Cisco ASA Series 명령 참조, I~R 명령

업데이트 날짜: 2014년 11월 12일

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트
www.cisco.com/go/offices에서 확인하십시오.

텍스트 파트 번호: 해당 사항 없음, 온라인 전용

Cisco ASA Series 명령 참조, I~R 명령

파트 1

I 명령

1 장

icmp through import webvpn webcontent 명령

icmp

ASA 인터페이스에서 종료되는 ICMP 트래픽에 대한 액세스 규칙을 구성하려면 **icmp** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

구문 설명

deny	조건이 일치하는 경우 액세스를 거부합니다.
icmp_type	(선택 사항) ICMP 메시지 유형입니다(표 1-1 참조).
if_name	인터페이스 이름입니다.
ip_address	인터페이스에 ICMP 메시지를 전송하는 호스트의 IP 주소입니다.
net_mask	호스트의 IP 주소에 적용할 네트워크 마스크입니다.
permit	조건이 일치하는 경우 액세스를 허용합니다.

기본값

ASA의 기본 동작은 ASA 인터페이스에 대한 모든 ICMP 트래픽을 허용하는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

icmp 명령은 임의의 ASA 인터페이스에서 종료되는 ICMP 트래픽을 제어합니다. 구성된 ICMP 제어 리스트가 없는 경우 ASA는 외부 인터페이스를 포함하여 임의의 인터페이스에서 종료되는 모든 ICMP 트래픽을 허용합니다. 그러나 기본적으로 ASA는 브로드캐스트 주소로 전달되는 ICMP 에코 요청에 응답하지 않습니다.

ASA는 트래픽이 들어오는 인터페이스로 전송되는 ICMP 트래픽에만 응답합니다. 인터페이스를 통해 먼 인터페이스로 ICMP 트래픽을 전송할 수 없습니다.

icmp deny 명령은 인터페이스에 대한 ping을 비활성화하고 **icmp permit** 명령은 인터페이스에 대한 ping을 활성화합니다. Ping이 비활성화되면 네트워크에서 ASA를 감지할 수 없습니다. 이를 구성 가능한 프록시 ping이라고도 합니다.

보호되는 인터페이스의 목적지에 대한 ASA를 통해 라우팅되는 ICMP 트래픽에는 **access-list extended** 또는 **access-group** 명령을 사용합니다.

ICMP Unreachable 메시지 유형(type 3)은 허용하는 것이 좋습니다. ICMP Unreachable 메시지를 거부하면 ICMP 경로 MTU 검색이 비활성화되고, 그 결과 IPsec 및 PPTP 트래픽이 정지할 수 있습니다. 경로 MTU 검색에 대한 자세한 내용은 RFC 1195 및 RFC 1435를 참조하십시오.

인터페이스에 대해 ICMP 제어 리스트가 구성된 경우 ASA는 먼저 지정된 ICMP 트래픽을 확인한 다음 해당 인터페이스에서 다른 모든 ICMP 트래픽에 대해 암시적 거부를 적용합니다. 첫 번째 일치 엔트리가 허용 엔트리이면 ICMP 패킷이 계속 처리됩니다. 첫 번째 일치 엔트리가 거부 엔트리이거나 엔트리가 일치하지 않으면 ASA는 ICMP 패킷을 삭제하고 syslog 메시지를 생성합니다. ICMP 제어 리스트가 구성되지 않은 경우는 예외입니다. 이 경우에는 허용 명령문으로 간주됩니다.

표 1-1은 지원되는 ICMP 유형 값을 나열합니다.

표 1-1 ICMP 유형 및 리터럴

ICMP 유형	리터럴
0	echo-reply
3	unreachable
8	echo
11	time-exceeded

예

다음 예는 모든 ping 요청을 거부하고 외부 인터페이스의 모든 Unreachable 메시지를 허용합니다.

```
ciscoasa(config)# icmp permit any unreachable outside
```

ICMP 트래픽을 거부할 각각의 추가 인터페이스에 대해 계속해서 **icmp deny any** *interface* 명령을 입력합니다.

다음 예는 호스트 172.16.2.15 또는 서브넷 172.22.1.0/16의 호스트에서 외부 인터페이스를 ping하도록 허용합니다.

```
ciscoasa(config)# icmp permit host 172.16.2.15 echo-reply outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
ciscoasa(config)# icmp permit any unreachable outside
```

관련 명령

명령	설명
clear configure icmp	ICMP 컨피그레이션을 지웁니다.
debug icmp	ICMP에 대한 디버그 정보의 표시를 활성화합니다.
show icmp	ICMP 컨피그레이션을 표시합니다.
timeout icmp	ICMP의 유휴 시간 제한을 구성합니다.

icmp unreachable

ASA 인터페이스에서 종료되는 ICMP 트래픽에 대해 Unreachable ICMP 메시지 속도 제한을 구성하려면 **icmp unreachable** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

icmp unreachable rate-limit *rate* **burst-size** *size*

no icmp unreachable rate-limit *rate* **burst-size** *size*

구문 설명

rate-limit *rate*	Unreachable 메시지의 속도 제한을 설정합니다(초당 메시지 1~100개). 기본값은 초당 메시지 1개입니다.
burst-size *size*	버스트 속도를 설정합니다(1~10). 이 키워드는 현재 시스템에서 사용되지 않으므로 아무 값이나 선택할 수 있습니다.

기본값

기본값 속도 제한은 초당 메시지 1개입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(2)	이 명령이 추가되었습니다.

사용 지침

Unreachable 메시지를 비롯한 ICMP 메시지가 ASA 인터페이스에서 종료되도록 허용하려면(**icmp** 명령 참조) Unreachable 메시지의 속도를 제어할 수 있습니다.

ASA를 홉(hop) 중 하나로 표시하는 traceroute를 ASA 전체에서 허용하려면 **set connection decrement-ttl** 명령과 함께 이 명령을 사용해야 합니다.

예

다음 예는 TTL(Time to Live) 감소를 활성화하고 ICMP Unreachable 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 permit host 172.16.2.15 echo-reply outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
ciscoasa(config)# icmp permit any unreachable outside
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 1
```

관련 명령

명령	설명
clear configure icmp	ICMP 컨피그레이션을 지웁니다.
debug icmp	ICMP에 대한 디버그 정보의 표시를 활성화합니다.
set connection decrement-ttl	패킷의 TTL(Time to Live) 값을 줄입니다.
show icmp	ICMP 컨피그레이션을 표시합니다.
timeout icmp	ICMP의 유휴 시간 제한을 구성합니다.

icmp-object

ICMP 객체 그룹에 ICMP 유형을 추가하려면 icmp-type 컨피그레이션 모드에서 **icmp-object** 명령을 사용합니다. ICMP 유형을 제거하려면 이 명령의 **no** 형식을 사용합니다.

icmp-object *icmp_type*

no icmp-object *icmp_type*

구문 설명

icmp_type	ICMP 유형 이름 또는 숫자(0-255)를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Icmp-type 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ICMP 객체를 정의하려면 **icmp-object** 명령을 **object-group icmp-type** 명령과 함께 사용합니다. 이 명령은 icmp-type 컨피그레이션 모드에서 사용됩니다.

ICMP 유형을 포함하는 서비스 그룹을 만들려면 이 명령 대신 **object-group service** 및 **service-group** 명령을 사용합니다. 서비스 그룹에 ICMP6 및 ICMP 코드는 포함할 수 있지만 ICMP 객체는 포함할 수 없습니다.

ICMP 유형 번호 및 이름에는 다음이 포함됩니다.

번호	ICMP 유형 이름
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**

번호	ICMP 유형 이름
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

예

다음 예는 icmp-type 컨피그레이션 모드에서 **icmp-object** 명령을 사용하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group icmp-type icmp_allowed
ciscoasa(config-icmp-type)# icmp-object echo
ciscoasa(config-icmp-type)# icmp-object time-exceeded
ciscoasa(config-icmp-type)# exit
```

관련 명령

명령	설명
clear configure object-group	컨피그레이션에서 모든 **object-group** 명령을 제거합니다.
object-group	컨피그레이션을 최적화하기 위해 객체 그룹을 정의합니다.
show running-config object-group	현재 객체 그룹을 표시합니다.

id-cert-issuer

이 신뢰 지점(Trustpoint)과 관련된 CA에서 발급한 피어 인증서를 시스템에서 허용하는지를 나타내려면 crypto ca-trustpoint 컨피그레이션 모드에서 **id-cert-issuer** 명령을 사용합니다. 신뢰 지점과 관련된 CA에서 발급한 인증서를 허용하지 않으려면 이 명령의 **no** 형식을 사용합니다. 이는 널리 사용되는 루트 CA를 나타내는 신뢰 지점에 유용합니다.

id-cert-issuer

no id-cert-issuer

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 설정은 활성화입니다(ID 인증서가 허용됨).

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca-trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

널리 사용되는 루트 인증서의 하위 인증서에 의해 발급된 인증서의 허용 범위를 제한하려면 이 명령을 사용합니다. 이 기능을 허용하지 않으면 ASA는 이 발급자가 서명한 모든 IKE 피어 인증서를 거부합니다.

예

다음 예에서는 trustpoint central에 대한 crypto ca trustpoint 컨피그레이션 모드로 들어가서, trustpoint central의 발급자가 서명한 ID 인증서를 관리자가 수락하도록 허용합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# id-cert-issuer
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다.
default enrollment	enrollment 매개변수를 기본값으로 되돌립니다.
enrollment retry count	enrollment 요청을 전송하려고 하는 재시도 횟수를 지정합니다.
enrollment retry period	enrollment 요청을 전송하려고 시도하기 전에 대기하는 시간(분)을 지정합니다.
enrollment terminal	이 신뢰 지점의 cut-and-paste enrollment를 지정합니다.

id-mismatch

과도한 DNS ID 불일치의 기록을 활성화하려면 매개변수 컨피그레이션 모드에서 **id-mismatch** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

id-mismatch [**count** *number* **duration** *seconds*] **action log**

no id-mismatch [**count** *number* **duration** *seconds*] **action log**]

구문 설명

count *number*	시스템 메시지 로그를 전송하기까지의 최대 불일치 인스턴스 수입니다.
duration *seconds*	모니터링 기간(초)입니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다. 명령이 활성화되었을 때 옵션이 지정되지 않은 경우 기본 속도는 3초 동안 30입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

DNS ID 불일치 속도가 높으면 캐시 악성 침입 공격을 나타내는 것일 수 있습니다. 그러한 시도를 모니터링하고 경고하기 위해 이 명령을 사용할 수 있습니다. 불일치 속도가 구성된 값을 초과하면 요약된 시스템 메시지 로그가 출력됩니다. **id-mismatch** 명령은 시스템 관리자에게 정기적인 이벤트 기반 시스템 메시지 로그에 대한 추가 정보를 제공합니다.

예

다음 예는 DNS 검사 정책 맵에서 ID 불일치를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-mismatch action log
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

id-randomization

DNS 쿼리에 대해 DNS 식별자를 임의 지정하려면 매개변수 컨피그레이션 모드에서 **id-randomization** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

id-randomization

no id-randomization

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 비활성화되어 있습니다. DNS 쿼리의 DNS 식별자는 수정되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ID 임의 지정은 캐시 악성 침입 공격을 막는 데 도움이 됩니다.

예

다음 예는 DNS 검사 정책 맵에서 ID 임의 지정을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-randomization
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

id-usage

등록된 인증서 ID의 사용 방법을 지정하려면 crypto ca trustpoint 컨피그레이션 모드에서 **id-usage** 명령을 사용하십시오. 인증서의 사용을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

id-usage {**ssl-ipsec** | **code-signer** | **mdm-proxy**}

no id-usage {**ssl-ipsec** | **code-signer** | **mdm-proxy**}

구문 설명

code-signer	이 인증서에서 나타내는 디바이스 ID는 원격 사용자에게 제공되는 애플릿 검증을 위한 Java code signer로 사용됩니다.
ssl-ipsec	(기본값) 이 인증서에서 나타내는 디바이스 ID는 SSL 또는 IPsec 암호화 연결을 위한 서버 측 ID로서 사용될 수 있습니다.
mdm-proxy	이 인증서에 표시된 디바이스 ID는 MDM 클라이언트 대신 ISE MDM 서버에 대해 ASA MDM 프록시 서비스를 인증하는 데 사용될 수 있습니다.

기본값

id-usage 명령 기본값은 **ssl-ipsec**입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.
9.3(1)	이제 이 명령을 MDM 프록시 서비스에 사용할 수 있습니다.

사용 지침

원격 액세스 VPN에서는 실제로 모든 네트워크 애플리케이션 또는 리소스에 대한 액세스를 허용하기 위해 요구 사항에 따라 SSL이나 IPsec 또는 두 프로토콜을 모두 사용할 수 있습니다. **id-usage** 명령을 사용하면 인증서로 보호되는 각종 리소스에 대한 액세스 유형을 지정할 수 있습니다.

CA ID(그리고 경우에 따라 디바이스 ID)는 CA에서 발급한 인증서를 기반으로 합니다. Crypto ca trustpoint 컨피그레이션 모드 내 모든 명령은 CA 전용 컨피그레이션 매개 변수로서 ASA가 CA 인증서를 얻는 방법, ASA가 CA에서 인증서를 얻는 방법, 그리고 CA에서 발급한 사용자 인증서에 대한 인증 정책을 지정합니다.

신뢰 지점 컨피그레이션에는 **id-usage** 명령의 단일 인스턴스만 가능합니다. **code-signer** 및/또는 **ssl-ipsec** 옵션의 신뢰 지점을 활성화하려면 두 옵션 중 하나 또는 둘 다를 지정할 수 있는 단일 인스턴스를 사용합니다.

예

다음 예에서는 trustpoint central에 대한 crypto ca trustpoint 컨피그레이션 모드로 들어가서 trustpoint central을 code-signer 인증서로 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer
ciscoasa(config-ca-trustpoint)#
```

다음 예에서는 trustpoint general에 대한 crypto ca trustpoint 컨피그레이션 모드로 들어가서, trustpoint general을 SSL 또는 IPsec 연결을 위한 code-signer 인증서 및 서버 측 ID로 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

다음 예에서는 trustpoint checkin1에 대한 crypto ca trustpoint 컨피그레이션 모드로 들어가서, SSL 또는 IPsec 연결의 사용을 제한하기 위해 trustpoint checkin1을 재설정합니다.

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# no id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

다음 예에서는 trustpoint MDMtrustpoint에 대한 crypto ca trustpoint 컨피그레이션 모드로 들어가서, trustpoint MDMtrustpoint를 mdm-proxy 인증서로서 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint MDMtrustpoint
ciscoasa(config-ca-trustpoint)# id-usage mdm-proxy
ciscoasa(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다.
java-trustpoint	지정된 신뢰 지점 위치에서 PKCS12 인증서 및 키 지정 자료를 사용할 수 있도록 WebVPN Java 객체 서명 기능을 구성합니다.
ssl trust-point	인터페이스용 SSL 인증서를 나타내는 인증서를 지정합니다.
trust-point (tunnel-group ipsec-attributes mode)	IKE 피어로 전송할 인증서를 식별하는 이름을 지정합니다.
validation-policy	사용자 연결과 관련된 인증서를 검증하기 위한 조건을 지정합니다.
trustpoint (config-mdm-proxy mode)	ASA의 ISE MDM 인증에 사용되는 신뢰 지점을 지정합니다.

igmp

인터페이스에서 IGMP 프로세싱을 복구하려면 인터페이스 컨피그레이션 모드에서 **igmp** 명령을 사용합니다. 인터페이스에서 IGMP 프로세싱을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

igmp

no igmp

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

활성화됨.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

실행 중인 컨피그레이션에는 이 명령의 **no** 형식만 나타납니다.

예

다음 예는 선택한 인터페이스에서 IGMP 프로세싱을 비활성화합니다.

```
ciscoasa(config-if)# no igmp
```

관련 명령

명령	설명
show igmp groups	ASA에 직접 연결되어 있고 IGMP를 통해 학습된 수신자가 있는 멀티캐스트 그룹을 표시합니다.
show igmp interface	인터페이스에 대한 멀티캐스트 정보를 표시합니다.

igmp access-group

인터페이스에서 서비스하는 서브넷의 호스트가 가입할 수 있는 멀티캐스트 그룹을 제어하려면 인터페이스 컨피그레이션 모드에서 **igmp access-group** 명령을 사용합니다. 인터페이스에서 그룹을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

igmp access-group *acl*

no igmp access-group *acl*

구문 설명

acl	IP 액세스 목록의 이름입니다. 표준 또는 확장 액세스 목록을 지정할 수 있습니다. 그러나 확장 액세스 목록을 지정하는 경우 수신 주소만 확인됩니다. 소스에 대해 **any**를 지정해야 합니다.

기본값

인터페이스에서 모든 그룹의 가입이 허용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 인터페이스 컨피그레이션 모드로 이전되었습니다. 이전 버전에서는 멀티캐스트 인터페이스 컨피그레이션 모드로 들어가야 했지만, 이제 이 모드는 더 이상 사용할 수 없습니다.

예

다음 예는 액세스 목록 1에서 그룹에 가입하도록 허용된 호스트를 제한합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp access-group 1
```

관련 명령

명령	설명
show igmp interface	인터페이스에 대한 멀티캐스트 정보를 표시합니다.

igmp forward interface

모든 IGMP 호스트 보고서의 전달을 활성화하고 수신 메시지를 지정된 인터페이스에 남겨두려면 인터페이스 컨피그레이션 모드에서 **igmp forward interface** 명령을 사용합니다. 전달을 제거하려면 이 명령의 **no** 형식을 사용합니다.

igmp forward interface *if-name*

no igmp forward interface *if-name*

구문 설명

if-name	인터페이스의 논리적 이름입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 인터페이스 컨피그레이션 모드로 이전되었습니다. 이전 버전에서는 멀티캐스트 인터페이스 컨피그레이션 모드로 들어가야 했지만, 이제 이 모드는 더 이상 사용할 수 없습니다.

사용 지침

이 명령은 입력 인터페이스에서 입력합니다. 이 명령은 스텁 멀티캐스트 라우팅에 사용되며 PIM과 동시에 구성할 수 없습니다.

예

다음 예는 IGMP 호스트 보고서를 현재 인터페이스에서 지정된 인터페이스로 전달합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp forward interface outside
```

관련 명령

명령	설명
show igmp interface	인터페이스에 대한 멀티캐스트 정보를 표시합니다.

igmp join-group

인터페이스를 지정된 그룹의 논리적으로 연결된 멤버로 구성하려면 인터페이스 컨피그레이션 모드에서 **igmp join-group** 명령을 사용합니다. 그룹에서 멤버십을 취소하려면 **no** 형식을 사용합니다.

igmp join-group *group-address*

no igmp join-group *group-address*

구문 설명

group-address	멀티캐스트 그룹의 IP 주소입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 인터페이스 컨피그레이션 모드로 이전되었습니다. 이전 버전에서는 멀티캐스트 인터페이스 컨피그레이션 모드로 들어가야 했지만, 이제 이 모드는 더 이상 사용할 수 없습니다.

사용 지침

이 명령은 ASA 인터페이스를 멀티캐스트 그룹의 멤버로 구성합니다. **igmp join-group** 명령은 지정된 멀티캐스트 그룹으로 이동할 멀티캐스트 패킷을 ASA에서 수락 및 전달하도록 합니다.

멀티캐스트 그룹의 멤버가 되지 않고도 ASA에서 멀티캐스트 트래픽을 전달하도록 구성하려면 **igmp static-group** 명령을 사용합니다.

예

다음 예는 선택한 인터페이스가 IGMP 그룹 255.2.2.2에 가입하도록 구성합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp join-group 225.2.2.2
```

관련 명령

명령	설명
igmp static-group	인터페이스가 지정된 멀티캐스트 그룹의 고정으로 연결된 멤버가 되도록 구성합니다.

igmp limit

인터페이스 단위로 IGMP 상태의 수를 제한하려면 인터페이스 컨피그레이션 모드에서 **igmp limit** 명령을 사용합니다. 기본 제한을 복원하려면 이 명령의 **no** 형식을 사용합니다.

igmp limit *number*

no igmp limit [*number*]

구문 설명

number	인터페이스에서 허용된 IGMP 상태의 수입니다. 유효한 값의 범위는 0~500입니다. 기본값은 500입니다. 이 값을 0으로 설정하면 학습된 그룹이 추가되지 않지만 수동으로 정의한 그룹(**igmp join-group** 및 **igmp static-group** 명령 사용)은 여전히 허용됩니다.

기본값

기본값은 500입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다. **igmp max-groups** 명령을 대신합니다.

예

다음 예는 인터페이스에서 허용된 IGMP 상태의 수를 250으로 제한합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp limit 250
```

관련 명령

명령	설명
igmp	인터페이스에서 IGMP 프로세싱을 복구합니다.
igmp join-group	인터페이스가 지정된 그룹의 로컬로 연결된 멤버가 되도록 구성합니다.
igmp static-group	인터페이스가 지정된 멀티캐스트 그룹의 고정으로 연결된 멤버가 되도록 구성합니다.

igmp query-interval

인터페이스에서 IGMP 호스트 쿼리 메시지를 전송하는 빈도를 구성하려면 인터페이스 컨피그레이션 모드에서 **igmp query-interval** 명령을 사용합니다. 기본 빈도를 복원하려면 이 명령의 **no** 형식을 사용합니다.

igmp query-interval *seconds*

no igmp query-interval *seconds*

구문 설명

seconds	IGMP 호스트 쿼리 메시지를 전송하는 빈도(초)입니다. 유효한 값의 범위는 1~3600입니다. 기본값은 125초입니다.

기본값

기본 쿼리 간격은 125초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 인터페이스 컨피그레이션 모드로 이전되었습니다. 이전 버전에서는 멀티캐스트 인터페이스 컨피그레이션 모드로 들어가야 했지만, 이제 이 모드는 더 이상 사용할 수 없습니다.

사용 지침

멀티캐스트 라우터는 인터페이스에 연결된 네트워크에 멤버가 있는 멀티캐스트 그룹이 어떤 것인지 검색하기 위해 호스트 쿼리 메시지를 전송합니다. 호스트는 특정 그룹에 대한 멀티캐스트 패킷을 받고 싶다는 의미의 IGMP 보고 메시지로 응답합니다. 호스트 쿼리 메시지는 주소가 224.0.0.1이고 TTL 값이 1인 모든 호스트 멀티캐스트 그룹으로 전달됩니다.

LAN용으로 지정된 라우터가 IGMP 호스트 쿼리 메시지를 전송하는 유일한 라우터입니다.

- IGMP 버전 1의 경우 지정된 라우터는 LAN에서 실행되는 멀티캐스트 라우팅 프로토콜에 따라 선정됩니다.
- IGMP 버전 2의 경우 지정된 라우터는 서브넷에서 가장 낮은 IP 주소의 멀티캐스트 라우터입니다.

시간 제한 기간(**igmp query-timeout** 명령으로 제어) 동안 라우터에서 쿼리를 수신하지 못하는 경우 해당 라우터는 쿼리 발생기가 됩니다.

주의 이 값을 변경하면 멀티캐스트 전달에 심각한 영향이 미칠 수 있습니다.

예

다음 예는 IGMP 쿼리 간격을 120초로 변경합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-interval 120
```

관련 명령

명령	설명
igmp query-max-response-time	IGMP 쿼리에서 광고되는 최대 응답 시간을 구성합니다.
igmp query-timeout	이전 쿼리 발생기가 쿼리를 중단한 이후 라우터가 인터페이스에 대해 쿼리 발생기 역할을 맡게 되기까지의 시간 제한 기간을 구성합니다.

igmp query-max-response-time

IGMP 쿼리에서 광고되는 최대 응답 시간을 지정하려면 인터페이스 컨피그레이션 모드에서 **igmp query-max-response-time** 명령을 사용합니다. 기본 응답 시간 값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

igmp query-max-response-time *seconds*

no igmp query-max-response-time *seconds*

구문 설명

seconds	IGMP 쿼리에서 광고되는 최대 응답 시간(초)입니다. 유효한 값은 1~25입니다. 기본값은 10초입니다.

