy-map** 명령을 사용하여 적용합니다. TCP 검사는 **service-policy** 명령을 사용하여 활성화합니다.

tcp-map 명령을 사용하여 tcp-map 컨피그레이션 모드를 시작할 수 있습니다. tcp-map 컨피그레이션 모드에서 **syn-data** 명령을 사용하여 SYN 패킷에서 데이터가 있는 패킷을 삭제할 수 있습니다.

TCP 사양에 따라, SYN 패킷에 포함된 데이터를 허용하려면 TCP 구현이 필요합니다. 이는 명확하지 않기 때문에 일부 구현에서는 이를 올바르게 처리하지 못할 수 있습니다. 잘못된 엔드 시스템 구현과 관련된 삽입 공격에 대한 취약점을 방지하기 위해 SYN 패킷에서 데이터가 포함된 패킷을 삭제하도록 선택할 수 있습니다.

예

다음 예에서는 모든 TCP 흐름에서 데이터가 포함된 SYN 패킷을 삭제하는 방법을 보여 줍니다.

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# syn-data drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 컨피그레이션 모드에 대한 액세스를 허용합니다.

sysopt connection permit-vpn

VPN 터널을 통해 ASA에 진입한 다음 암호가 해독되는 트래픽의 경우 글로벌 컨피그레이션 모드에서 **sysopt connection permit-vpn** 명령을 사용하여 트래픽이 인터페이스 액세스 목록을 우회하도록 허용할 수 있습니다. 그룹 정책 및 사용자별 권한 부여 액세스 목록이 트래픽에 계속 적용됩니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

sysopt connection permit-vpn

no sysopt connection permit-vpn

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 기능은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 이제 기본적으로 활성화되어 있습니다. 또한 인터페이스 액세스 목록만 우회됩니다. 그룹 정책 또는 사용자별 액세스 목록은 그대로 적용됩니다.
7.1(1)	이 명령이 **sysopt connection permit-ipsec**에서 변경되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

기본적으로 ASA는 VPN 트래픽이 ASA 인터페이스에서 종료되도록 허용합니다. 인터페이스 액세스 목록에서 IKE 또는 ESP(또는 다른 유형의 VPN 패킷)를 허용하지 않아도 됩니다. 또한 기본적으로 암호 해독된 VPN 패킷의 로컬 IP 주소에 대한 인터페이스 액세스 목록이 필요 없습니다. VPN 터널이 VPN 보안 메커니즘을 통해 성공적으로 종료되므로 이 기능은 보안 위험 없이 컨피그레이션을 간소화하고 ASA 성능을 극대화합니다. 그룹 정책 및 사용자별 권한 부여 액세스 목록이 트래픽에 계속 적용됩니다.

no sysopt connection permit-vpn 명령을 입력하여 인터페이스 액세스 목록을 로컬 IP 주소에 적용해야 하도록 할 수 있습니다. 액세스 목록을 생성하여 인터페이스에 적용하려면 **access-list** 및 **access-group** 명령을 참고하십시오. 액세스 목록은 로컬 IP 주소에 적용되며, VPN 패킷이 암호 해독되기 전에 사용된 원래 클라이언트 IP 주소에는 적용되지 않습니다.

예

다음 예에서는 암호 해독된 VPN 트래픽이 인터페이스 액세스 목록을 준수하도록 설정합니다.

```
ciscoasa(config)# no sysopt connection permit-vpn
```

관련 명령

명령	설명
clear configure sysopt	**sysopt** 명령 컨피그레이션을 지웁니다.
show running-config sysopt	**sysopt** 명령 컨피그레이션을 표시합니다.
sysopt connection tcpmss	최대 TCP 세그먼트 크기를 재정의하거나 최대값이 지정된 크기 이상이 되도록 합니다.
sysopt connection timewait	최종 일반 TCP close-down 시퀀스 후 각 TCP 연결이 단축된 TIME_WAIT 상태로 남아 있도록 합니다.

sysopt connection preserve-vpn-flows

터널이 삭제되고 복구된 후 시간 제한 기간 내에 상태 저장(TCP) 터널링된 IPsec LAN-to-LAN 트래픽을 유지하고 다시 시작하려면 **sysopt connection preserve-vpn-flows** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 기능은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

영구 IPsec 터널링된 흐름 기능이 활성화된 경우 터널이 시간 제한 기간 내에서 다시 생성되는 한, 데이터 흐름이 정상적으로 지속됩니다. 이는 보안 어플라이언스가 원래 흐름에서 상태 정보에 대한 액세스 권한을 계속 유지하기 때문입니다.