기본값

10초

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 인터페이스 컨피그레이션 모드로 이전되었습니다. 이전 버전에서는 멀티캐스트 인터페이스 컨피그레이션 모드로 들어가야 했지만, 이제 이 모드는 더 이상 사용할 수 없습니다.

사용 지침

IGMP 버전 2 또는 3이 실행 중인 경우에만 이 명령이 유효합니다.

이 명령은 라우터가 그룹을 삭제하기까지 responder가 IGMP 쿼리 메시지에 응답할 수 있는 기간을 제어합니다.

예

다음 명령은 최대 쿼리 응답 시간을 8초로 변경합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-max-response-time 8
```

관련 명령

명령	설명
igmp query-interval	인터페이스에서 IGMP 호스트 쿼리 메시지를 전송하는 빈도를 구성합니다.
igmp query-timeout	이전 쿼리 발생기가 쿼리를 중단한 이후 라우터가 인터페이스에 대해 쿼리 발생기 역할을 맡게 되기까지의 시간 제한 기간을 구성합니다.

igmp query-timeout

이전 쿼리 발생기가 쿼리를 중단한 이후 인터페이스가 쿼리 발생기 역할을 맡게 되기까지의 시간 제한 기간을 구성하려면 인터페이스 컨피그레이션 모드에서 **igmp query-timeout** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

igmp query-timeout *seconds*

no igmp query-timeout *seconds*

구문 설명

seconds	이전 쿼리 발생기가 쿼리를 중단한 이후 라우터가 쿼리 발생기 역할을 맡게 되기까지 라우터의 대기 시간(초)입니다. 유효한 값은 60~300초입니다. 기본값은 255초입니다.

기본값

기본 쿼리 간격은 255초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IGMP 버전 2 또는 3에서 실행할 수 있습니다.

예

다음 예는 라우터가 마지막 쿼리를 받은 이후 인터페이스에 대한 쿼리 발생기 역할을 맡게 되기까지의 대기 시간을 200초로 구성합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-timeout 200
```

관련 명령

명령	설명
igmp query-interval	인터페이스에서 IGMP 호스트 쿼리 메시지를 전송하는 빈도를 구성합니다.
igmp query-max-response-time	IGMP 쿼리에서 광고되는 최대 응답 시간을 구성합니다.

igmp static-group

인터페이스를 지정된 멀티캐스트 그룹의 고정으로 연결된 멤버로 구성하려면 인터페이스 컨피그레이션 모드에서 **igmp static-group** 명령을 사용합니다. static group 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

igmp static-group *group*

no igmp static-group *group*

구문 설명

group	IP 멀티캐스트 그룹 주소입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

igmp static-group 명령으로 구성할 경우 ASA 인터페이스는 지정된 그룹 자체로 이동할 멀티캐스트 패킷을 수락하지 않고 전달만 합니다. 지정된 멀티캐스트 그룹에 대해 ASA에서 멀티캐스트 패킷을 수락 및 전달하도록 구성하려면 **igmp join-group** 명령을 사용합니다. **igmp join-group** 명령이 **igmp static-group** 명령과 동일한 주소 그룹에 대해 구성되는 경우 **igmp join-group** 명령이 우선 적용되며, 그룹은 로컬로 연결된 그룹처럼 작동합니다.

예

다음 예는 선택한 인터페이스를 멀티캐스트 그룹 239.100.100.101에 추가합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp static-group 239.100.100.101
```

관련 명령

명령	설명
igmp join-group	인터페이스가 지정된 그룹의 로컬로 연결된 멤버가 되도록 구성합니다.

igmp version

인터페이스에서 사용할 IGMP의 버전을 구성하려면 인터페이스 컨피그레이션 모드에서 **igmp version** 명령을 사용합니다. 버전을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

igmp version {**1** | **2**}

no igmp version [**1** | **2**]

구문 설명

1	IGMP 버전 1
2	IGMP 버전 2

기본값

IGMP 버전 2

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 인터페이스 컨피그레이션 모드로 이전되었습니다. 이전 버전에서는 멀티캐스트 인터페이스 컨피그레이션 모드로 들어가야 했지만, 이제 이 모드는 더 이상 사용할 수 없습니다.

사용 지침

서브넷의 모든 라우터는 동일한 IGMP 버전을 지원해야 합니다. 호스트의 IGMP 버전은 무엇이든 상관없으며(1 또는 2), ASA는 상황을 정확하게 감지하여 적절하게 쿼리합니다.

igmp query-max-response-time 및 **igmp query-timeout** 명령을 비롯한 일부 명령을 사용하려면 IGMP 버전 2가 필요합니다.

예

다음 예는 선택한 인터페이스에서 IGMP 버전 1을 사용하도록 구성합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp version 1
```

관련 명령

명령	설명
igmp query-max-response-time	IGMP 쿼리에서 광고되는 최대 응답 시간을 구성합니다.
igmp query-timeout	이전 쿼리 발생기가 쿼리를 중단한 이후 라우터가 인터페이스에 대해 쿼리 발생기 역할을 맡게 되기까지의 시간 제한 기간을 구성합니다.

ignore-ipsec-keyusage

IPsec 클라이언트 인증서에 대한 키 사용 점검을 억제하려면 ca-trustpoint 컨피그레이션 모드에서 **ignore-ipsec-keyusage** 명령을 사용합니다. 키 사용 점검을 다시 시작하려면 이 명령의 **no** 형식을 사용합니다.

ignore-ipsec-keyusage

no ignore-ipsec-keyusage

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-trustpoint 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령은 안전 조치를 위해 추가되었지만 그와 동시에 사용이 중단되었습니다. 향후 릴리스에서는 키 사용 점검 억제 기능이 제공되지 않을 수 있습니다.

사용 지침

이 명령을 사용하는 경우 IPsec 원격 클라이언트 인증서에서 Key Usage 및 확장 Key Usage 값이 검증되지 않습니다. 이 명령은 키 사용 점검을 무시하므로 호환되지 않는 배포에 유용합니다.

예

다음 예는 키 사용 점검의 결과를 무시하는 방법을 보여줍니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ipsec-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다.

ignore lsa mospf

라우터가 LSA Type 6 MOSPF 패킷을 수신할 때 syslog 메시지 전송을 억제하려면 라우터 컨피그레이션 모드에서 **ignore lsa mospf** 명령을 사용합니다. Syslog 메시지의 전송을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ignore lsa mospf

no ignore lsa mospf

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Type 6 MOSPF 패킷은 지원되지 않습니다.

예

다음 예에서는 LSA Type 6 MOSPF 패킷이 무시됩니다.

```
ciscoasa(config-router)# ignore lsa mospf
```

관련 명령

명령	설명
show running-config router ospf	OSPF 라우터 컨피그레이션을 표시합니다.

ignore-ssl-keyusage

SSL 클라이언트 인증서에 대한 키 사용 점검을 억제하려면 ca-trustpoint 컨피그레이션 모드에서 **ignore-ssl-keyusage** 명령을 사용합니다. 키 사용 점검을 다시 시작하려면 이 명령의 **no** 형식을 사용합니다.

ignore-ssl-keyusage

no ignore-ssl-keyusage

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-trustpoint 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령은 안전 조치를 위해 추가되었지만 그와 동시에 사용이 중단되었습니다. 향후 릴리스에서는 키 사용 점검 억제 기능이 제공되지 않을 수 있습니다.

사용 지침

이 명령을 사용하는 경우 IPsec 원격 클라이언트 인증서에서 Key Usage 및 확장 Key Usage 값이 검증되지 않습니다. 이 명령은 키 사용 점검을 무시하므로 호환되지 않는 배포에 유용합니다.

예

다음 예는 키 사용 점검의 결과를 무시하는 방법을 보여줍니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ssl-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다.

ike-retry-count

IKE를 사용하는 Cisco AnyConnect VPN Client가 연결을 시도하기 위해 SSL로 돌아가기까지 수행할 수 있는 최대 연결 재시도 횟수를 구성하려면 group-policy webvpn 컨피그레이션 모드 또는 username webvpn 컨피그레이션 모드에서 **ike-retry-count** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 최대 재시도 횟수를 재설정하려면 이 명령의 **no** 형식을 사용합니다.

ike-retry-count {**none** | *value*}

no ike-retry-count [**none** | *value*]

구문 설명

none	재시도가 허용되지 않음을 지정합니다.
value	초기 연결 실패 이후 Cisco AnyConnect VPN Client가 수행할 수 있는 최대 연결 재시도 횟수(1-10)를 지정합니다.

기본값

허용되는 기본 재시도 횟수는 3입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Group-policy webvpn 컨피그레이션	• 예	—	• 예	—	—
Username webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

Cisco AnyConnect VPN Client가 IKE를 사용하여 연결을 시도할 수 있는 횟수를 제어하려면 **ike-retry-count** 명령을 사용합니다. 이 명령으로 지정한 재시도 횟수 이후에도 클라이언트가 IKE를 사용하여 연결하지 못하면 연결을 시도하기 위해 SSL로 돌아가게 됩니다. 이 값은 Cisco AnyConnect VPN Client에 있는 다른 값을 재지정합니다.

참고 IPsec에서 SSL로 돌아가도록 지원하려면 **svc** 및 **ipsec** 인수를 구성하여 **vpn-tunnel-protocol** 명령을 사용해야 합니다.

예

다음 예는 FirstGroup이라는 그룹 정책에 대해 IKE 재시도 횟수를 7로 설정합니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# ike-retry-count 7
ciscoasa(config-group-webvpn)#
```

다음 예는 Finance라는 사용자 이름에 대해 IKE 재시도 횟수를 9로 설정합니다.

```
ciscoasa(config)# username Finance attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# ike-retry-count 9
ciscoasa(config-group-webvpn)#
```

관련 명령

명령	설명
group-policy	그룹 정책을 만들거나 편집합니다.
ike-retry-timeout	IKE 재시도 횟수 사이의 간격(초)을 지정합니다.
username	ASA 데이터베이스에 사용자를 추가합니다.
vpn-tunnel-protocol	VPN 터널 유형(IPsec, L2TP over IPsec 또는 WebVPN)을 구성합니다.
webvpn	group-policy webvpn 컨피그레이션 모드 또는 username webvpn 컨피그레이션 모드로 들어갑니다.

ikev1 pre-shared-key

사전 공유 키를 기반으로 IKEv1 연결을 지원하도록 사전 공유 키를 지정하려면 tunnel-group ipsec-attributes 컨피그레이션 모드에서 **pre-shared-key** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

pre-shared-key *key*

no pre-shared-key

구문 설명

key	1~128자 사이의 영숫자 키를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group ipsec-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.4(1)	명령 이름이 **pre-shared-key**에서 **ikev1 pre-shared-key**로 수정되었습니다.

사용 지침

모든 IPsec tunnel-group 유형에 이 특성을 적용할 수 있습니다.

예

config-ipsec 컨피그레이션 모드에서 다음 명령을 입력하면 209.165.200.225라는 IPSec LAN-to-LAN 터널 그룹에 대해 IKE 연결을 지원하도록 사전 공유 키 XYZX가 지정됩니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# pre-shared-key xyzx
ciscoasa(config-tunnel-ipsec)#
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 컨피그레이션을 보여줍니다.
tunnel-group ipsec-attributes	이 그룹에 대한 터널 그룹 IPsec 특성을 구성합니다.

ikev1 trust-point

IKEv1 피어로 전송할 인증서를 식별하는 신뢰 지점의 이름을 지정하려면 tunnel-group ipsec-attributes 모드에서 **trust-point** 명령을 사용합니다. Trustpoint 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

trust-point *trust-point-name*

no trust-point *trust-point-name*

구문 설명

trust-point-name	사용할 신뢰 지점의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group ipsec attributes	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.4(1)	명령 이름이 **trust-point**에서 **ikev1 trust-point**로 변경되었습니다.

사용 지침

모든 IPsec tunnel-group 유형에 이 특성을 적용할 수 있습니다.

예

tunnel-ipsec 컨피그레이션 모드에서 다음 예를 입력하면 209.165.200.225라는 IPsec LAN-to-LAN 터널 그룹에 대해 IKEv1 피어로 전송할 인증서를 식별하기 위한 신뢰 지점이 구성됩니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 trust-point mytrustpoint
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 컨피그레이션을 보여줍니다.
tunnel-group ipsec-attributes	이 그룹에 대한 터널 그룹 IPsec 특성을 구성합니다.

ikev1 user-authentication

IKE 중에 하이브리드 인증을 구성하려면 tunnel-group ipsec-attributes 컨피그레이션 모드에서 **ikev1 user-authentication** 명령을 사용합니다. 하이브리드 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ikev1 user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

no ikev1 user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

구문 설명

hybrid	IKE 중에 하이브리드 XAUTH 인증을 지정합니다.
interface	(선택 사항) 사용자 인증 방법을 구성할 인터페이스를 지정합니다.
none	IKE 중에 사용자 인증을 비활성화합니다.
xauth	확장 사용자 인증이라고도 하는 XAUTH를 지정합니다.

기본값

기본 인증 방법은 XAUTH 또는 확장 사용자 인증입니다. 기본값은 모든 인터페이스입니다.

참고 기존의 L2TP over IPsec 세션을 유지하려면 XAUTH 기본값을 그대로 사용해야 합니다. tunnel-group이 다른 값(예: isakmp ikev1-user-authentication none)으로 설정되면 L2TP over IPsec 세션을 설정할 수 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group ipsec-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.4(1)	명령 이름이 **isakmp ikev1-user-authentication**에서 **ikev1 user-authentication**으로 변경되었습니다.

사용 지침

ASA 인증에는 디지털 인증서를 사용하고 원격 VPN 사용자 인증에는 다른 기존 방법(예: RADIUS, TACACS+ 또는 SecurID)을 사용해야 하는 경우 이 명령을 사용합니다. 이 명령은 IKE의 1단계를 다음의 두 단계로 나눕니다. 둘을 합쳐 하이브리드 인증이라고 합니다.

1. ASA에서 표준 공개 키 방식으로 원격 VPN 사용자를 인증합니다. 그러면 단방향으로 인증되는 IKE 보안 연결이 설정됩니다.
2. 그런 다음 XAUTH exchange에서 원격 VPN 사용자를 인증합니다. 이 확장 인증은 지원되는 기존 인증 방법 중 하나를 사용할 수 있습니다.

참고 인증 유형을 하이브리드로 설정하기 전에 인증 서버를 구성하고, 사전 공유 키를 만들고, 신뢰 지점을 구성해야 합니다.

Exchange 유형이 주 모드인 경우에는 IPsec 하이브리드 RSA 인증 유형이 거부됩니다.

선택 사항인 *interface* 인수를 생략하면 명령이 모든 인터페이스에 적용되며, per-interface 명령을 지정하지 않은 경우 백업으로 사용됩니다. 터널 그룹에 대해 두 개의 **ikev1 user-authentication** 명령을 지정하면서 한 명령에서는 *interface* 인수를 사용하고 다른 명령에서는 사용하지 않는 경우, interface 인수를 지정한 명령이 해당 특정 인터페이스에 우선 적용됩니다.

예

다음 명령 예는 example-group이라는 터널 그룹에 대해 내부 인터페이스에서 하이브리드 XAUTH를 활성화합니다.

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 user-authentication (inside) hybrid
ciscoasa(config-tunnel-ipsec)#
```

관련 명령

명령	설명
aaa-server	AAA 서버를 정의합니다.
pre-shared-key	IKE 연결을 지원하기 위한 사전 공유 키를 만듭니다.
tunnel-group	IPsec, L2TP/IPsec 및 WebVPN 연결에 대한 연결 전용 레코드의 데이터베이스를 만들고 관리합니다.

ikev2 local-authentication

IKEv2 LAN-to-LAN 연결에 대해 로컬 인증을 지정하려면 tunnel-group ipsec-attributes 컨피그레이션 모드에서 **ikev2 local-authentication** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ikev2 local-authentication {**pre-shared-key** *key_value* | **certificate** *trustpoint*}

no ikev2 local-authentication {**pre-shared-key** *key_value* | **certificate** *trustpoint*}

구문 설명

certificate	인증서 인증을 지정합니다.
key_value	키 값은 1~128자입니다.
pre-shared-key	원격 피어를 인증하는 데 사용되는 로컬 사전 공유 키를 지정합니다.
trustpoint	원격 피어로 전송할 인증서를 식별하는 신뢰 지점을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group ipsec-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IPsec IKEv2 LAN-to-LAN 터널 그룹에만 적용됩니다.

예

다음 명령은 209.165.200.225라는 IPsec LAN-to-LAN 터널 그룹에 대해 IKE 연결을 지원하도록 사전 공유 키 XYZX를 지정합니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key XYZX
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 컨피그레이션을 보여줍니다.
tunnel-group ipsec-attributes	이 그룹에 대한 터널 그룹 IPsec 특성을 구성합니다.

ikev2 remote-authentication

IPsec IKEv2 LAN-to-LAN 연결에 대해 원격 인증을 지정하려면 tunnel-group ipsec-attributes 컨피그레이션 모드에서 **ikev2 remote-authentication** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ikev2 remote-authentication {**pre-shared-key** *key_value* | **certificate** | }

no ikev2 remote-authentication {**pre-shared-key** *key_value* | **certificate** | }

구문 설명

certificate	인증서 인증을 지정합니다.
key_value	키 값은 1~128자입니다.
pre-shared-key	원격 피어를 인증하는 데 사용되는 로컬 사전 공유 키를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group ipsec-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IPsec IKEv2 LAN-to-LAN 터널 그룹에만 적용됩니다.

예

다음 명령은 209.165.200.225라는 IPsec LAN-to-LAN 터널 그룹에 대해 IKEv2 연결을 지원하도록 사전 공유 키 XYZX를 지정합니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key xyzx
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 컨피그레이션을 보여줍니다.
tunnel-group ipsec-attributes	이 그룹에 대한 터널 그룹 IPsec 특성을 구성합니다.

im

SIP를 통해 인스턴트 메시징을 활성화하려면 정책 맵 컨피그레이션 모드에서 액세스할 수 있는 매개변수 컨피그레이션 모드에서 **im** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

im

no im

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 SIP 검사 정책 맵에서 SIP를 통해 인스턴트 메시징을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# im
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

imap4s

IMAP4S 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **imap4s** 명령을 사용합니다. IMAP4S 명령 모드에서 입력한 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

imap4s

no imap4s

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

IMAP4는 인터넷 서버에서 사용자 대신 이메일을 받아서 보관하는 데 사용하는 클라이언트/서버 프로토콜입니다. 사용자(또는 이메일 고객)는 메일의 제목과 전송자만을 본 후 다운로드 여부를 결정할 수 있습니다. 또한 서버에 여러 폴더를 만들고 관리하거나, 메시지를 삭제하거나, 내용의 일부 또는 전체를 검색할 수도 있습니다. 사용자가 메일로 작업하는 동안 IMAP는 지속적으로 서버에 액세스할 수 있어야 합니다. IMAP4S를 사용하면 SSL 연결을 통해 이메일을 수신할 수 있습니다.

예

다음 예는 IMAP4S 컨피그레이션 모드로 들어가는 방법을 보여줍니다.

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)#
```

관련 명령

명령	설명
clear configure imap4s	IMAP4S 컨피그레이션을 제거합니다.
show running-config imap4s	IMAP4S에 대해 실행 중인 컨피그레이션을 표시합니다.

import webvpn customization

사용자 지정 객체를 ASA의 플래시 디바이스에 로드하려면 특별 권한 EXEC 모드에서 **import webvpn customization** 명령을 입력합니다.

import webvpn customization *name URL*

구문 설명

name	사용자 지정 객체를 식별하는 이름입니다. 최대 길이는 64자입니다.
URL	XML 사용자 지정 객체의 소스에 대한 원격 경로입니다. 최대 길이는 255자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	—	• 예		—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

import customization 명령을 입력하기 전에 ASA 인터페이스에서 WebVPN이 활성화되었는지 확인하십시오. 확인하려면 **show running-config** 명령을 입력합니다.

사용자 지정 객체를 가져오면 ASA에서는 다음을 수행합니다.

- URL의 사용자 지정 객체를 ASA 파일 시스템 disk0:/csco_config/customization에 MD5*name*으로 복사합니다.
- 파일에 대해 기본 XML 구문 점검을 수행합니다. 유효하지 않은 경우 ASA는 파일을 삭제합니다.
- index.ini의 파일에 MD5*name* 레코드가 포함되어 있는지 확인합니다. 포함되어 있지 않으면 ASA는 MD5*name*을 파일에 추가합니다.
- MD5*name* 파일을 RAMFS /csco_config/customization/에 ramfs *name*으로 복사합니다.

예

다음 예는 URL 209.165.201.22/customization에서 사용자 지정 객체 *General.xml*을 ASA로 가져와서 이름을 *custom1*로 지정합니다.

```
ciscoasa# import webvpn customization custom1 tftp://209.165.201.22/customization
/General.xml
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

관련 명령

명령	설명
revert webvpn customization	지정된 사용자 지정 객체를 ASA의 플래시 디바이스에서 제거합니다.
show import webvpn customization	ASA의 플래시 디바이스에 있는 사용자 지정 객체를 나열합니다.

import webvpn plug-in protocol

ASA의 플래시 디바이스에 플러그인을 설치하려면 특별 권한 EXEC 모드에서 **import webvpn plug-in protocol** 명령을 입력합니다.

import webvpn plug-in protocol *protocol URL*

구문 설명

protocol	• **rdp -**Remote Desktop Protocol 플러그인은 원격 사용자가 Microsoft Terminal Services를 실행하는 컴퓨터에 연결하도록 허용합니다. Cisco에서는 변경 없이 이 플러그인을 재배포합니다. 원본이 있는 웹사이트는 http://properjavardp.sourceforge.net/입니다. • **ssh,telnet -** Secure Shell 플러그인은 원격 사용자가 원격 컴퓨터에 대해 안전한 채널을 설정하도록 허용하거나, 원격 사용자가 텔넷을 사용하여 원격 컴퓨터에 연결하도록 허용합니다. Cisco에서는 변경 없이 이 플러그인을 재배포합니다. 원본이 있는 웹사이트는 http://javassh.org/입니다. **주의** **import webvpn plug-in protocol ssh,telnet** *URL* 명령은 SSH 및 Telnet 플러그인을 *모두* 설치합니다 . SSH 와 Telnet 에 대해 각각 이 명령을 입력하지 *마십시오* . **ssh,telnet** 문자열을 입력할 때 공백을 삽입하지 *마십시오* . 이러한 명령에서 벗어나는 **import webvpn plug-in protocol** 명령을 제거하려면 **revert webvpn plug-in protocol** 명령을 사용합니다 . • **vnc -** Virtual Network Computing 플러그인은 원격 사용자가 모니터, 키보드 및 마우스를 사용하여 원격 데스크톱 공유가 켜진 컴퓨터를 보고 제어할 수 있도록 허용합니다. Cisco에서는 변경 없이 이 플러그인을 재배포합니다. 원본이 있는 웹사이트는 http://www.tightvnc.com/입니다.
URL	플러그인의 소스에 대한 원격 경로입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예		—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

플러그인을 설치하기 전에 다음을 수행합니다.

- Clientless SSL VPN("webvpn")이 ASA의 인터페이스에서 활성화되었는지 확인합니다. 확인하려면 **show running-config** 명령을 입력합니다.
- 로컬 TFTP 서버(예: 호스트 이름 "local_tftp_server")에 "plugins"라는 임시 디렉토리를 만들고 Cisco 웹사이트에서 "plugins" 디렉토리로 플러그인을 다운로드합니다. TFTP 서버의 호스트 이름 또는 주소와 **import webvpn plug-in protocol** 명령의 URL 필드에 필요한 플러그인의 경로를 입력합니다.

플러그인을 가져오면 ASA에서는 다음을 수행합니다.

- *URL*에 지정된 jar 파일의 압축을 풉니다.
- ASA 파일 시스템의 csco-config/97/plugin 디렉토리에 파일을 씁니다.
- ASDM의 URL 특성 옆에 있는 드롭다운 메뉴를 채웁니다.
- 모든 향후 Clientless SSL VPN 세션에 대해 플러그인을 활성화하고, 포털 페이지의 Address 필드 옆에 있는 드롭다운 메뉴에 주 메뉴 옵션을 추가합니다. 다음 표는 포털 페이지의 주 메뉴 및 주소 필드에 대한 변경 사항을 보여줍니다.

플러그인	포털 페이지에 추가되는 주 메뉴 옵션	포털 페이지에 추가되는 Address 필드 옵션
rdp	터미널 서버	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

ASA는 컨피그레이션에 **import webvpn plug-in protocol** 명령을 유지하지 않습니다. 대신 csco-config/97/plugin 디렉토리의 내용을 자동으로 로드합니다. 보조 ASA는 기본 ASA에서 플러그인을 가져옵니다.

Clientless SSL VPN 세션에 있는 사용자가 포털 페이지에서 관련 메뉴 옵션을 클릭하면 포털 페이지에는 인터페이스에 대한 창과 도움말 창이 표시됩니다. 사용자는 드롭다운 메뉴에 표시된 프로토콜을 선택하고 Address 필드에 URL을 입력하여 연결을 설정할 수 있습니다.

참고 이전의 SSH V1 및 Telnet 외에도 SSH V2에 대한 지원이 추가되었습니다. 플러그인 프로토콜은 여전히 동일하고(ssh 및 telnet), URL 형식은 다음과 같습니다.
ssh://<target> - SSH V2 사용
ssh://<target>/?version=1 - SSH V1 사용
telnet://<target> - telnet 사용

개별 **import webvpn plug-in protocol** 명령을 제거하고 프로토콜에 대한 지원을 비활성화하려면 **revert webvpn plug-in protocol** 명령을 사용합니다.

예

다음 명령은 RDP에 대한 Clientless SSL VPN 지원을 추가합니다.

```
ciscoasa# import webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
Accessing
tftp://209.165.201.22/plugins/rdp-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/rdp...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

다음 명령은 SSH 및 Telnet에 대한 Clientless SSL VPN 지원을 추가합니다.

```
ciscoasa# import webvpn plug-in protocol ssh,telnet
tftp://209.165.201.22/plugins/ssh-plugin.jar

Accessing
tftp://209.165.201.22/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

다음 명령은 VNC에 대한 Clientless SSL VPN 지원을 추가합니다.

```
ciscoasa# import webvpn plug-in protocol vnc tftp://209.165.201.22/plugins/vnc-plugin.jar

Accessing tftp://209.165.201.22/plugins/vnc-plugin.jar...!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/vnc...
!!!!!!!!!!!!!!!!
58147 bytes copied in 2.40 secs (29073 bytes/sec)
ciscoasa#
```

관련 명령

명령	설명
revert webvpn plug-in protocol	지정된 플러그인을 ASA의 플래시 디바이스에서 제거합니다.
show import webvpn plug-in	ASA의 플래시 디바이스에 있는 플러그인을 나열합니다.

import webvpn translation-table

SSL VPN 연결을 설정하는 원격 사용자에게 표시되는 용어 번역에 사용되는 번역 테이블을 가져오려면 특별 권한 EXEC 모드에서 **import webvpn translation-table** 명령을 사용합니다.

import webvpn translation-table *translation_domain* **language** *language url*

구문 설명

language	번역 테이블의 언어를 지정합니다. 브라우저 언어 옵션에 표시된 방식으로 *language* 값을 입력합니다.
translation_domain	원격 사용자에게 표시되는 기능 영역 및 관련 메시지를 지정합니다.
url	사용자 지정 객체를 만드는 데 사용되는 XML 파일의 URL을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

ASA는 브라우저 기반 클라이언트리스 SSL VPN 연결을 시작하는 사용자에게 표시되는 화면과 포털은 물론 AnyConnect VPN Client 사용자에게 표시되는 사용자 인터페이스에 대해서도 언어 번역 서비스를 제공합니다.

원격 사용자에게 표시되는 각 기능 영역 및 해당 메시지에는 자체 번역 도메인이 있으며 *translation_domain* 인수로 지정됩니다. 다음 표는 번역 도메인 및 번역되는 기능 영역을 보여줍니다.

번역 도메인	번역되는 기능 영역
AnyConnect	Cisco AnyConnect VPN Client의 사용자 인터페이스에 표시되는 메시지입니다.
banners	VPN 액세스가 거부될 때 원격 사용자 및 메시지에 표시되는 배너입니다.
CSD	CSD(Cisco Secure Desktop)의 메시지입니다.
customization	로그인 및 로그아웃 페이지와 포털 페이지의 메시지, 사용자 지정 가능한 모든 메시지입니다.
plugin-ica	Citrix 플러그인의 메시지입니다.

번역 도메인(계속)	번역되는 기능 영역(계속)
plugin-rdp	Remote Desktop Protocol 플러그인의 메시지입니다.
plugin-telnet,ssh	Telnet 및 SSH 플러그인의 메시지입니다.
plugin-vnc	VNC 플러그인의 메시지입니다.
PortForwarder	포트 전달 사용자에게 표시되는 메시지입니다.
url-list	사용자가 포털 페이지에서 URL 북마크에 대해 지정하는 텍스트입니다.
webvpn	모든 Layer 7, AAA 및 사용자 지정 불가능한 포털 메시지입니다.

번역 템플릿은 번역 테이블과 동일한 형식의 XML 파일이지만 번역은 모두 비어 있습니다. ASA의 소프트웨어 이미지 패키지에는 표준 기능의 일부인 각 도메인에 대한 템플릿이 포함되어 있습니다. 플러그인용 템플릿은 플러그인과 함께 포함되어 있으며 고유한 번역 도메인을 정의합니다. 로그인 및 로그아웃 페이지, 포털 페이지, 클라이언트리스 사용자의 URL 북마크 등을 사용자 지정할 수 있으므로 ASA에서는 **customization** 및 **url-list** 번역 도메인 템플릿을 동적으로 생성하며, 이러한 기능 영역에 대한 변경 사항은 템플릿에 자동으로 반영됩니다.

export webvpn translation-table 명령을 사용하여 번역 도메인용 템플릿을 다운로드하고, 메시지를 변경하고, **import webvpn translation-table** 명령을 사용하여 객체를 만들 수 있습니다. **show import webvpn translation-table** 명령으로 사용 가능한 객체를 볼 수 있습니다.

브라우저 언어 옵션의 표현 방식으로 언어를 지정해야 합니다. 예를 들어, Microsoft Internet Explorer에서는 중국어에 대해 약어 *zh*를 사용합니다. 따라서 ASA로 가져온 번역 테이블에서도 *zh* 이름을 사용해야 합니다.

AnyConnect 번역 도메인은 예외입니다. 이 경우 번역 테이블이 영향을 미치지 않으며, 사용자가 사용자 지정 객체를 만들고 해당 객체에서 사용할 번역 테이블을 식별하고 그룹 정책 또는 사용자에 대해 사용자 지정을 지정할 때까지 메시지가 번역되지 않습니다. AnyConnect 도메인용 번역 테이블 변경 사항은 AnyConnect 클라이언트 사용자에게 즉시 표시됩니다. 자세한 내용은 **import webvpn customization** 명령을 참조하십시오.

예

다음 예는 AnyConnect 클라이언트 사용자 인터페이스에 영향을 미치는 번역 도메인용 translation-table을 가져오고 중국어에 대한 번역 테이블을 지정합니다. **show import webvpn translation-table** 명령은 새 객체를 표시합니다.

```
ciscoasa# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
zh AnyConnect
```

관련 명령

명령	설명
export webvpn translation-table	번역 테이블을 내보냅니다.
import webvpn customization	번역 테이블을 참조하는 사용자 지정 객체를 가져옵니다.
revert	플래시에서 번역 테이블을 제거합니다.
show import webvpn translation-table	사용 가능한 번역 테이블 템플릿 및 번역 테이블을 표시합니다.

import webvpn url-list

URL 리스트를 ASA의 플래시 디바이스에 로드하려면 특별 권한 EXEC 모드에서 **import webvpn url-list** 명령을 입력합니다.

import webvpn url-list *name URL*

구문 설명

name	URL 리스트를 식별하는 이름입니다. 최대 길이는 64자입니다.
URL	URL 리스트의 소스에 대한 원격 경로입니다. 최대 길이는 255자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

import url-list 명령을 입력하기 전에 ASA 인터페이스에서 WebVPN이 활성화되었는지 확인하십시오. 확인하려면 **show running-config** 명령을 입력합니다.

URL 리스트를 가져오면 ASA에서는 다음을 수행합니다.

- URL의 URL 리스트를 ASA 파일 시스템 disk0:/csco_config/url-lists에 *name on flash* = base 64*name*으로 복사합니다.
- 파일에 대해 기본 XML 구문 점검을 수행합니다. 구문이 유효하지 않은 경우 ASA는 파일을 삭제합니다.
- index.ini의 파일에 base 64*name* 레코드가 포함되어 있는지 확인합니다. 포함되어 있지 않으면 ASA는 base 64*name*을 파일에 추가합니다.
- *name* 파일을 ramfs name = *name*으로 RAMFS /csco_config/url-lists/에 복사합니다.

예

다음 예는 URL 리스트 *NewList.xml*을 URL 209.165.201.22/url-lists에서 ASA로 가져오고 이름을 *ABCList*로 지정합니다.

```
ciscoasa# import webvpn url-list ABCList tftp://209.165.201.22/url-lists/NewList.xml
Accessing
tftp://209.165.201.22/url-lists/NewList.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/ABClist...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

관련 명령

명령	설명
revert webvpn url-list	지정된 URL 리스트를 ASA의 플래시 디바이스에서 제거합니다.
show import webvpn url-list	ASA의 플래시 디바이스에 있는 URL 리스트를 나열합니다.

import webvpn webcontent

원격 Clientless SSL VPN 사용자에게 표시되는 플래시 메모리의 콘텐츠를 가져오려면 특별 권한 EXEC 모드에서 **import webvpn webcontent** 명령을 사용합니다.

import webvpn webcontent *destination url source url*

구문 설명

destination url	내보낼 URL입니다. 최대 길이는 255자입니다.
source url	콘텐츠가 상주하는 ASA 플래시 메모리의 URL입니다. 최대 길이는 64자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

webcontent 옵션으로 가져온 콘텐츠는 원격 Clientless 사용자에게 표시됩니다. 여기에는 사용자 화면을 사용자 지정하는 사용자 지정 객체에 사용되는 로고 및 Clientless 포털에서 볼 수 있는 도움말 콘텐츠가 포함됩니다.

/+CSCOE+/ 경로와 함께 URL로 가져온 콘텐츠는 권한이 있는 사용자에게만 표시됩니다.

/+CSCOU+/ 경로와 함께 URL로 가져온 콘텐츠는 권한이 있는 사용자와 권한이 없는 사용자 모두에게 표시됩니다.

예를 들어 /+CSCOU+/logo.gif로 가져온 회사 로고는 포털 사용자 지정 객체에 사용할 수 있으며 로그온 페이지 및 포털 페이지에 표시할 수 있습니다. 그러나 /+CSCOE+/logo.gif로 가져온 동일한 logo.gif 파일은 성공적으로 로그인한 원격 사용자에게만 표시됩니다.

다양한 애플리케이션 화면에 나타나는 도움말 콘텐츠는 특정 URL로 가져와야 합니다. 다음 표는 표준 Clientless 애플리케이션에 표시되는 도움말 콘텐츠의 URL 및 화면 영역을 보여줍니다.

URL	Clientless 화면 영역
/+CSCOE+/help/*language*/app-access-hlp.inc	애플리케이션 액세스
/+CSCOE+/help/*language*/file-access-hlp.inc	네트워크 찾아보기
/+CSCOE+/help/*language*/net_access_hlp.html	AnyConnect 클라이언트
/+CSCOE+/help/*language*/web-access-help.inc	웹 액세스

다음 표는 선택적 플러그인 Clientless 애플리케이션에 표시되는 도움말 콘텐츠의 URL 및 화면 영역을 보여줍니다.

URL	클라이언트리스 화면 영역
/+CSCOE+/help/*language*/ica-hlp.inc	MetaFrame 액세스
/+CSCOE+/help/*language*/rdp-hlp.inc	터미널 서버
/+CSCOE+/help/*language*/ssh,telnet-hlp.inc	Telnet/SSH 서버
/+CSCOE+/help/*language*/vnc-hlp.inc	VNC 연결

URL 경로의 *language* 엔트리는 도움말 콘텐츠에 대해 지정하는 언어 약어입니다. ASA는 사용자가 지정한 언어로 파일을 실제로 번역하는 것이 아니라 언어 약어로 파일에 레이블을 지정합니다.

예

다음 예는 209.165.200.225에 있는 TFTP 서버의 HTML 파일 *application_access_help.html*을 플래시 메모리에 Application Access 도움말 콘텐츠를 저장하는 URL로 가져옵니다. URL에는 영어에 대한 약어 *en*이 포함되어 있습니다.

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

다음 예는 209.165.200.225에 있는 tftp 서버의 HTML 파일 *application_access_help.html*을 플래시 메모리에 Application Access 도움말 콘텐츠를 저장하는 URL로 가져옵니다. URL에는 영어에 대한 약어 *en*이 포함되어 있습니다.

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

관련 명령

명령	설명
export webvpn webcontent	이전에 가져왔으며 클라이언트리스 SSL VPN 사용자에게 표시되는 콘텐츠를 내보냅니다.
revert webvpn webcontent	플래시 메모리에서 콘텐츠를 제거합니다.
show import webvpn webcontent	가져온 콘텐츠에 대한 정보를 표시합니다.

2 장

inspect ctiqbe through inspect xdmcp 명령

inspect ctiqbe

CTIQBE 프로토콜 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect ctiqbe** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 검사를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

inspect ctiqbe

no inspect ctiqbe

기본값

이 명령은 기본적으로 비활성화되어 있습니다 .

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 기존의 **fixup** 명령을 대체했습니다.

사용 지침

inspect ctiqbe 명령은 NAT, PAT 및 양방향 NAT를 지원하는 CTIQBE 프로토콜 검사를 활성화합니다. 이 검사는 Cisco IP SoftPhone 및 기타 Cisco TAPI/JTAPI 애플리케이션이 ASA 전체에서 통화 설정을 위해 Cisco CallManager와 성공적으로 작동하도록 지원합니다.

TAPI(Telephony Application Programming Interface) 및 JTAPI(Java Telephony Application Programming Interface)는 많은 Cisco VoIP 애플리케이션에서 사용됩니다. CTIQBE(Computer Telephony Interface Quick Buffer Encoding)는 TSP(Cisco TAPI Service Provider)에서 Cisco CallManager와 통신하는 데 사용됩니다.

다음은 CTIQBE 애플리케이션 검사 사용 시 해당되는 제한 사항을 요약한 것입니다.

- CTIQBE 통화의 상태 저장 장애 조치는 지원되지 않습니다.
- **debug ctiqbe** 명령을 사용하면 메시지 전송이 지연될 수 있으며, 이는 실시간 환경에 성능 영향을 미칠 수 있습니다. 이 디버깅 또는 기록을 활성화한 경우 Cisco IP SoftPhone에서 ASA를 통해 통화 설정을 완료하지 못할 것 같으면 Cisco IP SoftPhone을 실행하는 시스템의 Cisco TSP 설정에서 시간 제한 값을 늘리십시오.
- CTIQBE 애플리케이션 검사는 여러 TCP 패킷에 조각화된 CTIQBE 메시지를 지원하지 *않습니다.*

다음은 특정 시나리오에서 CTIQBE 애플리케이션 검사를 사용할 경우 특별히 고려해야 할 내용을 요약한 것입니다.

- ASA의 서로 다른 인터페이스에 연결된 서로 다른 Cisco CallManager로 두 개의 Cisco IP SoftPhone을 등록한 경우 두 전화기 간 통화가 실패합니다.
- Cisco CallManager가 Cisco IP SoftPhone보다 보안 수준이 높은 인터페이스에 있을 때 Cisco CallManager IP 주소에 NAT 또는 외부 NAT가 필요한 경우에는 고정인 매핑을 사용해야 합니다. Cisco IP SoftPhone을 사용하려면 PC의 Cisco TSP 컨피그레이션에 Cisco CallManager IP 주소가 명시적으로 지정되어 있어야 하기 때문입니다.
- PAT 또는 외부 PAT 사용 시 Cisco CallManager IP 주소를 변환해야 하는 경우, Cisco IP SoftPhone을 성공적으로 등록하려면 TCP 포트 2748을 PAT(인터페이스) 주소의 동일한 포트에 고정으로 매핑해야 합니다. CTIQBE 수신 대기 포트(TCP 2748)는 고정되어 있으므로 Cisco CallManager, Cisco IP SoftPhone 또는 Cisco TSP에서 사용자가 구성할 수 없습니다.

신호 메시지 검사

신호 메시지 검사에서 **inspect ctiqbe** 명령은 종종 미디어 엔드포인트(예: IP Phone)의 위치를 확인해야 합니다.

이 정보는 액세스 제어 및 미디어 트래픽의 NAT 상태가 수동 구성 없이 방화벽을 투명하게 통과하도록 준비하는 데 사용됩니다.

이러한 위치를 확인하는 과정에서 **inspect ctiqbe** 명령은 터널 기본 게이트웨이 경로를 사용하지 않습니다. 터널 기본 게이트웨이 경로는 **route** *interface* **0 0** *metric* **tunneled** 형식의 경로입니다. 이 경로는 IPsec 터널에서 이그레스(egress)하는 패킷의 기본 경로를 재지정합니다. 따라서 VPN 트래픽에 **inspect ctiqbe** 명령이 필요한 경우 터널 기본 게이트웨이 경로를 구성하지 마십시오. 대신 다른 고정 라우팅 또는 동적 라우팅을 사용하십시오.

예

다음 예는 기본 포트(2748)에서 CTIQBE 트래픽을 확인하기 위해 클래스 맵을 만드는 CTIQBE 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다.