이 명령은 네트워크 확장 모드를 포함하여 IPsec LAN-to-LAN 터널만 지원합니다. AnyConnect/SSL VPN 또는 IPsec 원격 액세스 터널은 지원되지 않습니다.

예

다음 예에서는 터널이 삭제되고 시간 제한 기간 내에 재설정된 후 터널의 상태 정보가 유지되고 터널링된 IPsec LAN-to-LAN VPN 트래픽이 다시 시작되도록 지정합니다.

```
ciscoasa(config)# no sysopt connection preserve-vpn-flows
```

이 기능이 활성화되어 있는지 확인하려면 sysopt에 대해 show run all show 명령을 입력합니다.

```
ciscoasa(config)# show run all sysopt
```

샘플 결과는 다음과 같습니다. 설명을 위해 이 예와 다음의 모든 예에서 preserve-vpn-flows 항목이 굵게 표시되어 있습니다.

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

기존 VPN 흐름을 다시 분류하려면 글로벌 컨피그레이션 모드에서 **sysopt connection reclassify-vpn** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

sysopt connection reclassify-vpn

no sysopt connection reclassify-vpn

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 기능은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령이 도입되었습니다.
9.0(1)	다중 상황 모드 지원이 추가되었습니다.

사용 지침

VPN 터널이 있는 경우 이 명령은 기존 VPN 흐름을 다시 분류하여 암호화가 필요한 흐름이 끊어졌다가 다시 생성되도록 합니다.

이 명령은 LAN-to-LAN 및 동적 VPN에만 적용됩니다. EZVPN 또는 VPN 클라이언트 연결은 영향을 받지 않습니다.

예

다음 예에서는 VPN 재분류를 활성화합니다.

```
ciscoasa(config)# sysopt connection reclassify-vpn
```

관련 명령

명령	설명
clear configure sysopt	**sysopt** 명령 컨피그레이션을 지웁니다.
show running-config sysopt	**sysopt** 명령 컨피그레이션을 표시합니다.
sysopt connection permit-vpn	인터페이스에 대한 액세스 목록을 확인하지 않고 IPsec 터널에서 전달되는 모든 패킷을 허용합니다.
sysopt connection tcpmss	최대 TCP 세그먼트 크기를 재정의하거나 최대값이 지정된 크기 이상이 되도록 합니다.
sysopt connection timewait	최종 일반 TCP close-down 시퀀스 후 각 TCP 연결이 단축된 TIME_WAIT 상태로 남아 있도록 합니다.

sysopt connection tcpmss

최대 TCP 세그먼트 크기가 설정한 값을 초과하지 않고 최대값이 지정된 크기보다 작지 않도록 하려면 글로벌 컨피그레이션 모드에서 **sysopt connection tcpmss** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

구문 설명

bytes	최대 TCP 세그먼트 크기(바이트)를 48에서 최대값 사이로 설정합니다. 기본값은 1380바이트입니다. *bytes*를 0으로 설정하여 이 기능을 비활성화할 수 있습니다. **minimum** 키워드의 경우 *bytes*는 허용되는 가장 작은 최대값을 나타냅니다.
minimum	최대 세그먼트 크기를 48~65535바이트 범위에서 *bytes*보다 작지 않은 값으로 재정의합니다. 이 기능은 기본적으로 비활성화되어 있습니다(0으로 설정).

기본값

기본 최대값은 1380바이트입니다. 최소값 기능은 기본적으로 비활성화되어 있습니다(0으로 설정).

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

연결을 먼저 설정한 경우 호스트와 서버 모두 최대 세그먼트 크기를 설정할 수 있습니다. 두 최대값 중 하나가 **sysopt connection tcpmss** 명령을 사용하여 설정한 값을 초과하면 ASA에서 최대값을 재정의하여 설정한 값을 삽입합니다. 두 최대값 중 하나가 **sysopt connection tcpmss minimum** 명령을 사용하여 설정한 값보다 작으면 ASA에서 최대값을 재정의하여 설정한 "최소"값(실제로 최소값은 허용되는 가장 작은 최대값임)을 삽입합니다. 예를 들어 최대 크기를 1200바이트로 설정하고 최소 크기를 400바이트로 설정한 경우 호스트에서 1300바이트의 최대 크기를 요청하면 ASA에서 1200바이트(최대값)를 요청하도록 패킷을 변경합니다. 다른 호스트에서 300바이트의 최대값을 요청하는 경우에는 ASA에서 400바이트(최소값)를 요청하도록 패킷을 변경합니다.

기본값 1380바이트는 총 패킷 크기가 이더넷의 기본 MTU인 1500바이트를 초과하지 않도록 헤더 정보에 대한 여유를 제공합니다. 다음 계산을 참고하십시오.

1380 데이터 + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1500바이트

호스트 또는 서버에서 최대 세그먼트 크기를 요청하지 않는 경우 ASA는 RFC 793 기본값 536바이트가 적용되는 것으로 간주합니다.

최대 크기를 1380보다 크게 설정하면 MTU 크기(기본적으로 1500바이트)에 따라 패킷이 조각화될 수 있습니다. 프래그먼트가 많으면 Frag Guard 기능을 사용할 때 ASA의 성능이 영향을 받을 수 있습니다. 최소 크기를 설정하면 TCP 서버가 작은 TCP 데이터 패킷을 클라이언트로 많이 보내 서버 및 네트워크의 성능에 영향에 미치는 것을 방지할 수 있습니다.

참고 이 기능의 일반적인 사용에는 권장되지 않지만 syslog IPFRAG 메시지 209001 및 209002가 발생한 경우 *bytes* 값을 높일 수 있습니다.

예

다음 예에서는 최대 크기를 1200으로 설정하고, 최소 크기를 400으로 설정합니다.

```
ciscoasa(config)# sysopt connection tcpmss 1200
ciscoasa(config)# sysopt connection tcpmss minimum 400
```

관련 명령

명령	설명
clear configure sysopt	**sysopt** 명령 컨피그레이션을 지웁니다.
show running-config sysopt	**sysopt** 명령 컨피그레이션을 표시합니다.
sysopt connection permit-ipsec	인터페이스에 대한 ACL을 확인하지 않고 IPsec 터널에서 전달되는 모든 패킷을 허용합니다.
sysopt connection timewait	최종 일반 TCP close-down 시퀀스 후 각 TCP 연결이 단축된 TIME_WAIT 상태로 남아 있도록 합니다.

sysopt connection timewait

최종 일반 TCP close-down 시퀀스 후 각 TCP 연결이 최소 15초의 단축된 TIME_WAIT 상태로 남아 있도록 하려면 글로벌 컨피그레이션 모드에서 **sysopt connection timewait** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 종단 호스트 애플리케이션의 기본 TCP 종료 시퀀스가 동시 닫힘인 경우 이 기능을 사용할 수 있습니다.

sysopt connection timewait

no sysopt connection timewait

참고 RST 패킷(일반 TCP close-down 시퀀스가 아님)도 15초 지연을 트리거합니다. ASA는 연결의 마지막 패킷(FIN/ACK 또는 RST)을 받은 후 15초 동안 연결을 유지합니다.

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 기능은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

ASA의 기본 동작은 종료 시퀀스를 추적하고 마지막 FIN 세그먼트의 두 FIN 및 ACK 후 연결을 해제하는 것입니다. 이 빠른 해제 추론은 ASA가 가장 일반적인 닫기 시퀀스(일반 닫기 시퀀스라고 함)에 따라 높은 연결률을 유지할 수 있도록 해줍니다. 그러나 동시 닫기에서는 한 쪽 종단이 닫히고 다른 쪽 종단이 닫기 시퀀스를 시작하기 전에 확인 응답을 보내는 일반 닫기 시퀀스와 달리, 트랜잭션의 두 종단 모두에서 닫기 시퀀스를 시작합니다(RFC 793 참고). 따라서 동시 닫기에서는 빠른 해제 시 연결의 한 쪽 종단이 강제로 CLOSING 상태로 유지됩니다. CLOSING 상태의 소켓이 많으면 종단 호스트의 성능이 저하될 수 있습니다. 예를 들어 일부 Winsock 메인프레임 클라이언트는 이 동작을 실행하여 메인프레임 서버의 성능을 저하시킵니다. **sysopt connection timewait** 명령을 사용하면 동시 종료 시퀀스가 완료될 때까지의 기간이 생성됩니다.

예

다음 예에서는 timewait 기능을 활성화합니다.

```
ciscoasa(config)# sysopt connection timewait
```

관련 명령

명령	설명
clear configure sysopt	**sysopt** 명령 컨피그레이션을 지웁니다.
show running-config sysopt	**sysopt** 명령 컨피그레이션을 표시합니다.
sysopt connection permit-ipsec	인터페이스에 대한 ACL을 확인하지 않고 IPsec 터널에서 전달되는 모든 패킷을 허용합니다.
sysopt connection tcpmss	최대 TCP 세그먼트 크기를 재정의하거나 최대값이 지정된 크기 이상이 되도록 합니다.

sysopt noproxyarp

인터페이스에서 NAT 전역 주소 또는 VPN 클라이언트 주소에 대한 프록시 ARP를 비활성화하려면 글로벌 컨피그레이션 모드에서 **sysopt noproxyarp** 명령을 사용합니다. 프록시 ARP를 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

구문 설명

interface_name	프록시 ARP를 비활성화할 인터페이스 이름입니다.