```
ciscoasa(config)# class-map ctiqbe-port
ciscoasa(config-cmap)# match port tcp eq 2748
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ctiqbe_policy
ciscoasa(config-pmap)# class ctiqbe-port
ciscoasa(config-pmap-c)# inspect ctiqbe
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ctiqbe_policy interface outside
```

모든 인터페이스에 대해 CTIQBE 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
show conn	서로 다른 연결 유형의 연결 상태를 표시합니다.
show ctiqbe	ASA 전체에 설정된 CTIQBE 세션 및 CTIQBE 검사 엔진에서 할당한 미디어 연결에 대한 정보를 표시합니다.
timeout	서로 다른 프로토콜 및 세션 유형에 대한 최대 유휴 시간을 설정합니다.

inspect dcerpc

엔드포인트 매퍼로 이동할 DCERPC 트래픽의 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect dcerpc** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

구문 설명

map_name	(선택 사항) DCERPC 검사 맵의 이름

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

inspect dcerpc 명령은 DCERPC 프로토콜에 대한 애플리케이션 검사를 활성화 또는 비활성화합니다.

예

다음 예는 DCERPC 핀홀에 대해 구성된 시간 제한으로 DCERPC 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout pinhole 0:10:00

ciscoasa(config)# class-map dcerpc
ciscoasa(config-cmap)# match port tcp eq 135

ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# class dcerpc
ciscoasa(config-pmap-c)# inspect dcerpc dcerpc_map

ciscoasa(config)# service-policy global-policy global
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.
timeout pinhole	DCERPC 핀홀의 시간 제한을 구성하고 전역 시스템 핀홀 시간 제한을 재지정합니다.

inspect dns

DNS 검사를 활성화하거나(전에 비활성화된 경우) DNS 검사 매개변수를 구성하려면 클래스 컨피그레이션 모드에서 **inspect dns** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. DNS 검사를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

inspect dns [*map_name*] [**dynamic-filter-snoop**]

no inspect dns [*map_name*] [**dynamic-filter-snoop**]

구문 설명

dynamic-filter-snoop	(선택 사항) Botnet Traffic Filter에서만 사용되는 동적 필터 스누핑을 활성화합니다. Botnet Traffic Filtering을 사용하는 경우에만 이 키워드를 포함하십시오. 외부 DNS 요청이 이동하는 인터페이스에서만 DNS 스누핑을 활성화하는 것이 좋습니다. 내부 DNS 서버로 이동하는 트래픽을 포함하여 모든 UDP DNS 트래픽에서 DNS 스누핑을 활성화하면 ASA에 불필요한 부하가 발생합니다.
map_name	(선택 사항) DNS 맵의 이름을 지정합니다.

기본값

이 명령은 기본적으로 사용됩니다. Botnet Traffic Filter 스누핑은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.
7.2(1)	추가 DNS 검사 매개변수의 구성을 허용하도록 이 명령이 수정되었습니다.
8.2(1)	**dynamic-filter-snoop** 키워드가 추가되었습니다.

사용 지침

DNS 검사는 preset_dns_map 검사 클래스 맵을 사용하여 기본적으로 활성화됩니다.

- 최대 DNS 메시지 길이는 512바이트입니다.
- 최대 클라이언트 DNS 메시지 길이는 자동으로 리소스 레코드에 맞게 설정됩니다.
- DNS Guard가 사용되므로 ASA에 의해 DNS 회신이 전달되자마자 ASA에서 DNS 쿼리와 관련된 DNS 세션을 해제합니다. ASA는 또한 DNS 회신의 ID가 DNS 쿼리의 ID와 일치하는지 확인하기 위해 메시지 교환을 모니터링합니다.

- NAT 컨피그레이션으로 기반으로 하는 DNS 레코드의 변환이 활성화됩니다.
- 프로토콜 적용이 활성화되고, 이에 따라 DNS 메시지 형식 확인이 활성화됩니다. 여기에는 도메인 이름 길이 최대 255자, 레이블 길이 63자, 압축 및 반복되는 포인터 확인 등이 포함됩니다.

DNS 재작성에 필요한 DNS 검사

DNS 검사가 활성화되면 DNS 재작성은 모든 인터페이스에서 오는 DNS 메시지의 NAT를 완전히 지원합니다.

내부 네트워크의 클라이언트가 외부 인터페이스에 있는 DNS 서버에서 내부 주소의 DNS 확인을 요청하는 경우 DNS A 레코드가 정확히 변환됩니다. DNS 검사 엔진이 비활성화되어 있으면 A 레코드가 변환되지 않습니다.

DNS 재작성은 두 가지 기능을 수행합니다.

- DNS 클라이언트가 비공개 인터페이스에 있을 때 DNS reply의 공용 주소(라우팅 가능한 주소 또는 "매핑된" 주소)를 사설 주소로 변환
- DNS 클라이언트가 공개 인터페이스에 있을 때 사설 주소를 공용 주소로 변환

DNS 검사가 활성화되어 있는 동안에는 NAT를 위한 DNS 재작성을 구성할 수 있습니다.

예

다음 예는 최대 DNS 메시지 길이를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns dns-inspect
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 1024
```

다음 예는 모든 UDP DNS 트래픽에 대한 클래스 맵을 만들고, 기본 DNS 검사 정책 맵으로 DNS 검사 및 Botnet Traffic Filter 스누핑을 활성화하고, 이를 외부 인터페이스에 적용합니다.

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
ciscoasa(config-cmap)# match port udp eq domain
ciscoasa(config-cmap)# policy-map dynamic-filter_snoop_policy
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
ciscoasa(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
ciscoasa(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
dynamic-filter enable	액세스 목록을 지정하지 않는 경우 트래픽의 클래스 또는 모든 트래픽에 대해 Botnet Traffic Filter를 활성화합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect esmtp

SMTP/ESMTP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect esmtp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect esmtp [*map_name*]

no inspect esmtp [*map_name*]

구문 설명

map_name	(선택 사항) ESMTP 맵의 이름

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

ESMTP 검사는 _default_esmtp_map 검사 정책 맵을 사용하여 기본적으로 활성화됩니다.

- 서버 배너는 마스크 처리됩니다 .
- 암호화된 트래픽은 검사됩니다 .
- 발신자와 수신자 주소의 특수 문자는 검사되지 않고 , 작업이 수행되지 않습니다 .
- 명령줄 길이가 512가 넘는 연결은 삭제 및 기록됩니다.
- 수신자가 100명이 넘는 연결은 삭제 및 기록됩니다.
- 본문 길이가 998바이트가 넘는 메시지는 기록됩니다.
- 헤더 줄 길이가 998이 넘는 연결은 삭제 및 기록됩니다.
- MIME 파일 이름이 255자가 넘는 메시지는 삭제 및 기록됩니다.
- "others"와 일치하는 EHLO 회신 매개변수는 마스크 처리됩니다.

ESMTP 애플리케이션 검사는 ASA를 통과할 수 있는 SMTP 명령의 유형을 제한하고 모니터링 기능을 추가하여 SMTP 기반 공격을 더 잘 방어할 수 있습니다.

ESMTP는 SMTP 프로토콜의 향상된 버전이며 SMTP와 상당 부분이 유사합니다. 이 문서에서는 편의상 SMTP와 ESMTP를 모두 가리키는 데 SMTP라는 용어를 사용합니다. Extended SMTP에 대한 애플리케이션 검사 프로세스는 SMTP 애플리케이션 검사와 유사하며 SMTP 세션에 대한 지원을 포함합니다. Extended SMTP 세션에 사용되는 대부분의 명령은 SMTP 세션에 사용되는 것과 동일하지만, ESMTP 세션이 훨씬 빠르며 안정성 및 보안과 관련된 더 많은 옵션(예: 배달 상태 알림)을 제공합니다.

Extended SMTP 애플리케이션 검사는 Extended SMTP 명령(AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS 및 VRFY)에 대한 지원을 추가로 제공합니다. 7개의 RFC 821 명령(DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET)을 포함하여 ASA는 총 15개의 SMTP 명령을 지원합니다.

기타 Extended SMTP 명령(예: ATRN, ONEX, VERB, CHUNKING) 및 비공개 확장은 지원되지 않습니다. 지원되지 않는 명령은 X로 변환되고 내부 서버에서 거부됩니다. 메시지의 예를 들면 "500 Command unknown: 'XXX'"와 같습니다. 불완전한 명령은 취소됩니다.

ESMTP 검사 엔진은 서버 SMTP 배너의 문자를 별표로 변경합니다("2", "0", "0" 문자 제외). CR(캐리지 리턴) 및 LF(라인피드) 문자는 무시됩니다.

SMTP 검사를 활성화한 경우, 'SMTP 명령은 길이가 최소 4자여야 하고, 캐리지 리턴 및 라인피드로 끝나야 하며, 다음 회신을 보내기 전에 응답을 기다려야 함' 등의 규칙이 없으면 대화형 SMTP에 사용된 텔넷 세션이 중단될 수 있습니다.

SMTP 서버는 숫자 회신 코드 및 선택적으로 사람이 읽을 수 있는 문자열로 클라이언트 요청에 응답합니다. SMTP 애플리케이션 검사는 사용자가 사용할 수 있는 명령 및 서버가 반환할 수 있는 메시지를 제어 및 축소합니다. SMTP 검사는 세 가지 기본 작업을 수행합니다.

- SMTP 요청을 7개의 기본 SMTP 명령 및 8개의 확장 명령으로 제한합니다.
- SMTP 명령-응답 시퀀스를 모니터링합니다.
- 감사 추적 생성 - 메일 주소에 잘못된 문자가 포함되어 교체된 경우 감사 레코드 108002가 생성됩니다. 자세한 내용은 RFC 821을 참조하십시오.

SMTP 검사는 다음과 같은 비정상적 시그니처에 대한 명령 및 응답을 모니터링합니다.

- 명령이 잘림.
- 명령의 끝이 잘못됨(<CR><LR>로 끝나지 않음).
- MAIL 및 RCPT 명령은 메일의 발신자 및 수신자를 지정합니다. 메일 주소에서 이상한 문자를 스캔합니다. 파이프라인 문자(|)를 삭제합니다(공백으로 전환). "<", ">" 문자는 메일 주소를 정의하기 위해 사용된 경우에만 허용됩니다(">" 문자는 "<" 문자 뒤에 와야 함).
- SMTP 서버에 의한 예기치 않은 전환.
- 알 수 없는 명령에 대해 ASA는 패킷의 모든 문자를 X로 변경합니다. 이 경우 서버는 클라이언트에 오류 코드를 생성합니다. 패킷의 변경 때문에 TCP 체크섬이 다시 계산되거나 조정됩니다.
- TCP 스트림 편집.
- 명령 파이프라인.

예

다음 예는 기본 포트(25)에서 SMTP 트래픽을 확인하기 위해 클래스 맵을 만드는 SMTP 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다.

```
ciscoasa(config)# class-map smtp-port
ciscoasa(config-cmap)# match port tcp eq 25
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map smtp_policy
ciscoasa(config-pmap)# class smtp-port
ciscoasa(config-pmap-c)# inspect esmtp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy smtp_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.
show conn	SMTP를 비롯한 서로 다른 연결 유형의 연결 상태를 표시합니다.

inspect ftp

FTP 검사를 위한 포트를 구성하거나 고급 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect ftp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

구문 설명

map_name	FTP 검사 맵의 이름
strict	(선택 사항) FTP 트래픽의 고급 검사를 활성화하고 RFC 표준으로 규정 준수를 적용합니다.

기본값

FTP 검사는 기본적으로 활성화되어 있으며 ASA는 FTP용 포트 21에서 수신 대기합니다.

FTP를 더 높은 포트로 이동할 경우 경고를 사용합니다. 예를 들어 FTP 포트를 2021로 설정하면 포트 2021에 대해 시작되는 모든 연결은 FTP 명령으로서 해석되는 데이터 페이로드를 갖게 됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다. *map_name* 옵션이 추가되었습니다.

사용 지침

FTP 애플리케이션 검사는 FTP 세션을 검사하고 4가지 작업을 수행합니다.

- 동적 보조 데이터 연결 준비
- FTP 명령-응답 시퀀스 추적
- 감사 추적 생성
- 포함된 IP 주소 변환

FTP 애플리케이션 검사는 FTP 데이터 전송을 위한 보조 채널을 준비합니다. 이러한 채널용 포트는 PORT 또는 PASV 명령을 통해 협상됩니다. 파일 업로드, 파일 다운로드 또는 디렉토리 나열 이벤트에 대한 응답으로 채널이 할당됩니다.

참고 검사를 FTP 제어 연결용 포트에만 적용하고 데이터 연결용 포트에는 적용하지 않습니다. ASA 스테이트풀 검사 엔진은 필요에 따라 데이터 연결을 동적으로 준비합니다.

no inspect ftp 명령으로 FTP 검사 엔진을 비활성화하면 아웃바운드 사용자는 패시브 모드에서만 연결을 시작할 수 있으며 모든 인바운드 FTP는 비활성화됩니다.

엄격한 FTP

엄격한 FTP는 웹 브라우저가 FTP 요청에 포함된 명령을 전송하지 못하게 함으로써 보호 네트워크의 보안을 강화합니다. **inspect ftp** 명령을 이용하는 경우 **strict** 옵션을 포함합니다.

엄격한 FTP를 사용할 때에는 ASA를 통과할 수 없는 FTP 명령을 지정하기 위해 선택적으로 FTP 검사 정책 맵을 지정할 수 있습니다.

인터페이스에서 **strict** 옵션을 활성화하면 FTP 검사에서 다음 동작을 적용합니다.

- ASA에서 새 명령을 허용하려면 우선 FTP 명령을 인식해야 합니다.
- ASA는 포함된 명령을 전송하는 연결을 삭제합니다.
- 227 및 PORT 명령이 오류 문자열에 나타나지 않는지 확인합니다.

주의 **strict** 옵션을 사용하면 FTP RFC를 엄격하게 준수하지 않는 FTP 클라이언트가 실패할 수 있습니다.

strict 옵션이 활성화되면 FTP 명령 및 응답 시퀀스에서 다음과 같은 비정상적인 활동이 추적됩니다.

- 잘린 명령 - PORT 및 PASV 회신 명령에 쉼표가 5개 있는지 확인합니다. 5개가 아니면 PORT 명령이 잘린 것으로 간주되어 TCP 연결이 닫힙니다.
- 부정확한 명령 - RFC에서 규정한 대로 FTP 명령이 <CR><LF> 문자로 끝나는지 확인합니다. 그렇지 않으면 연결이 닫힙니다.
- RETR 및 STOR 명령의 크기 - 고정 상수를 기준으로 검토됩니다. 크기가 더 크면 오류 메시지가 기록되고 연결이 닫힙니다.
- 명령 스푸핑 - PORT 명령은 항상 클라이언트에서 전송되어야 합니다. PORT 명령이 서버에서 전송되면 TCP 연결이 거부됩니다.
- 회신 스푸핑 - PASV 회신 명령(227)은 항상 서버에서 전송되어야 합니다. PASV 회신 명령이 클라이언트에서 전송되면 TCP 연결이 거부됩니다. 이렇게 하여 사용자가 "227 xxxxx a1, a2, a3, a4, p1, p2"를 실행할 경우 보안 허점을 방지합니다.
- TCP 스트림 편집 - TCP 스트림 편집이 감지되면 ASA는 연결을 닫습니다.
- 잘못된 포트 협상 - 협상된 동적 포트 값이 1024 미만인지 확인합니다. 1~1024 범위의 포트 번호는 잘 알려진 연결에 예약되어 있으므로 협상된 포트가 이 범위에 있지 않으면 TCP 연결이 해제됩니다.
- 명령 파이프라인 - PORT 및 PASV 회신 명령에서 포트 번호 이후에 나오는 문자의 수를 상수 값 8로 확인합니다. 8보다 크면 TCP 연결이 종료됩니다.
- ASA는 FTP 클라이언트에 서버의 시스템 유형이 노출되는 것을 방지하기 위해 SYST 명령에 대한 FTP 서버 응답을 일련의 X로 교체합니다. 이 기본 동작을 재지정하려면 FTP 맵에서 **no mask-syst-reply** 명령을 사용합니다.

FTP 로그 메시지

FTP 애플리케이션 검사는 다음 로그 메시지를 생성합니다.

- 검색하거나 업로드하는 각 파일에 대해 감사 레코드 302002가 생성됩니다.
- 메모리가 부족하여 보조 동적 채널 준비가 실패하면 감사 레코드 201005가 생성됩니다.

예

사용자 이름과 비밀번호를 제출하기 전에 모든 FTP 사용자에게 인사 배너가 표시됩니다. 기본적으로 이 배너에는 시스템의 취약점을 파악하려는 해커에게 유용한 버전 정보가 포함되어 있습니다. 다음 예는 이러한 배너를 마스크 처리하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect ftp mymap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# class-map match-all ftp-traffic
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ftp-policy
ciscoasa(config-pmap)# class ftp-traffic
ciscoasa(config-pmap-c)# inspect ftp strict mymap
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy ftp-policy interface inside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
mask-syst-reply	클라이언트에서 오는 FTP 서버 응답을 숨깁니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
request-command deny	허용하지 않을 FTP 명령을 지정합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect gtp

GTP 검사를 활성화 또는 비활성화하거나, GTP 트래픽 또는 터널의 제어를 위해 GTP 맵을 정의하려면 클래스 컨피그레이션 모드에서 **inspect gtp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

참고 GTP 검사에는 특별한 라이센스가 필요합니다.

구문 설명

map_name	(선택 사항) GTP 맵의 이름

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

GTP는 GPRS용 터널링 프로토콜로서, 무선 네트워크를 통한 안전한 액세스를 제공합니다. GPRS는 기존 GSM 네트워크와 통합하도록 설계된 데이터 네트워크 아키텍처로서, 모바일 가입자에게 회사 네트워크 및 인터넷에 대한 패킷 교환식 무중단 데이터 서비스를 제공합니다. GTP의 개요는 CLI 컨피그레이션 가이드를 참조하십시오.

GTP 검사는 기본적으로 사용되지 않습니다. 그러나 자신의 검사 맵을 지정하지 않은 채 GTP 검사를 활성화하면 다음 프로세싱을 제공하는 기본 맵이 사용됩니다. 다른 값을 원하는 경우에만 맵을 구성해야 합니다.

- 오류는 허용되지 않습니다.
- 최대 요청 수는 200입니다.
- 최대 터널 수는 500입니다.
- GSN 시간 제한은 30분입니다.
- PDP 컨텍스트 시간 제한은 30분입니다.

- 요청 시간 제한은 1분입니다.
- 신호 시간 제한은 30분입니다.
- 터널링 시간 제한은 1시간입니다.
- T3 응답 시간 제한은 20초입니다.
- 알 수 없는 메시지 ID가 삭제 및 기록됩니다.

GTP용 매개변수를 정의하려면 **policy-map type inspect gtp** 명령을 사용합니다. GTP 맵을 정의한 후 **inspect gtp** 명령을 사용하여 맵을 활성화할 수 있습니다. 그런 다음 **class-map**, **policy-map** 및 **service-policy** 명령을 사용하여 트래픽의 클래스를 정의하고, 클래스에 **inspect** 명령을 적용하고, 하나 이상의 인터페이스에 정책을 적용할 수 있습니다.

잘 알려진 GTP용 포트는 UDP 3386 및 2123입니다.

신호 메시지 검사

신호 메시지 검사에서 **inspect gtp** 명령은 종종 미디어 엔드포인트(예: IP Phone)의 위치를 확인해야 합니다.

이 정보는 액세스 제어 및 미디어 트래픽의 NAT 상태가 수동 구성 없이 방화벽을 투명하게 통과하도록 준비하는 데 사용됩니다.

이러한 위치를 확인하는 과정에서 **inspect gtp** 명령은 터널 기본 게이트웨이 경로를 사용하지 **않습니다.** 터널 기본 게이트웨이 경로는 **route** *interface* **0 0** *metric* **tunneled** 형식의 경로입니다. 이 경로는 IPsec 터널에서 이그레스(egress)하는 패킷의 기본 경로를 재지정합니다. 따라서 VPN 트래픽에 **inspect gtp** 명령이 필요한 경우 터널 기본 게이트웨이 경로를 구성하지 마십시오. 대신 다른 고정 라우팅 또는 동적 라우팅을 사용하십시오.

예

다음 예는 네트워크에서 터널 수를 제한하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect gtp gmap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tunnel-limit 3000

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect gtp gmap

ciscoasa(config)# service-policy global_policy global
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.
show service-policy inspect gtp	**inspect gtp** 정책의 상태 및 통계를 보여줍니다.

inspect h323

H.323 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect h323** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect h323 {**h225** | **ras**} [*map_name*]

no inspect h323 {**h225** | **ras**} [*map_name*]

구문 설명

h225	H.225 신호 검사를 활성화합니다.
map_name	(선택 사항) H.323 맵의 이름.
ras	RAS 검사를 활성화합니다.

기본값

기본 포트 할당은 다음과 같습니다.

- h323 h225 1720
- h323 ras 1718-1719

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

inspect h323 명령은 Cisco CallManager 및 VocalTec Gatekeeper와 같은 H.323 호환 애플리케이션에 대한 지원을 제공합니다. H.323은 LAN을 통한 멀티미디어 회의를 위해 ITU(International Telecommunication Union)에서 정의한 프로토콜 모음입니다. ASA은 버전 6에서 H.323을 지원하며, 여기에는 H.323 v3 기능인 단일 통화 신호 채널에서의 다중 통화(Multiple Calls on One Call Signaling Channel)가 포함됩니다.

H.323 검사가 활성화되면 ASA는 H.323 버전 3에 추가된 기능인 동일한 통화 신호 채널에서의 다중 통화를 지원합니다. 이 기능은 통화 설정 시간을 단축하고 ASA의 포트 사용을 줄입니다.

H.323 검사의 중요한 두 가지 기능은 다음과 같습니다.

- H.225 및 H.245 메시지에 포함된 필수 IPv4 주소를 NAT 처리. H.323 메시지는 PER 인코딩 형식으로 인코딩되므로 ASA는 ASN.1 디코더를 사용하여 H.323 메시지를 디코딩합니다.
- 협상된 H.245 및 RTP/RTCP 연결을 동적으로 할당합니다.

신호 메시지 검사

신호 메시지 검사에서 **inspect h323** 명령은 종종 미디어 엔드포인트(예: IP Phone)의 위치를 확인해야 합니다.

이 정보는 액세스 제어 및 미디어 트래픽의 NAT 상태가 수동 구성 없이 방화벽을 투명하게 통과하도록 준비하는 데 사용됩니다.

이러한 위치를 확인하는 과정에서 **inspect h323** 명령은 터널 기본 게이트웨이 경로를 사용하지 **않습니다.** 터널 기본 게이트웨이 경로는 **route** *interface* **0 0** *metric* **tunneled** 형식의 경로입니다. 이 경로는 IPsec 터널에서 이그레스(egress)하는 패킷의 기본 경로를 재지정합니다. 따라서 VPN 트래픽에 **inspect h323** 명령이 필요한 경우 터널 기본 게이트웨이 경로를 구성하지 마십시오. 대신 다른 고정 라우팅 또는 동적 라우팅을 사용하십시오.

예

다음 예는 기본 포트(1720)에서 H.323 트래픽을 확인하기 위해 클래스 맵을 만드는 H.323 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다.

```
ciscoasa(config)# class-map h323-port
ciscoasa(config-cmap)# match port tcp eq 1720
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map h323_policy
ciscoasa(config-pmap)# class h323-port
ciscoasa(config-pmap-c)# inspect h323
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy h323_policy interface outside
```

관련 명령

명령	설명
policy-map type inspect	검사 정책 맵을 만듭니다.
show h225	ASA 전체에 설정된 H.225 세션에 대한 정보를 표시합니다.
show h245	느린 시작을 사용하여 엔드포인트에 의해 ASA 전체에 설정된 H.245 세션에 대한 정보를 표시합니다.
show h323 ras	ASA 전체에 설정된 H.323 RAS 세션에 대한 정보를 표시합니다.
timeout {h225 | h323}	H.225 신호 연결 또는 H.323 제어 연결이 닫히기까지의 유휴 시간을 구성합니다.

inspect http

HTTP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect http command** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect http [*map_name*]

no inspect http [*map_name*]

구문 설명

map_name	(선택 사항) HTTP 검사 맵의 이름

기본값

HTTP의 기본 포트는 80입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

팁 애플리케이션 및 URL 필터링을 수행하는 서비스 모듈을 설치할 수 있습니다 . 여기에는 ASA CX 또는 ASA FirePOWER 등의 HTTP 검사가 포함됩니다 . ASA 에서 실행되는 HTTP 검사는 이러한 모듈과 호환되지 않습니다 . HTTP 검사 정책 맵을 사용하여 ASA 에서 수동으로 구성하는 것보다 특수 모듈을 사용해 애플리케이션 필터링을 구성하는 것이 훨씬 쉽습니다 .

특정 공격 및 HTTP 트래픽과 관련된 기타 위협으로부터 보호하려면 HTTP 검사 엔진을 사용하십시오.

HTTP 애플리케이션 검사는 HTTP 헤더와 본문을 스캔하고 데이터에 대해 다양한 점검을 수행합니다. 이러한 점검은 HTTP 구조, 콘텐츠 유형, 터널링 및 메시징 프로토콜이 보안 어플라이언스를 통과하지 못하게 합니다.

애플리케이션 방화벽이라고도 하며 HTTP 검사 정책 맵을 구성할 때 이용할 수 있는 고급 HTTP 검사 기능은 네트워크 보안 정책을 우회하기 위해 HTTP 메시지를 사용하려는 공격자를 차단하는 데 도움이 될 수 있습니다.

HTTP 애플리케이션 검사는 악의적인 콘텐츠가 웹 서버에 도달하지 못하도록 HTTP 요청 및 응답에서 비 ASCII 문자 및 터널링된 애플리케이션을 차단할 수 있습니다. HTTP 요청 및 응답 헤더에서 다양한 요소의 크기 제한, URL 차단, HTTP 서버 헤더 유형 스푸핑 등도 지원됩니다.

고급 HTTP 검사는 모든 HTTP 메시지에서 다음을 확인합니다.

- RFC 2616에 적합한지 여부
- RFC 정의 메서드만 사용하는지 여부
- 추가 기준을 따르는지 여부

예

이 예에서는 모든 인터페이스를 통해 ASA로 들어오는 HTTP 연결(포트 80의 TCP 트래픽)이 HTTP 검사를 위해 분류됩니다. 정책은 글로벌 정책이므로 트래픽이 각 인터페이스로 들어갈 때에만 검사가 발생합니다.