기본값

프록시 ARP는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(3)	VPN 클라이언트 주소가 내부 네트워크와 겹치는 경우 VPN 프록시 ARP에 영향을 주도록 이 명령이 확장되었습니다.

사용 지침

기존 네트워크와 겹치는 VPN 클라이언트 주소 풀이 있는 경우 ASA는 기본적으로 모든 인터페이스에서 프록시 ARP를 전송합니다. 동일한 계층 2 도메인에 다른 인터페이스가 있는 경우 ASA는 ARP 요청을 보고 해당 인터페이스의 MAC 주소로 응답합니다. 따라서 내부 호스트로 반환되는 VPN 클라이언트의 트래픽이 잘못된 인터페이스로 이동하여 삭제됩니다. 이 경우 프록시 ARP가 필요 없는 인터페이스에 대해 **sysopt noproxyarp** 명령을 입력해야 합니다.

간혹 NAT 전역 주소에 대해 프록시 ARP를 비활성화할 수 있습니다.

호스트에서 동일한 이더넷 네트워크에 있는 다른 디바이스로 IP 트래픽을 보내는 경우 해당 디바이스의 MAC 주소를 알아야 합니다. ARP는 IP 주소를 MAC 주소로 확인하는 계층 2 프로토콜입니다. 호스트가 "Who is this IP address?"라는 ARP 요청을 보내면 IP 주소를 소유한 디바이스가 "I own that IP address; here is my MAC address"라고 응답합니다.

프록시 ARP를 사용하면 디바이스가 IP 주소를 소유하지 않은 경우에도 자신의 MAC 주소로 ARP 요청에 응답합니다. ASA에서는 NAT를 구성하고 ASA 인터페이스와 동일한 네트워크에 있는 전역 주소를 지정할 때 프록시 ARP를 사용합니다. 트래픽이 호스트에 도달하려면 ASA에서 프록시 ARP를 사용하여 ASA MAC 주소가 대상 전역 주소에 할당되어 있음을 클레임해야 합니다.

예

다음 예에서는 내부 인터페이스에서 프록시 ARP를 비활성화합니다.

```
ciscoasa(config)# sysopt noproxyarp inside
```

관련 명령

명령	설명
alias	외부 주소를 변환하고 이 변환을 수용하도록 DNS 레코드를 변경합니다.
clear configure sysopt	**sysopt** 명령 컨피그레이션을 지웁니다.
show running-config sysopt	**sysopt** 명령 컨피그레이션을 표시합니다.
sysopt nodnsalias	**alias** 명령을 사용할 때 DNS A 레코드 주소의 변경을 비활성화합니다.

sysopt radius ignore-secret

RADIUS 계정 관리 응답에서 인증 키를 무시하려면 글로벌 컨피그레이션 모드에서 **sysopt radius ignore-secret** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 일부 RADIUS 서버와의 호환성을 위해 키를 무시해야 할 수도 있습니다.

sysopt radius ignore-secret

no sysopt radius ignore-secret

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 기능은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서 명령을 입력할 수 있는 모드를 확인할 수 있습니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령이 도입되었습니다.

사용 지침

일부 RADIUS 서버는 계정 관리 확인 응답 내에서 인증자 해시에 키를 포함할 수 없습니다. 이로 인해 ASA가 계정 관리 요청을 지속적으로 재전송할 수 있습니다. **sysopt radius ignore-secret** 명령을 사용하여 이러한 확인 응답에서 키를 무시함으로써 재전송 문제를 방지할 수 있습니다. 여기서 식별되는 키는 **aaa-server host** 명령을 사용하여 설정한 키와 같습니다.

예

다음 예에서는 계정 관리 응답에서 인증 키를 무시합니다.

```
ciscoasa(config)# sysopt radius ignore-secret
```

관련 명령

명령	설명
aaa-server host	AAA 서버를 식별합니다.
clear configure sysopt	**sysopt** 명령 컨피그레이션을 지웁니다.
show running-config sysopt	**sysopt** 명령 컨피그레이션을 표시합니다.