```
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80

ciscoasa(config)# policy-map http_traffic_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# inspect http
ciscoasa(config)# service-policy http_traffic_policy global
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
policy-map type inspect	검사 정책 맵을 만듭니다.

inspect icmp

ICMP 검사 엔진을 구성하려면 클래스 컨피그레이션 모드에서 **inspect icmp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect icmp

no inspect icmp

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

ICMP 검사 엔진은 ICMP 트래픽을 TCP 및 UDP 트래픽처럼 검사할 수 있도록 허용합니다. ICMP 검사 엔진이 없는 경우에는 ICMP가 ACL에서 ASA를 통과하도록 허용하지 않는 것이 좋습니다. 상태 저장 검사가 없으면 ICMP가 네트워크를 공격하는 데 사용될 수 있습니다. ICMP 검사 엔진을 사용하면 각 요청에 대해 하나의 응답만 존재할 수 있으며 시퀀스 번호의 정확성이 보장됩니다.

ICMP 검사가 비활성화되면(기본 컨피그레이션) 더 낮은 보안 인터페이스에서 더 높은 보안 인터페이스로의 ICMP 에코 응답 메시지가 거부됩니다(ICMP 에코 요청에 응답하는 경우에도).

예

다음 예와 같이 ICMP 애플리케이션 검사 엔진을 활성화하면, ICMP 프로토콜 ID(IPv4의 경우 1, IPv6의 경우 58)를 사용하여 ICMP 트래픽을 확인하는 클래스 맵이 생성됩니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 ICMP 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy
ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
icmp	ASA 인터페이스에서 종료되는 ICMP 트래픽에 대한 액세스 규칙을 구성합니다.
policy-map	보안 작업을 하나 이상의 트래픽 클래스와 연결하는 정책을 정의합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect icmp error

ICMP 오류 메시지에 대한 애플리케이션 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect icmp error** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect icmp error

no inspect icmp error

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

ICMP 오류 검사가 활성화되면 ASA는 NAT 컨피그레이션을 기반으로 ICMP 오류 메시지를 전송하는 중간 홉(hop)에 대한 변환 세션을 만듭니다. ASA는 패킷을 변환된 IP 주소로 덮어씁니다.

이 검사가 비활성화되면 ASA는 ICMP 오류 메시지를 생성하는 중간 노드용 변환 세션을 만들지 않습니다. 내부 호스트와 ASA 사이의 중간 노드에 의해 생성되는 ICMP 오류 메시지는 NAT 리소스를 추가로 소모하지 않은 채 외부 호스트에 도달합니다. 외부 호스트가 traceroute 명령을 사용하여 ASA의 내부에 있는 목적지에 대한 홉을 추적하는 경우에는 이 방법이 바람직하지 않습니다. ASA가 중간 홉을 변환하지 않는 경우 모든 중간 홉은 매핑된 대상 IP 주소로 나타납니다.

원래 패킷에서 5개 튜플을 검색할 수 있도록 ICMP 페이로드 스캔이 수행됩니다. 검색된 5개 튜플을 사용하여 클라이언트의 원래 주소를 확인하기 위한 조회가 수행됩니다. ICMP 오류 검사 엔진은 ICMP 패킷을 다음과 같이 변경합니다.

- IP 헤더 - 매핑된 IP가 실제 IP(수신 주소)로 변경되고 IP 체크섬이 수정됩니다.
- ICMP 헤더 - ICMP 패킷의 변경으로 인해 ICMP 체크섬이 수정됩니다.
- 페이로드 변경 사항:
  - 원래 패킷의 매핑된 IP 가 실제 IP 로 변경됨
  - 원래 패킷의 매핑된 포트가 실제 포트로 변경됨
  - 원래 패킷 IP 체크섬이 다시 계산됨

예

다음 예는 ICMP 오류 애플리케이션 검사 엔진을 활성화하고, ICMP 프로토콜 ID(IPv4의 경우 1, IPv6의 경우 58)를 사용하여 ICMP 트래픽을 확인하는 클래스 맵을 생성합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 ICMP 오류 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy
ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp error
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
icmp	ASA 인터페이스에서 종료되는 ICMP 트래픽에 대한 액세스 규칙을 구성합니다.
inspect icmp	ICMP 검사 엔진을 활성화 또는 비활성화합니다.
policy-map	보안 작업을 하나 이상의 트래픽 클래스와 연결하는 정책을 정의합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect ils

ILS 애플리케이션 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect ils** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect ils

no inspect ils

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

inspect ils 명령은 LDAP를 사용해 ILS 서버와 디렉토리 정보를 교환하는 Microsoft NetMeeting, SiteServer 및 Active Directory 제품에 대한 NAT 지원을 제공합니다.

ASA는 ILS 또는 SiteServer Directory에서 엔드포인트를 등록하고 찾는 데 사용되는 ILS용 NAT를 지원합니다. LDAP 데이터베이스에는 IP 주소만 저장되므로 PAT는 지원되지 않습니다.

검색 응답을 위해, LDAP 서버가 외부에 있는 경우 내부 피어가 로컬로 통신하는 한편 외부 LDAP 서버에 등록하도록 하려면 NAT를 고려해야 합니다. 그러한 검색 응답에서는 xlate가 먼저 검색되고 그런 다음 정확한 주소를 얻기 위해 DNAT 항목이 검색됩니다. 두 검색에 모두 실패하면 주소가 변경되지 않습니다. NAT 0(NAT 없음)을 사용하고 DNAT 상호 작용이 예상되지 않는 사이트에 대해서는 성능 향상을 위해 검사 엔진을 꺼두는 것이 좋습니다.

ILS 서버가 ASA 경계 내부에 있는 경우 추가 컨피그레이션이 필요할 수 있습니다. 이 경우 외부 클라이언트가 지정된 포트(대개 TCP 389)에 있는 LDAP 서버에 액세스하려면 홀(hole)이 필요합니다.

ILS 트래픽은 보조 UDP 채널에서만 발생하므로 TCP 비활성 간격 이후 TCP 연결이 해제됩니다. 기본적으로 이 간격은 60분이며 **timeout** 명령으로 조정 가능합니다.

ILS/LDAP는 단일 TCP 연결을 통해 처리되는 세션이 있는 클라이언트/서버 모델을 따릅니다. 클라이언트의 작업에 따라 이러한 세션이 여러 개 생성될 수 있습니다.

연결 협상 기간 중에는 클라이언트에서 서버로 BIND PDU가 전송됩니다. 서버의 BIND RESPONSE가 성공적으로 수신되면 ILS Directory에서 작업을 수행할 수 있도록 다른 운영 메시지(예: ADD, DEL, SEARCH 또는 MODIFY)가 교환될 수 있습니다. ADD REQUEST 및 SEARCH RESPONSE PDU에는 NetMeeting 세션 설정을 위해 H.323(SETUP 및 CONNECT 메시지)에서 사용하는 NetMeeting 피어의 IP 주소가 포함될 수 있습니다. Microsoft NetMeeting v2.X 및 v3.X는 ILS 지원을 제공합니다.

ILS 검사는 다음 작업을 수행합니다.

- BER 디코딩 기능을 사용하여 LDAP REQUEST/RESPONSE PDU를 디코딩합니다.
- LDAP 패킷을 구문 분석합니다.
- IP 주소를 추출합니다.
- 필요에 따라 IP 주소를 변환합니다.
- ER 인코딩 기능을 사용하여 변환된 주소로 PDU를 인코딩합니다.
- 새로 인코딩된 PDU를 TCP 패킷에 다시 복사합니다.
- 점진적 TCP 체크섬 및 시퀀스 번호 조정을 수행합니다.

ILS 검사에는 다음과 같은 제한이 있습니다.

- 추천 요청 및 응답이 지원되지 않습니다.
- 여러 디렉토리의 사용자들이 통합되지 않습니다.
- 여러 디렉토리에서 여러 ID를 가지고 있는 단일 사용자를 NAT에서 인식하지 못합니다.

참고 H.225 통화 신호 트래픽은 보조 UDP 채널에서만 발생하므로 TCP **timeout** 명령으로 지정한 간격이 지나면 TCP 연결이 끊어집니다. 기본적으로 이 간격은 60분으로 설정됩니다.

예

다음 예에서와 같이 ILS 검사 엔진을 활성화하면, 기본 포트(389)에서 ILS 트래픽을 확인할 수 있도록 클래스 맵이 생성됩니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 ILS 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map ils-port
ciscoasa(config-cmap)# match port tcp eq 389
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ils_policy
ciscoasa(config-pmap)# class ils-port
ciscoasa(config-pmap-c)# inspect ils
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ils_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect im

인스턴트 메신저 트래픽의 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect im** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect im *map_name*

no inspect im *map_name*

구문 설명

map_name	IM 맵의 이름

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

inspect im 명령은 IM 프로토콜에 대한 애플리케이션 검사를 활성화 또는 비활성화합니다. IM 검사 엔진을 사용하면 IM의 네트워크 사용량을 제어할 수 있으며 기밀 데이터 유출, 웜의 전파 및 기업 네트워크에 대한 기타 위협을 막을 수 있습니다.

예

다음 예는 IM 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# regex loginname1 "user1\@example.com"
ciscoasa(config)# regex loginname2 "user2\@example.com"
ciscoasa(config)# regex loginname3 "user3\@example.com"
ciscoasa(config)# regex loginname4 "user4\@example.com"
ciscoasa(config)# regex yahoo_version_regex "1\.0"
ciscoasa(config)# regex gif_files ".*\.gif"
ciscoasa(config)# regex exe_files ".*\.exe"

ciscoasa(config)# class-map type regex match-any yahoo_src_login_name_regex
ciscoasa(config-cmap)# match regex loginname1
ciscoasa(config-cmap)# match regex loginname2

ciscoasa(config)# class-map type regex match-any yahoo_dst_login_name_regex
ciscoasa(config-cmap)# match regex loginname3
ciscoasa(config-cmap)# match regex loginname4
```

```
ciscoasa(config)# class-map type inspect im match-any yahoo_file_block_list
ciscoasa(config-cmap)# match filename regex gif_files
ciscoasa(config-cmap)# match filename regex exe_files

ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy
ciscoasa(config-cmap)# match login-name regex class yahoo_src_login_name_regex
ciscoasa(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy2
ciscoasa(config-cmap)# match version regex yahoo_version_regex

ciscoasa(config)# class-map im_inspect_class_map
ciscoasa(config-cmap)# match default-inspection-traffic

ciscoasa(config)# policy-map type inspect im im_policy_all
ciscoasa(config-pmap)# class yahoo_file_block_list
ciscoasa(config-pmap-c)# match service file-transfer
ciscoasa(config-pmap)# class yahoo_im_policy
ciscoasa(config-pmap-c)# drop-connection
ciscoasa(config-pmap)# class yahoo_im_policy2
ciscoasa(config-pmap-c)# reset
ciscoasa(config)# policy-map global_policy_name
ciscoasa(config-pmap)# class im_inspect_class_map
ciscoasa(config-pmap-c)# inspect im im_policy_all
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.
match protocol	검사 클래스 또는 정책 맵에서 특정 IM 프로토콜을 확인합니다.

inspect ip-options

패킷에서 IP 옵션의 검사를 활성화하려면 클래스 또는 정책 맵 유형 검사 컨피그레이션 모드에서 **inspect ip-options** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect ip-options [*map_name*]

no inspect ip-options *map_name*

구문 설명

map_name	(선택 사항) IP Options 맵의 이름.

기본값

이 명령은 전역 정책에서 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 또는 클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(2)	이 명령이 추가되었습니다.

사용 지침

패킷의 IP 헤더에는 Options 필드가 포함되어 있습니다. Options 필드(일반적으로 IP Options라고 함)는 몇몇 상황에서 필요한 제어 기능을 제공합니다. 그러나 대부분의 일반적인 통신에는 이러한 기능이 필요하지 않습니다. 특히 IP Options에는 타임스탬프, 보안 및 특별 라우팅을 위한 프로비전이 포함되어 있습니다. IP Options의 사용은 선택 사항이며, 필드에는 0개, 1개 또는 그 이상의 옵션을 포함할 수 있습니다.

ASA를 통과하도록 허용할 특정 IP 옵션의 IP 패킷을 제어하려면 IP Options 검사를 구성할 수 있습니다. 이 검사를 구성하면 ASA는 패킷이 통과하도록 허용하거나, 지정된 IP 옵션을 지운 다음 패킷이 통과하도록 허용합니다.

IP Options 검사는 패킷에서 다음 3개의 IP 옵션을 검사할 수 있습니다.

- EOOL(End of Options List) 또는 IP Option 0 - 단일 0바이트만을 포함하는 이 옵션은 모든 옵션의 끝에 나타나며 옵션 리스트의 끝을 마스크 처리합니다. 이것은 헤더 길이에 따른 헤더의 끝과 일치하지 않을 수 있습니다.
- NOP(No Operation) 또는 IP Option 1 - IP 헤더의 Options 필드는 0개, 1개 또는 그 이상의 옵션을 포함할 수 있습니다. 그러나 IP 헤더는 32비트의 배수여야 합니다. 모든 옵션의 비트 수가 32비트의 배수가 아니면 32비트 경계에 옵션을 맞추기 위해 NOP 옵션이 "internal padding"으로 사용됩니다.

- RTRALT(Router Alert) 또는 IP Option 20 - 이 옵션은 트랜싯 라우터에 패킷의 내용을 검사하도록 알립니다(패킷의 목적지가 해당 라우터가 아닌 경우에도). 이 검사는 RSVP 및 패킷의 배달 경로에 있는 라우터에서 비교적 복잡한 프로세싱을 수행하도록 요구하는 유사 프로토콜을 구현할 때 매우 유용합니다.

정책 맵 유형 검사 컨피그레이션 모드에서 **parameter** 명령을 사용하여 이 세 가지 IP 옵션의 검사를 구성합니다. 이러한 명령의 구문에 대한 자세한 내용은 **eool**, **nop** 및 **router-alert** 명령 페이지를 참조하십시오.

참고 IP Options 검사는 전역 검사 정책에 기본적으로 포함되어 있습니다. 따라서 ASA에서는 Router Alert 옵션(옵션 20)의 패킷을 포함하는 RSVP 트래픽을 허용합니다(ASA가 라우팅된 모드에 있을 때).

Router Alert 옵션이 포함된 RSVP 패킷을 삭제하면 VoIP 구현 시 문제가 발생할 수 있습니다.

IP 헤더에서 Router Alert 옵션을 지우도록 ASA를 구성하면 IP 헤더가 다음과 같이 변경됩니다.

- Options 필드가 32비트 경계로 끝나도록 채워집니다.
- IHL(Internet header length)이 변경됩니다.
- 패킷의 총 길이가 변경됩니다.
- 체크섬이 다시 계산됩니다.

IP 헤더에 EOOL, NOP 또는 RTRALT 이외의 옵션이 포함된 경우, 이러한 옵션을 허용하도록 ASA를 구성했는지 여부와 상관없이 ASA는 패킷을 삭제합니다.

예

다음 예는 ASA에서 패킷 헤더에 EOOL, NOP 및 RTRALT 옵션이 포함된 패킷을 전달하도록 허용하는 IP Options 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

패킷이 ASA를 통과하기 전에 **clear** 명령을 입력하면 패킷에서 IP 옵션이 지워집니다.

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
policy-map type inspect	검사 정책 맵을 만듭니다.

inspect ipsec-pass-thru

IPsec pass-through 검사를 활성화하려면 클래스 맵 컨피그레이션 모드에서 **inspect ipsec-pass-thru** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect ipsec-pass-thru [*map_name*]

no inspect ipsec-pass-thru [*map_name*]

구문 설명

map_name	(선택 사항) IPsec pass-through 맵의 이름.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

inspect ipsec-pass-thru 명령은 애플리케이션 검사를 활성화 또는 비활성화합니다. IPsec Pass-Through 애플리케이션 검사를 사용하면 IKE UDP 포트 500으로 연결된 ESP(IP 프로토콜 50) 및/또는 AH(IP 프로토콜 51) 트래픽의 통과를 편리하게 관리할 수 있습니다. 이 검사에서는 ESP 및 AH 트래픽 허용을 위해 긴 액세스 목록 컨피그레이션을 피하며, 시간 제한 및 최대 연결 수를 사용하여 보안을 제공합니다.

검사용 매개변수를 정의하는 데 사용할 특정 맵을 지정하려면 IPsec pass-through 매개변수 맵을 사용합니다. 매개변수 컨피그레이션에 액세스하려면 ESP 또는 AH 트래픽에 대한 제한을 지정할 수 있는 **policy-map type inspect** 명령을 사용합니다. 매개변수 컨피그레이션 모드에서 클라이언트당 최대 연결 수 및 유휴 시간 제한을 설정할 수 있습니다.

class-map, **policy-map** 및 **service-policy** 명령을 사용하여 트래픽의 클래스를 정의하고, 클래스에 **inspect** 명령을 적용하고, 하나 이상의 인터페이스에 정책을 적용할 수 있습니다. 정의된 매개변수 맵은 **inspect ipsec-pass-thru** 명령과 함께 사용할 경우 활성화됩니다.

NAT 및 비 NAT 트래픽은 허용되지만, PAT는 지원되지 않습니다.

참고 ASA 7.0(1)에서 **inspect ipsec-pass-thru** 명령은 ESP 트래픽의 통과만 허용했습니다. 이후 버전에서는 인수 없이 **inspect ipsec-pass-thru** 명령을 지정하는 경우 ESP를 허용하는 기본 맵이 생성 및 첨부되어 동일한 효과를 얻을 수 있습니다. 이 맵은 **show running-config all** 명령의 출력에서 볼 수 있습니다.

예

다음 예는 액세스 목록을 사용하여 IKE 트래픽을 식별하고, IPsec Pass-Through 매개변수 맵을 정의하고, 정책을 정의하고, 외부 인터페이스에 정책을 적용하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list ipsecpassthruacl permit udp any any eq 500
ciscoasa(config)# class-map ipsecpassthru-traffic
ciscoasa(config-cmap)# match access-list ipsecpassthruacl
ciscoasa(config)# policy-map type inspect ipsec-pass-thru iptmap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
ciscoasa(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
ciscoasa(config)# policy-map inspection_policy
ciscoasa(config-pmap)# class ipsecpassthru-traffic
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru iptmap
ciscoasa(config)# service-policy inspection_policy interface outside
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.
match protocol	검사 클래스 또는 정책 맵에서 특정 IM 프로토콜을 확인합니다.

inspect ipv6

IPv6 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect ipv6** 명령을 사용합니다. 매개변수 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect ipv6 [*map_name*]

no inspect ipv6 [*map_name*]

구문 설명

map_name	(선택 사항) IPv6 검사 정책 맵의 이름

기본값

IPv6 검사는 기본적으로 비활성화되어 있습니다.

IPv6 검사를 활성화하고 검사 정책 맵을 지정하지 않으면, 기본 IPv6 검사 정책 맵이 사용되며 다음과 같은 작업이 수행됩니다.

- 알려진 IPv6 확장 헤더만 허용됩니다. 적합하지 않은 패킷은 삭제되고 기록됩니다.
- IPv6 확장 헤더의 순서가 RFC 2460 사양에 정의된 대로 적용됩니다. 적합하지 않은 패킷은 삭제되고 기록됩니다.
- 라우팅 유형(routing type) 헤더가 포함된 패킷은 삭제됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

IPv6 검사를 사용하면 확장 헤더를 기반으로 IPv6 트래픽을 선택적으로 기록 또는 삭제할 수 있습니다. 또한 IPv6 검사는 IPv6 패킷에 있는 확장 헤더의 유형과 순서에 대해 RFC 2460의 준수 여부를 확인할 수 있습니다.

예

다음 예는 hop-by-hop, destination-option, routing-address 및 routing type 0 헤더의 모든 IPv6 트래픽을 삭제합니다.

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop
 match header destination-option
  drop
 match header routing-address count gt 0
  drop
 match header routing-type eq 0
  drop
policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
match header	IPv6 검사 정책 맵에서 IPv6 헤더를 확인합니다.
policy-map type inspect ipv6	IPv6용 검사 정책 맵을 생성합니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
verify-header	IPv6 검사 매개변수를 구성합니다.

inspect mgcp

MGCP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect mgcp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

구문 설명

map_name	(선택 사항) MGCP 맵의 이름

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

MGCP를 사용하려면 적어도 **inspect** 명령을 두 번 구성해야 합니다. 하나는 게이트웨이가 명령을 수신하는 포트에 대해, 다른 하나는 통화 에이전트가 명령을 수신하는 포트에 대해 구성합니다. 일반적으로 통화 에이전트는 게이트웨이 2427용 기본 MGCP 포트로 명령을 전송하고, 게이트웨이는 통화 에이전트 2727용 기본 MGCP 포트로 명령을 전송합니다.

MGCP는 미디어 게이트웨이 컨트롤러 또는 통화 에이전트라고 하는 외부 통화 제어 요소에서 미디어 게이트웨이를 제어하는 데 사용됩니다. 미디어 게이트웨이는 일반적으로 전화 회로에서 전달되는 오디오 신호와 인터넷이나 기타 패킷 네트워크를 통해 전달되는 데이터 패킷 간에 전환을 제공하는 네트워크 요소입니다. NAT 및 PAT를 MGCP와 함께 사용하면 제한된 외부(글로벌) 주소 집합으로 내부 네트워크에서 대량의 디바이스를 지원할 수 있습니다.

미디어 게이트웨이의 예는 다음과 같습니다.

- 트렁킹 게이트웨이 - 전화 네트워크와 VoIP(Voice over IP) 네트워크를 연결합니다. 이러한 게이트웨이는 일반적으로 대량의 디지털 회로를 관리 합니다.
- 가정용 게이트웨이 - VoIP 네트워크에 기존의 아날로그(RJ11) 인터페이스를 제공합니다. 가정용 게이트웨이의 예에는 케이블 모뎀/케이블 셋톱박스, xDSL 디바이스, 광대역 무선 디바이스 등이 있습니다.
- 비즈니스 게이트웨이 - VoIP 네트워크에 기존의 디지털 PBX 인터페이스 또는 통합된 소프트 PBX 인터페이스를 제공합니다.

MGCP 메시지는 UDP를 통해 전송됩니다. 응답은 명령의 소스 주소(IP 주소 및 UDP 포트 번호)로 다시 전송되지만, 명령 전송에 사용되었던 것과 동일한 주소에서 도착하지 않을 수 있습니다. 이는 장애 조치 컨피그레이션에서 여러 통화 엔진을 사용하는 경우, 명령을 수신한 통화 에이전트가 백업 통화 에이전트로 제어를 넘기고 백업 통화 에이전트에서 다시 응답을 전송하는 경우 발생합니다.

참고 MGCP 통화 에이전트는 MGCP 엔드포인트가 있는지 확인하기 위해 AUEP 메시지를 보냅니다. 이를 통해 ASA를 통과하는 흐름을 설정하고 MGCP 엔드포인트를 통화 에이전트에 등록할 수 있습니다.

하나 이상의 통화 에이전트 및 게이트웨이의 IP 주소를 구성하려면 MGCP 맵 컨피그레이션 모드에서 **call-agent** 및 **gateway** 명령을 사용합니다. 한 번에 명령 큐에서 허용할 최대 MGCP 명령 수를 지정하려면 MGCP 맵 컨피그레이션 모드에서 **command-queue** 명령을 사용합니다.

신호 메시지 검사

신호 메시지 검사에서 **inspect mgcp** 명령은 종종 미디어 엔드포인트(예: IP Phone)의 위치를 확인해야 합니다.

이 정보는 액세스 제어 및 미디어 트래픽의 NAT 상태가 수동 구성 없이 방화벽을 투명하게 통과하도록 준비하는 데 사용됩니다.

이러한 위치를 확인하는 과정에서 **inspect mgcp** 명령은 터널 기본 게이트웨이 경로를 사용하지 **않습니다.** 터널 기본 게이트웨이 경로는 **route** *interface* **0 0** *metric* **tunneled** 형식의 경로입니다. 이 경로는 IPsec 터널에서 이그레스(egress)하는 패킷의 기본 경로를 재지정합니다. 따라서 VPN 트래픽에 **inspect mgcp** 명령이 필요한 경우 터널 기본 게이트웨이 경로를 구성하지 마십시오. 대신 다른 고정 라우팅 또는 동적 라우팅을 사용하십시오.

큐에 추가할 수 있는 최대 MGCP 명령 수는 150입니다.

예 다음 예는 MGCP 트래픽을 식별하고, MGCP 검사 맵을 정의하고, 정책을 정의하고, 외부 인터페이스에 정책을 적용하는 방법을 보여줍니다. 먼저 기본 포트(2427 및 2727)에서 MGCP 트래픽을 확인할 클래스 맵이 생성됩니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 이 컨피그레이션에서는 통화 에이전트 10.10.11.5 및 10.10.11.6이 게이트웨이 10.10.10.115를 제어하고, 통화 에이전트 10.10.11.7 및 10.10.11.8이 게이트웨이 10.10.10.116 및 10.10.10.117을 제어할 수 있습니다. 모든 인터페이스에 대해 MGCP 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2427
ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2727
ciscoasa(config)# class-map mgcp_port
ciscoasa(config-cmap)# match access-list mgcp_acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect mgcp inbound_mgcp
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-agent 10.10.11.5 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.6 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.7 102
ciscoasa(config-pmap-p)# call-agent 10.10.11.8 102
ciscoasa(config-pmap-p)# gateway 10.10.10.115 101
ciscoasa(config-pmap-p)# gateway 10.10.10.116 102
ciscoasa(config-pmap-p)# gateway 10.10.10.117 102
ciscoasa(config-pmap-p)# command-queue 150
ciscoasa(config-mgcp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class mgcp_port
ciscoasa(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map type inspect mgcp	MGCP용 검사 정책 맵을 생성합니다.
show mgcp	ASA를 통해 설정된 MGCP 세션에 대한 정보를 표시합니다.
timeout	서로 다른 프로토콜 및 세션 유형에 대한 최대 유휴 시간을 설정합니다.

inspect mmp

MMP 검사 엔진을 구성하려면 클래스 컨피그레이션 모드에서 **inspect mmp** 명령을 사용합니다. MMP 검사를 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect mmp tls-proxy [*name*]

no inspect mmp tls-proxy [*name*]

구문 설명

name	TLS 프록시 인스턴스 이름을 지정합니다.
tls-proxy	MMP 검사용 TLS 프록시를 활성화합니다. MMP 프로토콜은 추가로 TCP 전송을 사용할 수 있지만, CUMA 클라이언트는 TLS 전송만 지원합니다. 따라서 MMP 검사를 활성화하려면 **tls-proxy** 키워드가 필요합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(4)	이 명령이 추가되었습니다.

사용 지침

ASA에는 CUMA MMP(Mobile Multiplexing Protocol)를 검증하기 위한 검사 엔진이 포함되어 있습니다. MMP는 CUMA 클라이언트와 서버 간에 데이터 엔티티를 전송하기 위한 데이터 전송 프로토콜입니다. ASA가 CUMA 클라이언트와 서버 간에 구축되어 있고 MMP 패킷의 검사가 필요한 경우 **inspect mmp** 명령을 사용합니다.

MMP 트래픽은 TLS 연결을 통해서만 전송되므로 MMP 검사는 TLS 프록시와 함께 활성화됩니다.

참고 MMP 검사 엔진을 구성하는 동안에는 기본 검사 클래스가 아닌 클래스에서만 추가할 수 있다는 점에 유의해야 합니다.

예

다음 예는 **inspect mmp** 명령을 사용하여 MMP 트래픽을 검사하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map mmp
ciscoasa(config-cmap)# match port tcp eq 5443
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map mmp-policy
ciscoasa(config-pmap)# class mmp
ciscoasa(config-pmap-c)# inspect mmp tls-proxy myproxy
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy mmp-policy interface outside
```

관련 명령

명령	설명
tls-proxy	TLS 프록시 인스턴스를 구성합니다.

inspect netbios

NetBIOS 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect netbios** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

구문 설명

map_name	(선택 사항) NetBIOS 맵의 이름

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

inspect netbios 명령은 NetBIOS 프로토콜에 대한 애플리케이션 검사를 활성화 또는 비활성화합니다. NetBIOS 검사는 기본적으로 사용됩니다. NetBIOS 검사 엔진은 ASA NAT 컨피그레이션에 따라 NBNS(NetBIOS Name Service) 패킷에서 IP 주소를 변환합니다. NetBIOS 프로토콜 위반 시 삭제 또는 기록하기 위한 정책 맵을 선택적으로 만들 수 있습니다.

예

다음 예는 NetBIOS 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect netbios netbios_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation drop
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
policy-map type inspect netbios	NetBIOS용 검사 정책 맵을 생성합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect pptp

PPTP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect pptp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect pptp

no inspect pptp

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

PPTP(Point-to-Point Tunneling Protocol)는 터널링 PPP 트래픽용 프로토콜입니다. PPTP 세션은 TCP 채널 1개 및 대개 PPTP GRE 터널 2개로 구성됩니다. TCP 채널은 PPTP GRE 터널의 협상 및 관리에 사용되는 제어 채널입니다. GRE 터널은 두 호스트 간 PPP 세션을 연결합니다.

활성화 시 PPTP 애플리케이션 검사는 PPTP 프로토콜 패킷을 검사하고, PPTP 트래픽 허용에 필요한 GRE 연결 및 xlate를 동적으로 만듭니다. RFC 2637에 정의된 대로 Version 1만 지원됩니다.

PAT는 PPTP TCP 제어 채널을 통해 협상된 경우 GRE의 수정된 버전[RFC 2637]에 대해서만 수행됩니다. GRE의 수정되지 않은 버전[RFC 1701, RFC 1702]에 대해서는 PAT(Port Address Translation)가 수행되지 *않습니다*.

특히 ASA는 PPTP 버전 선언 및 발신 전화 요청/응답 시퀀스를 검사합니다. RFC 2637에 정의된 대로 PPTP Version 1만 검사됩니다. 어느 한 쪽에서 선언한 버전이 Version 1이 아니면 TCP 제어 채널에 대한 추가 검사는 비활성화됩니다. 또한 발신 통화 요청 및 회신 시퀀스가 추적됩니다. 연결 및 xlate는 이후의 보조 GRE 데이터 트래픽을 허용하기 위해 필요한 경우 동적으로 할당됩니다.

PAT를 통해 변환하려면 PPTP 트래픽에 대해 PPTP 검사 엔진을 활성화해야 합니다. 또한 PAT는 GRE의 수정된 버전(RFC2637)에 대해서만, 그리고 PPTP TCP 제어 채널을 통해 협상된 경우에만 수행됩니다. GRE의 수정되지 않은 버전(RFC 1701 및 RFC 1702)에 대해서는 PAT가 수행되지 않습니다.

RFC 2637에 설명되어 있듯이 PPTP 프로토콜은 모뎀 뱅크 PAC(PPTP Access Concentrator)에서 시작되어 헤드엔드 PNS(PPTP Network Server)로 향하는 PPP 세션의 터널링에 주로 사용됩니다. 이렇게 사용되는 경우 PAC는 원격 클라이언트이고 PNS는 서버입니다.

그러나 Windows에서 VPN에 사용될 경우에는 상황이 반전됩니다. PNS는 중앙 네트워크에 액세스하기 위해 헤드엔드 PAC로의 연결을 시작하는 원격 단일 사용자 PC입니다.

모든 인터페이스에 대해 PPTP 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

예

다음 예에서와 같이 PPTP 검사 엔진을 활성화하면, 기본 포트(1723)에서 PPTP 트래픽을 확인할 수 있도록 클래스 맵이 생성됩니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다.

```
ciscoasa(config)# class-map pptp-port
ciscoasa(config-cmap)# match port tcp eq 1723
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pptp_policy
ciscoasa(config-pmap)# class pptp-port
ciscoasa(config-pmap-c)# inspect pptp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy pptp_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect radius-accouting

RADIUS 어카운팅 검사를 활성화 또는 비활성화하거나, 트래픽 또는 터널의 제어를 위해 맵을 정의하려면 클래스 컨피그레이션 모드에서 **inspect radius-accounting** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect radius-accounting *map_name*

no inspect radius-accounting [*map_name*]

구문 설명

map_name	RADIUS 어카운팅 맵의 이름

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

RADIUS 어카운팅 검사의 목적은 RADIUS 서버를 사용하는 GPRS 네트워크에 대한 과다 청구 공격을 방지하는 것입니다. RADIUS 어카운팅 검사를 구현하는 데 GTP/GPRS 라이센스가 필요하지는 않지만, GTP 검사를 구현하지 않고 GPRS 설정을 준비하지 않으면 아무런 소용이 없습니다.

RADIUS 어카운팅용 매개변수 정의에 사용할 검사 맵을 만들려면 **policy-map type inspect radius-accounting** 명령을 사용합니다. 매개변수 명령을 입력한 후 **send response**, **host**, **validate-attribute**, **enable gprs** 및 **timeout users** 명령을 사용하여 검사 특성 및 동작을 정의할 수 있습니다.

그런 다음 **class-map type management**, **policy-map** 및 **service-policy** 명령을 사용하여 트래픽의 클래스를 정의하고, 클래스에 **inspect radius-accounting** 명령을 적용하고, 하나 이상의 인터페이스에 정책을 적용할 수 있습니다.

참고 **inspect radius-accounting** 명령은 **class-map type management** 명령과 함께만 사용할 수 있습니다.

예

다음 예는 RADIUS 어카운팅 검사 맵을 구성하고 전체적으로 검사를 활성화하는 방법을 보여줍니다.

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

관련 명령

명령	설명
parameters	보안 작업을 적용할 트래픽 클래스를 정의합니다.
class-map type management	작업을 적용하고자 하는 ASA로 이동할 Layer 3 또는 4 관리 트래픽을 식별할 수 있습니다.
policy-map type inspect radius-accounting	RADIUS 어카운팅용 검사 정책 맵을 생성합니다.
show 및 **clear service-policy**	서비스 정책 설정을 보고 지울 수 있습니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect rsh

RSH 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect rsh** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect rsh

no inspect rsh

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

RSH 프로토콜은 RSH 클라이언트에서 RSH 서버로의 TCP 연결을 사용합니다(TCP 포트 514). 클라이언트와 서버는 클라이언트가 STDERR 출력 스트림을 수신 대기하는 TCP 포트 번호를 협상합니다. 필요한 경우 RSH 검사는 협상된 포트 번호의 NAT를 지원합니다.

예

다음 예는 기본 포트(514)에서 RSH 트래픽을 확인하기 위해 클래스 맵을 만드는 RSH 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 RSH 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map rsh-port
ciscoasa(config-cmap)# match port tcp eq 514
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rsh_policy
ciscoasa(config-pmap)# class rsh-port
ciscoasa(config-pmap-c)# inspect rsh
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rsh_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect rtsp

RTSP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect rtsp** 명령을 사용합니다. 매개변수 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect rtsp [*map_name*]

no inspect rtsp [*map_name*]

구문 설명

map_name	(선택 사항) RTSP 맵의 이름

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

inspect rtsp 명령은 ASA에서 RTSP 패킷을 전달하도록 합니다. RTSP는 RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer 및 Cisco IP/TV 연결에 사용됩니다.

참고 Cisco IP/TV에는 RTSP TCP 포트 554 및 TCP 8554를 사용하십시오.

RTSP 애플리케이션은 잘 알려진 포트 554와 함께 제어 채널로서 TCP(매우 드물게 UDP)를 사용합니다. ASA에서는 RFC 2326에 따라 TCP만 지원합니다. 이 TCP 제어 채널은 클라이언트에 구성된 전송 모드에 따라 오디오/비디오 트래픽 전송에 사용되는 데이터 채널을 협상하는 데 사용됩니다.

지원되는 RDT 전송은 rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp 및 x-pn-tng/udp입니다.

ASA에서는 상태 코드 200으로 Setup 응답 메시지를 구문 분석합니다. 응답 메시지가 인바운드로 이동하면 서버는 ASA를 기준으로 외부에 있는 것이며, 서버에서 인바운드로 들어오는 연결을 위해 동적 채널을 열어야 합니다. 응답 메시지가 아웃바운드로 이동하면 ASA에서는 동적 채널을 열 필요가 없습니다.

RFC 2326에서는 클라이언트 및 서버 포트가 setup 응답 메시지에 있어야 할 것을 요구하지 않으므로, ASA는 상태를 유지하며 setup 메시지에 있는 클라이언트 포트를 기억해야 합니다. QuickTime에서 setup 메시지에 클라이언트 포트를 추가하면 서버는 서버 포트로만 응답합니다.

RealPlayer 사용

RealPlayer를 사용할 때에는 전송 모드를 제대로 구성하는 것이 중요합니다. ASA에 대해 서버에서 클라이언트로 또는 그 반대로 **access-list** 명령을 추가합니다. RealPlayer의 경우 **Options > Preferences > Transport > RTSP Settings**를 선택하여 전송 모드를 변경합니다.

RealPlayer에서 TCP 모드를 사용하는 경우 **Use TCP to Connect to Server** 및 **Attempt to use TCP for all content** 확인란을 선택합니다. ASA에서 검사 엔진을 구성할 필요가 없습니다.

RealPlayer에서 UDP 모드를 사용하는 경우 **Use TCP to Connect to Server** 및 **Attempt to use UDP for static content** 확인란을 선택합니다. 멀티캐스트를 통해서는 라이브 콘텐츠를 이용할 수 없습니다. ASA에서 **inspect rtsp** *port* 명령을 추가합니다.

제한 사항

RSTP 검사에는 다음과 같은 제한이 적용됩니다.

- ASA는 UDP를 통한 멀티캐스트 RTSP 또는 RTSP 메시지를 지원하지 않습니다.
- ASA는 RTSP 메시지가 HTTP 메시지에 숨겨지는 HTTP 클로킹을 인식할 수 없습니다.
- 포함된 IP 주소가 HTTP 또는 RTSP 메시지의 일부로서 SDP에 포함되어 있지 않으므로 ASA는 RTSP 메시지에 대해 NAT를 수행할 수 없습니다. 패킷을 조각화할 수 없으므로 ASA는 조각난 패킷에 대해 NAT를 수행할 수 없습니다.
- Cisco IP/TV의 경우 ASA가 메시지의 SDP 부분에 대해 수행하는 변환의 수는 Content Manager에 있는 프로그램 목록의 수와 비례합니다(각 프로그램 목록에 추가할 수 있는 내장된 IP 주소는 최소 6개).
- Apple QuickTime 4 또는 RealPlayer에 대해 NAT를 구성할 수 있습니다. Viewer 및 Content Manager가 네트워크 외부에 있고 서버가 네트워크 내부에 있는 경우 Cisco IP/TV에는 NAT만 사용할 수 있습니다.

예

다음 예는 기본 포트(554 및 8554)에서 RTSP 트래픽을 확인하기 위해 클래스 맵을 만드는 RTSP 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다.

```
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 554
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 8554
ciscoasa(config)# class-map rtsp-traffic
ciscoasa(config-cmap)# match access-list rtsp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rtsp_policy
ciscoasa(config-pmap)# class rtsp-traffic
ciscoasa(config-pmap-c)# inspect rtsp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rtsp_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect scansafe

클래스에서 트래픽에 대해 Cloud Web Security 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect scansafe** 명령을 사용합니다. 먼저 **policy-map** 명령을 입력하여 클래스 컨피그레이션 모드에 액세스할 수 있습니다. 검사 작업을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

no inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

구문 설명

scansafe_policy_name	**policy-map type inspect scansafe** 명령으로 정의되는 검사 클래스 맵 이름을 지정합니다.
fail-open	(선택 사항) Cloud Web Security 서버를 사용할 수 없을 때 트래픽이 ASA를 통과하도록 허용합니다.
fail-close	(선택 사항) Cloud Web Security 서버를 사용할 수 없을 때 모든 트래픽을 삭제합니다. **fail-close**가 기본값입니다.

명령 기본값

fail-close가 기본값입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

Cisco Cloud Web Security는 SaaS(Software-as-a-Service) 모델을 통해 웹 보안 및 웹 필터링 서비스를 제공합니다. 네트워크에 ASA가 있는 기업은 추가 하드웨어를 설치하지 않고도 Cloud Web Security 서비스를 사용할 수 있습니다.

참고 이 기능을 "ScanSafe"라고 하며, 일부 명령에 ScanSafe 이름이 나타납니다.

Modular Policy Framework를 사용하여 이 명령을 구성합니다.

1. **policy-map type inspect scansafe** 명령을 사용하여 HTTP와 HTTPS용으로 각각 하나씩 검사 정책 맵을 만듭니다(두 가지 유형의 트래픽을 모두 검사한다고 가정).
2. (선택 사항) **class-map type inspect scansafe** 명령을 사용하여 화이트리스트를 구성합니다.

3. **class-map** 명령을 사용하여 검사하고자 하는 트래픽을 정의합니다. HTTP 및 HTTPS 트래픽에 대해 별도의 클래스 맵을 구성해야 합니다.
4. 정책을 정의하려면 **policy-map** 명령을 입력합니다.
5. HTTP의 경우 HTTP 클래스 맵을 참조하려면 **class** 명령을 입력합니다.
6. HTTP 검사 정책 맵을 참조하여 **inspect scansafe** 명령을 입력합니다.
7. HTTPS의 경우 HTTPS 클래스 맵을 참조하려면 **class** 명령을 입력합니다.
8. HTTPS 검사 정책 맵을 참조하여 **inspect scansafe** 명령을 입력합니다.
9. 끝으로 **service-policy** 명령을 사용하여 인터페이스에 정책 맵을 적용합니다.

예

다음 예는 HTTP 및 HTTPS에 대해 각각 하나씩 두 개의 클래스를 구성합니다. 각 ACL은 HTTP 및 HTTPS 모두에 대해 www.cisco.com, tools.cisco.com, DMZ 네트워크에 대한 트래픽을 제외합니다. 화이트리스트에 있는 몇몇 사용자와 그룹의 트래픽을 제외한 다른 모든 트래픽은 Cloud Web Security로 전송됩니다. 그런 다음 내부 인터페이스에 정책이 적용됩니다.

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# object network cisco1
ciscoasa(config-object-network)# fqdn www.cisco.com
ciscoasa(config)# object network cisco2
ciscoasa(config-object-network)# fqdn tools.cisco.com
ciscoasa(config)# object network dmz_network
ciscoasa(config-object-network)# subnet 10.1.1.0 255.255.255.0

ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
80
ciscoasa(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80

ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

ciscoasa(config)# class-map cws_class1
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTP
ciscoasa(config)# class-map cws_class2
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTPS
```

```
ciscoasa(config)# policy-map cws_policy
ciscoasa(config-pmap)# class cws_class1
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
ciscoasa(config-pmap)# class cws_class2
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
ciscoasa(config)# service-policy cws_policy inside
```

관련 명령

명령	설명
class-map type inspect scansafe	화이트리스트에 있는 사용자 및 그룹에 대한 검사 클래스 맵을 만듭니다.
default user group	ASA에서 ASA로 들어오는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**] (parameters)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
license	요청이 어느 조직에서 오는지를 나타내기 위해 ASA가 Cloud Web Security 프록시 서버에 전송하는 인증 키를 구성합니다.
match user group	화이트리스트를 기준으로 사용자 또는 그룹을 확인합니다.
policy-map type inspect scansafe	규칙에 대한 필수 매개변수를 구성하고 선택적으로 화이트리스트를 식별할 수 있도록 검사 정책 맵을 만듭니다.
retry-count	ASA 프록시 서버를 폴링하여 가용성 여부를 확인하기까지 Cloud Web Security에서 대기하는 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 컨텍스트 모드에서는 컨텍스트 단위로 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 정규화된 도메인 이름 또는 IP 주소를 구성합니다.
show conn scansafe	모든 Cloud Web Security 연결을 보여줍니다(대문자 Z 플래그로 표시됨).
show scansafe server	서버의 상태, 즉 현재 활성 서버인지, 백업 서버인지 또는 도달할 수 없는 서버인지를 보여줍니다.
show scansafe statistics	전체 및 현재 http 연결을 보여줍니다.
user-identity monitor	지정된 사용자 또는 그룹 정보를 AD 에이전트에서 다운로드합니다.
whitelist	트래픽의 클래스에 대해 화이트리스트 작업을 수행합니다.

inspect sip

SIP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect sip** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]

no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]

구문 설명

phone-proxy *proxy_name*	지정된 검사 세션에 대해 전화 프록시를 활성화합니다.
sip_map	SIP 정책 맵 이름을 지정합니다.
tls-proxy *proxy_name*	지정된 검사 세션에 대해 TLS 프록시를 활성화합니다. 키워드 **tls-proxy**는 Layer 7 정책 맵 이름으로서 사용할 수 없습니다.
uc-ime *proxy_name*	SIP 검사용 Cisco Intercompany Media Engine Proxy를 활성화합니다.

기본값

SIP 검사는 다음과 같은 기본 검사 맵을 사용하여 기본적으로 활성화됩니다.

- SIP IM(인스턴트 메시징) 확장: 사용됨
- SIP 포트의 비 SIP 트래픽: 허용됨
- 서버 및 엔드포인트의 IP 주소 숨기기: 사용되지 않음
- 마스크 소프트웨어 버전 및 비 SIP URI: 사용되지 않음
- 목적지로의 홉(hop) 수가 0보다 큰지 확인: 사용됨
- RTP 적합성: 적용되지 않음
- SIP 적합성: 상태 확인 및 헤더 검증을 수행하지 않음

암호화된 트래픽에 대한 검사도 수행되지 않습니다. 암호화된 트래픽을 검사하려면 TLS 프록시를 구성해야 합니다.

SIP에 기본적으로 할당되는 포트는 5060입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	**tls-proxy** 키워드가 추가되었습니다.
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

SIP는 인터넷 컨퍼런싱, 텔레포니, 프레즌스, 이벤트 알림 및 인스턴트 메시징에 가장 널리 사용되는 프로토콜입니다. 부분적으로 텍스트 기반 속성 때문에 그리고 부분적으로 유연성 때문에, SIP 네트워크는 다양한 보안 위협의 영향을 받을 수 있습니다.

SIP 애플리케이션 검사는 메시지 헤더 및 본문의 주소 변환, 동적인 포트 열기, 기본적인 온전성 확인 등을 제공합니다. 또한 애플리케이션 보안 및 프로토콜 적합성을 지원하여, SIP 메시지의 온전성을 적용하고 SIP 기반 공격을 감지합니다.

SIP 검사는 기본적으로 사용됩니다. 기본 이외의 프로세싱을 원하는 경우 또는 암호화된 트래픽 검사를 활성화하기 위해 TLS 프록시를 식별하고자 하는 경우에만 구성해야 합니다.

SIP 통화가 ASA를 통과하도록 지원하려면 미디어 연결 주소, 미디어 포트 및 미디어의 미발달 연결에 대한 신호 메시지를 검사해야 합니다. 잘 알려진 목적지 포트(UDP/TCP 5060)를 통해 신호가 전송되는 동안 미디어 스트림이 동적으로 할당되기 때문입니다. 또한 SIP는 IP 패킷의 사용자 데이터 부분에 IP 주소를 포함합니다. SIP 검사는 포함된 이러한 IP 주소에 대해 NAT를 적용합니다.

SIP 검사의 제한

SIP 검사는 포함된 IP 주소에 대해 NAT를 적용합니다. 그러나 소스 및 수신 주소를 모두 변환하도록 NAT를 구성하는 경우 외부 주소("trying" 응답 메시지에 대한 SIP 헤더의 "from")가 재작성되지 않습니다. 따라서 수신 주소를 변환하지 않도록 하려면 SIP 트래픽을 다룰 때 객체 NAT를 사용해야 합니다.

SIP와 함께 PAT를 사용할 때 다음과 같은 제한 및 제약이 적용됩니다.

- ASA에 의해 보호되는 네트워크에서 원격 엔드포인트가 SIP 프록시에 등록을 시도하면 다음과 같은 특별한 상황에서 등록이 실패합니다.
  - PAT 가 원격 엔드포인트용으로 구성되어 있습니다 .
  - SIP 등록 서버가 외부 네트워크에 있습니다 .
  - 엔드포인트가 프록시 서버로 보낸 REGISTER 메시지의 연락처 필드에 포트가 누락되어 있습니다 .
- SIP 디바이스가 SDP 부분에서 connection 필드(c=)가 아닌 owner/creator 필드(o=)에 IP 주소가 있는 패킷을 전송하는 경우, o= 필드의 IP 주소가 제대로 변환되지 않을 수 있습니다. 이는 o= 필드에 포트 값을 제공하지 않는 SIP 프로토콜의 제한 때문입니다.
- PAT를 사용할 때 포트 없이 내부 IP 주소를 포함하는 SIP 헤더 필드는 변환되지 않을 수 있는데, 이 경우 내부 IP 주소가 외부로 유출됩니다. 이 유출을 방지하려면 PAT 대신 NAT를 구성하십시오.

신호 메시지 검사

신호 메시지 검사에서 **inspect sip** 명령은 종종 미디어 엔드포인트(예: IP Phone)의 위치를 확인해야 합니다.

이 정보는 액세스 제어 및 미디어 트래픽의 NAT 상태가 수동 구성 없이 방화벽을 투명하게 통과하도록 준비하는 데 사용됩니다.

이러한 위치를 확인하는 과정에서 **inspect sip** 명령은 터널 기본 게이트웨이 경로를 사용하지 **않습니다.** 터널 기본 게이트웨이 경로는 **route** *interface* **0 0** *metric* **tunneled** 형식의 경로입니다. 이 경로는 IPsec 터널에서 이그레스(egress)하는 패킷의 기본 경로를 재지정합니다. 따라서 VPN 트래픽에 **inspect sip** 명령이 필요한 경우 터널 기본 게이트웨이 경로를 구성하지 마십시오. 대신 다른 고정 라우팅 또는 동적 라우팅을 사용하십시오.

예

다음 예는 기본 포트(5060)에서 SIP 트래픽을 확인하기 위해 클래스 맵을 만드는 SIP 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 SIP 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map sip-port
ciscoasa(config-cmap)# match port tcp eq 5060
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sip_policy
ciscoasa(config-pmap)# class sip-port
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sip_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map type inspect sip	SIP용 검사 정책 맵을 생성합니다.
show sip	ASA를 통해 설정된 SIP 세션에 대한 정보를 표시합니다.
show conn	서로 다른 연결 유형의 연결 상태를 표시합니다.
timeout	서로 다른 프로토콜 및 세션 유형에 대한 최대 유휴 시간을 설정합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

inspect skinny

SCCP(Skinny) 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect skinny** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

구문 설명

phone-proxy *proxy_name*	지정된 검사 세션에 대해 전화 프록시를 활성화합니다.
skinny_map	Skinny 정책 맵 이름을 지정합니다.
tls-proxy *proxy_name*	지정된 검사 세션에 대해 TLS 프록시를 활성화합니다. 키워드 **tls-proxy**는 Layer 7 정책 맵 이름으로서 사용할 수 없습니다.

기본값

SCCP 검사는 기본적으로 다음 기본값으로 사용됩니다.

- 등록: 적용되지 않음
- 최대 메시지 ID: 0x181
- 최소 접두사 길이: 4
- 미디어 시간 제한: 00:05:00
- 신호 시간 제한: 01:00:00
- RTP 적합성: 적용되지 않음

암호화된 트래픽에 대한 검사도 수행되지 않습니다. 암호화된 트래픽을 검사하려면 TLS 프록시를 구성해야 합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	**tls-proxy** 키워드가 추가되었습니다.
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

Skinny(SCCP)는 VoIP 네트워크에서 사용되는 간소화된 프로토콜입니다. SCCP를 사용하는 Cisco IP Phone이 H.323 환경에서 공존할 수 있습니다. Cisco CallManager와 함께 사용할 경우 SCCP 클라이언트는 H.323 호환 터미널과 상호 작용할 수 있습니다.

ASA는 SCCP용 PAT 및 NAT를 지원합니다. IP 전화기에 사용할 글로벌 IP 주소보다 IP 전화기가 더 많은 경우 PAT가 필요합니다. Skinny 애플리케이션 검사는 모든 SCCP 신호 및 미디어 패킷이 ASA를 통과할 수 있도록 SCCP 신호 패킷의 NAT 및 PAT를 지원합니다.

Cisco CallManager와 Cisco IP Phone 사이의 정상적인 트래픽은 SCCP를 사용하며, 특별한 컨피그레이션 없이 SCCP 검사에 의해 처리됩니다. ASA는 DHCP 옵션 150 및 66도 지원하며, 이는 TFTP 서버의 위치를 Cisco IP Phone 및 기타 DHCP 클라이언트에 전송하는 방식으로 구현됩니다. Cisco IP Phone의 요청에 기본 경로를 설정하는 DHCP 옵션 3도 포함될 수 있습니다.

참고 ASA는 SCCP 프로토콜 버전 22 이하에서 실행되는 Cisco IP Phone의 트래픽 검사를 지원합니다.

Cisco IP Phone 지원

Cisco CallManager가 Cisco IP Phone보다 보안 수준이 높은 인터페이스에 있을 때 Cisco CallManager IP 주소에 NAT가 필요한 경우에는 **고정인** 매핑을 사용해야 합니다. Cisco IP Phone을 사용하려면 컨피그레이션에 Cisco CallManager IP 주소가 명시적으로 지정되어 있어야 하기 때문입니다. 고정 ID 항목을 사용하면 보안 수준이 높은 인터페이스에 있는 Cisco CallManager에서 Cisco IP Phone의 등록을 허용할 수 있습니다.

Cisco IP Phone은 Cisco CallManager 서버에 연결하기 위해 필요한 컨피그레이션 정보를 다운로드하려면 TFTP 서버에 액세스할 수 있어야 합니다.

Cisco IP Phone이 TFTP 서버보다 보안 수준이 낮은 인터페이스에 있으면 UDP 포트 69에 있는 보호된 TFTP 서버에 연결하기 위해 ACL을 사용해야 합니다. TFTP 서버에 대해 고정 항목이 필요하지만, 고정 ID 항목일 필요는 없습니다. NAT를 사용할 경우 고정 ID 항목은 동일한 IP 주소에 매핑됩니다. PAT를 사용할 경우 정적 ID 항목은 동일한 IP 주소 및 포트에 매핑됩니다.

Cisco IP Phone이 TFTP 서버 및 Cisco CallManager보다 보안 수준이 *더 높은* 인터페이스에 있을 때 Cisco IP Phone이 연결을 시작할 수 있으려면 ACL 또는 고정 항목이 필요합니다.

제한 사항

내부 Cisco CallManager의 주소가 NAT 또는 PAT에 대해 다른 IP 주소 또는 포트로 구성된 경우, 외부 Cisco IP Phone의 등록이 실패하게 됩니다. ASA는 현재 TFTP를 통해 전송된 파일 콘텐츠에 대해 NAT 또는 PAT를 지원하지 않기 때문입니다. ASA는 TFTP 메시지의 NAT를 지원하고 TFTP 파일에 대한 핀홀을 엽니다. 그러나 ASA는 전화기 등록 중에 TFTP에 의해 전송된 Cisco IP Phone 컨피그레이션 파일에 포함된 Cisco CallManager IP 주소 및 포트를 변환할 수 없습니다.

참고 ASA는 통화 설정 중에 걸려오는 통화를 제외하고, SCCP 통화의 상태 기반 시스템 대체 작동을 지원합니다.

신호 메시지 검사

신호 메시지 검사에서 **inspect skinny** 명령은 종종 미디어 엔드포인트(예: IP Phone)의 위치를 확인해야 합니다.

이 정보는 액세스 제어 및 미디어 트래픽의 NAT 상태가 수동 구성 없이 방화벽을 투명하게 통과하도록 준비하는 데 사용됩니다.

이러한 위치를 확인하는 과정에서 **inspect skinny** 명령은 터널 기본 게이트웨이 경로를 사용하지 **않습니다.** 터널 기본 게이트웨이 경로는 **route** *interface* **0 0** *metric* **tunneled** 형식의 경로입니다. 이 경로는 IPsec 터널에서 이그레스(egress)하는 패킷의 기본 경로를 재지정합니다. 따라서 VPN 트래픽에 **inspect skinny** 명령이 필요한 경우 터널 기본 게이트웨이 경로를 구성하지 마십시오. 대신 다른 고정 라우팅 또는 동적 라우팅을 사용하십시오.

예

다음 예는 기본 포트(2000)에서 SCCP 트래픽을 확인하기 위해 클래스 맵을 만드는 SCCP 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 SCCP 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map skinny-port
ciscoasa(config-cmap)# match port tcp eq 2000
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map skinny_policy
ciscoasa(config-pmap)# class skinny-port
ciscoasa(config-pmap-c)# inspect skinny
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy skinny_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map type inspect skinny	SCCP용 검사 정책 맵을 생성합니다.
show skinny	ASA를 통해 설정된 SCCP 세션에 대한 정보를 표시합니다.
show conn	서로 다른 연결 유형의 연결 상태를 표시합니다.
timeout	서로 다른 프로토콜 및 세션 유형에 대한 최대 유휴 시간을 설정합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

inspect snmp

SNMP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect snmp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect snmp *map_name*

no inspect snmp *map_name*

구문 설명

map_name	SNMP 맵의 이름

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

snmp-map 명령으로 만든 SNMP 맵으로 구성된 설정을 사용하여 SNMP 검사를 활성화하려면 **inspect snmp** 명령을 사용합니다. SNMP 트래픽을 SNMP의 특정 버전으로 제한하려면 SNMP 맵 컨피그레이션 모드에서 **deny version** 명령을 사용합니다.

SNMP의 이전 버전은 덜 안전하므로, 보안 정책에서 SNMP 트래픽을 Version 2로 제한하도록 요구할 수 있습니다. SNMP의 특정 버전을 거부하려면 **snmp-map** 명령으로 만들 수 있는 SNMP 맵 내에서 **deny version** 명령을 사용합니다. SNMP 맵을 구성한 후 **inspect snmp** 명령을 사용하여 맵을 활성화하고 **service-policy** 명령을 사용하여 하나 이상의 인터페이스에 적용합니다.

모든 인터페이스에 대해 엄격한 snmp 애플리케이션 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

예

다음 예는 SNMP 트래픽을 식별하고, SNMP 맵을 정의하고, 정책을 정의하고, SNMP 검사를 활성화하고, 외부 인터페이스에 정책을 적용합니다.

```
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)# exit
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
deny version	SNMP의 특정 버전을 사용하여 트래픽을 거부합니다.
snmp-map	SNMP 맵을 정의하고 SNMP 맵 컨피그레이션 모드를 활성화합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect sqlnet

Oracle SQL*Net 애플리케이션 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect sqlnet** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect sqlnet

no inspect sqlnet

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 사용됩니다.

기본 포트 할당은 1521입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

SQL*Net 프로토콜은 데이터 스트림이 ASA의 양쪽에서 Oracle 애플리케이션에 일관성 있게 표시되도록 ASA에서 처리하는 서로 다른 패킷 유형으로 구성되어 있습니다.

SQL*Net에 기본적으로 할당되는 포트는 1521입니다. Oracle for SQL*Net에서 이 값을 사용하지만, 이 값은 SQL(Structured Query Language)용 IANA 포트 할당과 일치하지 않습니다. 포트 번호 범위에 SQL*Net 검사를 적용하려면 **class-map** 명령을 사용하십시오.

참고 SQL 컨트롤 TCP 포트 1521과 동일한 포트에서 SQL 데이터 전송이 발생하는 경우 SQL*Net 검사를 비활성화하십시오. SQL*Net 검사가 활성화되면 ASA는 프록시 역할을 하여 클라이언트 윈도우 크기를 65000에서 약 16000으로 줄이므로 데이터 전송 문제가 발생할 수 있습니다.

ASA는 모든 주소를 NAT 처리하고, SQL*Net Version 1에 대해 열 수 있도록 패킷에서 모든 포함된 포트를 찾습니다.

SQL*Net Version 2의 경우 데이터 길이 0으로 REDIRECT 패킷 바로 뒤에 오는 모든 DATA 또는 REDIRECT 패킷은 고정됩니다.

고정이 필요한 패킷에는 다음과 같은 형식으로 호스트/포트 주소가 포함되어 있습니다.

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net Version 2 TNSFrame 유형(Connect, Accept, Refuse, Resend 및 Marker)에서는 NAT에 대한 주소 스캔이 수행되지 않으며 패킷에 포함된 포트에 대한 개방형 동적 연결을 검사하지 않습니다.

페이로드에 대한 데이터 길이 0의 REDIRECT TNSFrame 유형이 앞에 오는 경우에는 열어야 하는 포트 및 NAT에 대한 주소를 SQL*Net Version 2 TNSFrames, Redirect 및 Data 패킷에서 스캔합니다. 데이터 길이 0의 Redirect 메시지가 ASA를 통과하면, 뒤이어 오는 NAT 처리해야 할 Data 또는 Redirect 메시지 및 동적으로 열어야 할 포트를 예상하여 연결 데이터 구조에 플래그가 설정됩니다. 이전 단락의 TNS 프레임 중 하나가 Redirect 메시지 뒤에 도착하면 플래그가 재설정됩니다.

SQL*Net 검사 엔진은 새 메시지와 이전 메시지의 길이 델타를 사용하여 체크섬을 다시 계산하고, IP와 TCP 길이를 변경하며, 시퀀스 번호 및 확인 응답 번호를 다시 조정합니다.

다른 모든 경우에는 SQL*Net Version 1로 간주됩니다. TNSFrame 유형(Connect, Accept, Refuse, Resend, Marker, Redirect 및 Data) 및 모든 패킷에서는 포트 및 주소가 스캔됩니다. 주소가 NAT 처리되며 포트 연결이 열립니다.

예

다음 예는 기본 포트(1521)에서 SQL*Net 트래픽을 확인하기 위해 클래스 맵을 만드는 SQL*Net 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 SQL*Net 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map sqlnet-port
ciscoasa(config-cmap)# match port tcp eq 1521
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sqlnet_policy
ciscoasa(config-pmap)# class sqlnet-port
ciscoasa(config-pmap-c)# inspect sqlnet
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sqlnet_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.
show conn	SQL*net을 비롯한 서로 다른 연결 유형의 연결 상태를 표시합니다.

inspect sunrpc

Sun RPC 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect sunrpc** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect sunrpc

no inspect sunrpc

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

Sun RPC 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면, 정책 맵 컨피그레이션 모드 내에서 **class** 명령을 사용하여 액세스할 수 있는 정책 맵 클래스 컨피그레이션 모드에서 **inspect sunrpc** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect sunrpc 명령은 Sun RPC 프로토콜에 대한 애플리케이션 검사를 활성화 또는 비활성화합니다. NFS 및 NIS에서 Sun RPC를 사용합니다. Sun RPC 서비스는 시스템의 어느 포트에서나 실행할 수 있습니다. 클라이언트가 서버의 Sun RPC 서비스에 액세스하려면 현재 서비스가 실행 중인 포트를 알아야 합니다. 이 작업은 잘 알려진 포트 111에서 portmapper 프로세스를 쿼리하여 수행됩니다.

클라이언트는 서비스의 Sun RPC 프로그램 번호를 전송하고 포트 번호를 가져옵니다. 이 시점부터 클라이언트 프로그램은 Sun RPC 쿼리를 새 포트에 전송합니다. 서버가 회신을 전송할 때 ASA는 이 패킷을 가로채고 해당 포트에서 두 개의 미발달 TCP 및 UDP 연결을 모두 엽니다.

참고 Sun RPC 페이로드 정보의 NAT 또는 PAT는 지원되지 않습니다.

예

다음 예는 기본 포트(111)에서 RPC 트래픽을 확인하기 위해 클래스 맵을 만드는 RPC 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 RPC 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map sunrpc-port
ciscoasa(config-cmap)# match port tcp eq 111
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sample_policy
ciscoasa(config-pmap)# class sunrpc-port
ciscoasa(config-pmap-c)# inspect sunrpc
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sample_policy interface outside
```

관련 명령

명령	설명
clear configure sunrpc_server	**sunrpc-server** 명령을 사용하여 수행된 컨피그레이션이 제거됩니다.
clear sunrpc-server active	NFS 또는 NIS 등 특정 서비스에 대한 Sun RPC 애플리케이션 검사에 의해 열린 핀홀이 지워집니다.
show running-config sunrpc-server	Sun RPC 서비스 테이블 컨피그레이션에 대한 정보를 표시합니다.
sunrpc-server	Sun RPC 서비스(예: NFS 또는 NIS)에 대해 지정된 시간 제한으로 핀홀을 생성하도록 허용합니다.
show sunrpc-server active	Sun RPC 서비스에 대해 열린 핀홀을 표시합니다.

inspect tftp

TFTP 애플리케이션 검사를 비활성화하려면(또는 전에 비활성화된 경우 활성화하려면) 클래스 컨피그레이션 모드에서 **inspect tftp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect tftp

no inspect tftp

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 사용됩니다.

기본 포트 할당은 69입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

RFC 1350에 기술되어 있는 TFTP(Trivial File Transfer Protocol)는 TFTP 서버와 클라이언트 간에 파일을 읽고 쓰기 위한 간단한 프로토콜입니다.

ASA는 TFTP 트래픽을 검사하고 TFTP 클라이언트와 서버 간 파일 전송을 허용하기 위해 필요할 경우 연결과 변환을 동적으로 생성합니다. 특히 검사 엔진은 TFTP 읽기 요청(RRQ), 쓰기 요청(WRQ) 및 오류 알림(ERROR)을 검사합니다.

유효한 읽기(RRQ) 또는 쓰기(WRQ) 요청을 수신할 경우 필요에 따라 동적 보조 채널 및 PAT 변환이 할당됩니다. 이 보조 채널은 이후 파일 전송 또는 오류 알림을 위해 TFTP에서 사용됩니다.

TFTP 서버만이 보조 채널을 통해 트래픽을 시작할 수 있으며, TFTP 클라이언트와 서버 사이에는 불완전한 보조 채널이 최대 하나만 존재할 수 있습니다. 서버에서 오류 알림을 보내면 보조 채널이 닫힙니다.

TFTP 트래픽 리디렉션에 고정 PAT가 사용되는 경우 TFTP 검사를 활성화해야 합니다.

예

다음 예는 기본 포트(69)에서 TFTP 트래픽을 확인하기 위해 클래스 맵을 만드는 TFTP 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 TFTP 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map tftp-port
ciscoasa(config-cmap)# match port udp eq 69
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map tftp_policy
ciscoasa(config-pmap)# class tftp-port
ciscoasa(config-pmap-c)# inspect tftp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy tftp_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect waas

WAAS 애플리케이션 검사를 활성화하려면 클래스 컨피그레이션 모드에서 **inspect waas** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect waas

no inspect waas

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 기본 검사 클래스에서 WAAS 애플리케이션 검사를 활성화하는 방법을 보여줍니다.

```
policy-map global_policy
 class inspection_default
  inspect waas
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

inspect xdmcp

XDMCP 애플리케이션 검사를 활성화하거나 ASA가 수신 대기하는 포트를 변경하려면 클래스 컨피그레이션 모드에서 **inspect xdmcp** 명령을 사용합니다. 클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

inspect xdmcp

no inspect xdmcp

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었고, 사용하지 않게 된 **fixup** 명령을 대체했습니다.

사용 지침

inspect xdmcp 명령은 XDMCP 프로토콜에 대한 애플리케이션 검사를 활성화 또는 비활성화합니다.

XDMCP는 UDP 포트 177을 사용하여 X 세션을 협상하는 프로토콜이며, 설정 시 TCP가 사용됩니다.

성공적으로 협상하여 XWindows 세션을 시작하려면 ASA는 Xhosted 컴퓨터에서 오는 TCP 반환 연결을 허용해야 합니다. 반환 연결을 허용하려면 ASA에서 **established** 명령을 사용합니다. XDMCP가 디스플레이를 전송할 포트에 대한 협상을 완료하면, 이 반환 연결의 허용 여부를 확인하기 위해 **established** 명령이 사용됩니다.

XWindows 세션 중에 관리자는 잘 알려진 포트 6000 l n의 디스플레이 Xserver와 통신합니다. 다음과 같은 터미널 설정의 결과 각 디스플레이는 Xserver에 별도로 연결됩니다.

```
setenv DISPLAY Xserver:n
```

여기서 *n*은 디스플레이 번호입니다.

XDMCP를 사용할 경우 IP 주소를 사용하여 디스플레이를 협상하며, 필요 시 ASA에서는 NAT를 지원할 수 있습니다. XDCMP 검사는 PAT를 지원하지 않습니다.

예

다음 예는 기본 포트(177)에서 XDMCP 트래픽을 확인하기 위해 클래스 맵을 만드는 XDMCP 검사 엔진을 활성화합니다. 그런 다음 외부 인터페이스에 서비스 정책이 적용됩니다. 모든 인터페이스에 대해 XDMCP 검사를 활성화하려면 **interface outside** 대신 **global** 매개변수를 사용합니다.

```
ciscoasa(config)# class-map xdmcp-port
ciscoasa(config-cmap)# match port tcp eq 177
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map xdmcp_policy
ciscoasa(config-pmap)# class xdmcp-port
ciscoasa(config-pmap-c)# inspect xdmcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy xdmcp_policy interface outside
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

3 장

integrity through ip verify reverse-path 명령

integrity

AnyConnect IPsec 연결을 위한 IKEv2 SA(Security Association)에서 ESP 무결성 알고리즘을 지정하려면 IKEv2 정책 컨피그레이션 모드에서 **integrity** 명령을 사용합니다. 이 명령을 제거하고 기본 설정을 사용하려면 이 명령의 **no** 형식을 사용합니다.

integrity {md5 | sha | sha256 | sha384 | sha512 | null}

no integrity {md5 | sha | sha256 | sha384 | sha512 | null}

구문 설명

md5	ESP 무결성 보호를 위해 MD5 알고리즘을 지정합니다.
null	암호화 알고리즘으로 AES-GCM을 지정한 경우 관리자가 IKEv2 무결성 알고리즘으로 null을 선택할 수 있게 합니다.
sha	(기본값) ESP 무결성 보호를 위해 SHA(Secure Hash Algorithm) SHA 1(미국 FIPS(Federal Information Processing Standard)에서 정의)을 지정합니다.
sha256	256비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha384	384비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha512	512비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.

기본값

기본값은 **sha**(SHA 1 알고리즘)입니다.

사용 지침

IKEv2 SA는 IKEv2 피어가 phase 2에서 안전하게 통신할 수 있도록 phase 1에서 사용되는 키입니다. ESP 프로토콜에 대해 무결성 알고리즘을 설정하려면 **crypto ikev2 policy** 명령을 입력한 후 **integrity** 명령을 사용합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.
8.4(2)	SHA 2 지원을 위해 **sha256**, **sha384** 및 **sha512** 키워드가 추가되었습니다.
9.0(1)	Null 옵션이 IKEv2 무결성 알고리즘으로 추가되었습니다.

예

다음 예는 IKEv2 정책 컨피그레이션 모드로 들어가서 무결성 알고리즘을 MD5로 설정합니다.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5
```

관련 명령

명령	설명
encryption	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 암호화 알고리즘을 지정합니다.
group	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 Diffie-Hellman 그룹을 지정합니다.
lifetime	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 SA 수명을 지정합니다.
prf	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 PRF(의사 난수 함수)를 지정합니다.

intercept-dhcp

DHCP 인터셉트를 활성화하려면 그룹 정책 컨피그레이션 모드에서 **intercept-dhcp enable** 명령을 사용합니다. 실행 중인 컨피그레이션에서 **intercept-dhcp** 특성을 제거하고 사용자가 기본 또는 기타 그룹 정책에서 DHCP 인터셉트 컨피그레이션을 상속하도록 하려면 이 명령의 **no** 형식을 사용합니다.

intercept-dhcp *netmask* {**enable** | **disable**}

no intercept-dhcp

구문 설명

disable	DHCP 인터셉트를 비활성화합니다.
enable	DHCP 인터셉트를 활성화합니다.
netmask	터널 IP 주소의 서브넷 마스크를 제공합니다.

기본값

DHCP 인터셉트는 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

DHCP 인터셉트를 비활성화하려면 **intercept-dhcp disable** 명령을 사용합니다.

Split tunnel 옵션이 255바이트를 초과하면 Microsoft XP에서 비정상적으로 도메인 이름이 손상될 수 있습니다. 이 문제를 피하기 위해 ASA는 전송하는 경로의 수를 27~40으로 제한하며 경로의 클래스에 따라 경로의 수를 조정합니다.

DHCP 인터셉트를 활성화하면 Microsoft XP 클라이언트는 ASA에서 split-tunneling을 사용할 수 있습니다. ASA는 Microsoft Windows XP 클라이언트 DHCP Inform 메시지에 직접 응답하여, 해당 클라이언트에 터널 IP 주소의 서브넷 마스크, 도메인 이름 및 클래스리스 고정 경로를 제공합니다. XP 이전의 Windows 클라이언트에 대해, DHCP 인터셉트는 도메인 이름 및 서브넷 마스크를 제공합니다. 이는 DHCP 서버 사용이 유리하지 않은 환경에서 유용합니다.

예

다음 예는 그룹 정책 FirstGroup에 대해 DHCP 인터셉트를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# intercept-dhcp enable
```

interface

인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **interface** 명령을 사용합니다. 하위 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다. 물리적 인터페이스 또는 매핑된 인터페이스를 제거할 수 없습니다.

물리적 인터페이스의 경우(ASASM을 제외한 모든 모델):

interface *physical_interface*

하위 인터페이스의 경우(ASA 5505 또는 ASASM, 또는 ASA 5512-X~ASA 5555-X의 관리 인터페이스에는 사용 불가):

interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}**.***subinterface*

no interface {*physical_interface* | **redundant** *number* | **port-channel** *number*}**.***subinterface*

매핑된 이름이 할당된 다중 컨텍스트 모드의 경우:

interface *mapped_name*

구문 설명

mapped_name	다중 컨텍스트 모드에서는 **allocate-interface** 명령을 사용하여 할당된 경우 매핑된 이름을 지정합니다.
physical_interface	물리적 인터페이스 유형, 슬롯 및 포트 번호를 *type*[*슬롯*/]*포트* 형식으로 지정합니다. type과 슬롯/포트 간 공백은 선택 사항입니다. 물리적 인터페이스 유형은 다음과 같습니다. • **ethernet** • **gigabitethernet** • **tengigabitethernet** • **management** 유형 뒤에는 슬롯/포트를 입력합니다(예: **gigabitethernet0/1**). 관리 인터페이스는 관리 트래픽 전용입니다. 그러나 모델에 따라 원하는 경우 통과 트래픽에 사용할 수도 있습니다(**management-only** 명령 참조). 인터페이스 유형, 슬롯 및 포트 번호를 확인하려면 모델과 함께 제공된 하드웨어 설명서를 참조하십시오.
subinterface	논리적 하위 인터페이스를 지정하는 1~4294967293 범위의 정수를 지정합니다. 하위 인터페이스의 최대 수는 ASA 모델에 따라 다릅니다. ASA 5505, ASASM 또는 ASA 5512-X~ASA 5555-X의 관리 인터페이스에는 하위 인터페이스를 사용할 수 없습니다. 플랫폼당 최대 하위 인터페이스(또는 VLAN)는 컨피그레이션 가이드를 참조하십시오. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다.

기본값

기본적으로 ASA는 모든 물리적 인터페이스에 대해 **interface** 명령을 자동으로 생성합니다.

다중 컨텍스트 모드에서 ASA는 **allocate-interface** 명령을 사용하여 컨텍스트에 할당된 모든 인터페이스에 대해 **interface** 명령을 자동으로 생성합니다.

인터페이스의 기본 상태는 유형 및 컨텍스트 모드에 따라 다릅니다.

- 다중 컨텍스트 모드, 컨텍스트 - 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 인터페이스가 시스템 실행 영역에서도 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 상황에서 중지됩니다.
- 단일 모드 또는 다중 컨텍스트 모드, 시스템 - 인터페이스에는 다음과 같은 기본 상태가 있습니다.
  - 물리적 인터페이스 - 비활성화되어 있습니다 .
  - 하위 인터페이스 - 활성화되어 있습니다 . 그러나 하위 인터페이스를 통해 트래픽을 전달하려면 물리적 인터페이스도 활성화되어야 합니다 .

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	새 하위 인터페이스 명명 규칙을 허용하고 인터페이스 컨피그레이션 모드에서 인수를 별도의 명령으로 변경할 수 있도록 이 명령이 수정되었습니다.

사용 지침

인터페이스 컨피그레이션 모드에서는 인터페이스 유형 및 보안 컨텍스트 모드에 따라 하드웨어 설정을 구성하고(물리적 인터페이스에 대해), 이름을 할당하고, VLAN을 할당하고, IP 주소를 할당하고, 기타 여러 설정을 구성할 수 있습니다.

활성화된 인터페이스가 트래픽을 통과하도록 하려면 **nameif** 및 **ip address**(라우팅된 모드의 경우) 인터페이스 컨피그레이션 모드 명령을 구성합니다. 하위 인터페이스의 경우 **vlan** 명령도 구성합니다.

인터페이스 설정을 변경한 경우, 기존 연결이 시간 초과될 때까지 기다리지 않고 새 보안 정보를 사용하려면 **clear local-host** 명령을 사용하여 연결을 해제합니다.

ASA 5512-X부터 ASA 5555-X 버전까지 Management 0/0 인터페이스의 특징은 다음과 같습니다.

- 통과 트래픽을 지원하지 않음
- 하위 인터페이스를 지원하지 않음
- 우선순위 대기열을 지원하지 않음
- 멀티캐스트 MAC을 지원하지 않음
- IPS SSP 소프트웨어 모듈에서는 Management 0/0 인터페이스를 공유합니다. ASA 및 IPS 모듈에 대해 별도의 MAC 주소와 IP 주소가 지원됩니다. IPS 운영 체제 내에서 IPS IP 주소의 컨피그레이션을 수행해야 합니다. 그러나 물리적 특성(예: 인터페이스 활성화)은 ASA에서 구성됩니다.

예

다음 예에서는 단일 모드에서 물리적 인터페이스의 매개변수를 구성합니다.

```
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
```

다음 예에서는 단일 모드에서 하위 인터페이스의 매개변수를 구성합니다.

```
ciscoasa(config)# interface gigabitethernet0/1.1
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 다중 컨텍스트 모드에서 시스템 컨피그레이션에 대한 인터페이스 매개변수를 구성하고, gigabitethernet 0/1.1 하위 인터페이스를 contextA에 할당합니다.

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# no shutdown
ciscoasa(config-subif)# context contextA
ciscoasa(config-ctx)# ...
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
```

다음 예에서는 다중 컨텍스트 모드에서 컨텍스트 컨피그레이션을 위한 매개변수를 구성합니다.

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# no shutdown
```

관련 명령

명령	설명
allocate-interface	보안 컨텍스트에 인터페이스 및 하위 인터페이스를 할당합니다.
member-interface	이중화 인터페이스에 인터페이스를 할당합니다.
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
vlan	하위 인터페이스에 VLAN을 할당합니다.

interface bvi

브리지 그룹에 대해 BVI(Bridge Virtual Interface)를 구성하려면 글로벌 컨피그레이션 모드에서 **interface bvi** 명령을 사용합니다. BVI 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

interface bvi *bridge_group_number*

no interface bvi *bridge_group_number*

구문 설명

bridge_group_number	브리지 그룹 수를 1~100 범위의 정수로 지정합니다. 9.3(1) 이상의 경우 범위가 1~250으로 증가합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.
9.3(1)	BVI 250개를 지원하도록 범위가 1~250으로 증가되었습니다.

사용 지침

브리지 그룹에 대한 관리 IP 주소를 구성하기 위해 인터페이스 컨피그레이션 모드로 들어가려면 이 명령을 사용합니다. 보안 컨텍스트의 오버헤드를 원치 않을 경우 또는 보안 컨텍스트 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브릿지 그룹 트래픽은 다른 브릿지 그룹과 분리됩니다. 트래픽은 ASA 내의 다른 브릿지 그룹으로 라우팅되지 않으며, 트래픽은 외부 라우터에 의해 ASA의 다른 브릿지 그룹으로 다시 라우팅되기 전에 ASA에서 나가야 합니다. 브리지 기능은 브리지 그룹마다 따로 있지만, 다른 여러 기능은 모든 브리지 그룹이 공유합니다. 예를 들어, 모든 브리지 그룹은 syslog 서버 또는 AAA 서버 컨피그레이션을 공유합니다. 완전한 보안 정책 분리를 위해서는 각 컨텍스트에서 한 브리지 그룹의 보안 컨텍스트를 사용합니다. 상황마다 또는 단일 모드에서 하나 이상의 브리지 그룹이 필요합니다.

각 브리지 그룹에는 관리 IP 주소가 필요합니다. ASA에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. 관리 IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. IPv4 트래픽의 경우 트래픽을 전달하려면 관리 IP 인터페이스가 필요합니다. IPv6 트래픽에서는 적어도 트래픽을 전달하기 위해서는 링크-로컬 주소를 구성해야 합니다. 그러나 원격 관리, 기타 관리 작업을 포함한 전체 기능에 하나의 전역 관리 주소를 사용하는 것이 좋습니다. 또 다른 관리 방법으로, 브리지 그룹과는 별도의 관리 인터페이스를 구성할 수 있습니다.

9.2 이상에서는 단일 모드에서 ?또는 다중 모드의 컨텍스트당 최대 8개의 브리지 그룹을 구성할 수 있습니다. 9.3(1) 이상에서는 최대 250개의 그룹을 구성할 수 있습니다. 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다. 동일한 인터페이스를 둘 이상의 브리지 그룹에 지정할 수 없습니다. 하나 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.

참고 ASA 5505에서 여러 개의 브릿지 그룹을 구성할 수는 있으나, ASA 5505의 투명 모드에서 데이터 인터페이스가 2개로 제한된다는 것은 실제로 사용 가능한 브릿지 그룹은 1개라는 의미입니다.

참고 별도의 관리 인터페이스에서는 컨피그레이션이 불가능한 브리지 그룹(ID 301)이 자동으로 컨피그레이션에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.

참고 ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

예 다음 예에서는 각각 3개의 인터페이스로 구성된 2개의 브리지 그룹과 관리 전용 인터페이스가 있습니다.

```
interface gigabitethernet 0/0
    nameif inside
    security-level 100
    bridge-group 1
    no shutdown
interface gigabitethernet 0/1
    nameif outside
    security-level 0
    bridge-group 1
    no shutdown
interface gigabitethernet 0/2
    nameif dmz
    security-level 50
    bridge-group 1
    no shutdown
interface bvi 1
    ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
    nameif inside
    security-level 100
    bridge-group 2
    no shutdown
interface gigabitethernet 1/1
    nameif outside
    security-level 0
    bridge-group 2
    no shutdown
interface gigabitethernet 1/2
    nameif dmz
    security-level 50
    bridge-group 2
    no shutdown
interface bvi 2
    ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
```

```
interface management 0/0
    nameif mgmt
    security-level 100
    ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
    no shutdown
```

관련 명령

명령	설명
ace/bvi	브리지 가상 인터페이스 컨피그레이션을 지웁니다.
bridge-group	투명 방화벽 인터페이스를 브리지 그룹으로 그룹화합니다.
interface	인터페이스를 구성합니다.
ip address	브리지 그룹의 관리 IP 주소를 설정합니다.
show bridge-group	멤버 인터페이스와 IP 주소를 비롯한 브리지 그룹 정보를 표시합니다.
show running-config interface bvi	브리지 그룹 인터페이스 컨피그레이션을 표시합니다.

interface port-channel

EtherChannel 인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **interface port-channel** 명령을 사용합니다. EtherChannel 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

interface port-channel *number*

no interface port-channel *number*

구문 설명

number	EtherChannel 채널 그룹 ID를 1~48 범위로 지정합니다. 이 인터페이스는 채널 그룹에 인터페이스를 추가할 경우 자동으로 생성된 것입니다. 인터페이스를 아직 추가하지 않은 경우 이 명령을 사용하면 포트 채널 인터페이스가 생성됩니다. **참고** 논리적 매개변수(예: 이름)를 구성하기 전에 하나 이상의 멤버 인터페이스를 포트-채널 인터페이스에 추가해야 합니다.

기본값

기본적으로 포트 채널 인터페이스는 활성화되어 있습니다. 그러나 EtherChannel을 통해 트래픽을 전달하려면 채널 그룹 물리적 인터페이스도 활성화되어야 합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스 컨피그레이션 모드에서는 이름과 IP 주소를 할당하고 다른 여러 설정을 구성할 수 있습니다.

활성화된 인터페이스가 트래픽을 통과하도록 하려면 **nameif** 및 **ip address**(라우팅된 모드의 경우) 인터페이스 컨피그레이션 모드 명령을 구성합니다.

인터페이스 설정을 변경한 경우, 기존 연결이 시간 초과될 때까지 기다리지 않고 새 보안 정보를 사용하려면 **clear local-host** 명령을 사용하여 연결을 해제합니다.

참고 ASA 5505 또는 ASASM에서는 이 명령이 지원되지 않습니다. 4GE SSM(ASA 5550 슬롯 1의 통합 4GE SSM 포함)에서는 EtherChannel의 일부로서 인터페이스를 사용할 수 없습니다.

인터페이스에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

예

다음 예에서는 세 가지 인터페이스를 EtherChannel의 일부로 구성합니다. 또한 시스템 우선순위를 더 높은 우선순위로 설정하고, EtherChannel에 8개 이상의 인터페이스가 할당된 경우 GigabitEthernet 0/2의 우선순위를 다른 인터페이스보다 높게 설정합니다.

```
ciscoasa(config)# lacp system-priority 1234
ciscoasa(config-if)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode passive
ciscoasa(config-if)# interface Port-channel1
ciscoasa(config-if)# lacp max-bundle 4
ciscoasa(config-if)# port-channel min-bundle 2
ciscoasa(config-if)# port-channel load-balance dst-ip
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
lacp max-bundle	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 지정합니다.
lacp port-priority	채널 그룹에서 물리적 인터페이스의 우선순위를 설정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel load-balance	로드 밸런싱 알고리즘을 구성합니다.
port-channel min-bundle	포트 채널 인터페이스를 액티브 상태로 설정하는 데 필요한 액티브 인터페이스의 최소 개수를 지정합니다.
show lacp	트래픽 통계, 시스템 식별자, 인접 디바이스 세부사항 같은 LACP 정보가 표시됩니다.
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령을 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel load-balance	정해진 매개변수 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

interface redundant

이중화 인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **interface redundant** 명령을 사용합니다. 이중화 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

interface redundant *number*

no interface redundant *number*

구문 설명

number	논리적 이중화 인터페이스 ID를 1~8 범위로 지정합니다. **redundant**와 ID 사이의 공백은 선택 사항입니다.

기본값

기본적으로 이중화 인터페이스는 활성화되어 있습니다. 그러나 이중화 인터페이스를 통해 트래픽을 전달하려면 멤버 물리적 인터페이스도 활성화되어야 합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

이중화 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다 (**member-interface** 명령 참조). 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다.

모든 ASA 컨피그레이션에서는 멤버 물리적 인터페이스 대신 논리적 이중화 인터페이스를 참조합니다.

인터페이스 컨피그레이션 모드에서는 이름과 IP 주소를 할당하고 다른 여러 설정을 구성할 수 있습니다.

활성화된 인터페이스가 트래픽을 통과하도록 하려면 **nameif** 및 **ip address**(라우팅된 모드의 경우) 인터페이스 컨피그레이션 모드 명령을 구성합니다.

인터페이스 설정을 변경한 경우, 기존 연결이 시간 초과될 때까지 기다리지 않고 새 보안 정보를 사용하려면 **clear local-host** 명령을 사용하여 연결을 해제합니다.

참고 ASA 5505 또는 ASASM에서는 이 명령이 지원되지 않습니다.

인터페이스에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

예

다음 예에서는 2개의 이중화 인터페이스를 생성합니다.

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

관련 명령

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
debug redundant-interface	이중화 인터페이스 이벤트 또는 오류와 관련된 디버그 메시지를 표시합니다.
member-interface	이중화 인터페이스에 물리적 인터페이스를 할당합니다.
redundant-interface	액티브 멤버 인터페이스를 변경합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

interface vlan

ASA 5505 및 ASASM의 경우 VLAN 인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **interface vlan** 명령을 사용합니다. VLAN 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

interface vlan *number*

no interface vlan *number*

구문 설명

number	VLAN ID를 지정합니다. ASA 5505의 경우 1~4090 범위의 ID를 사용합니다. VLAN 인터페이스 ID는 기본적으로 VLAN 1에서 활성화되어 있습니다. ASASM의 경우 2~1000 및 1025~4094의 ID를 사용합니다.

기본값

기본적으로 VLAN 인터페이스는 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.4(1)M	ASASM 지원이 추가되었습니다.

사용 지침

ASASM의 경우 어떤 VLAN ID도 컨피그레이션에 추가할 수 있으나, 스위치에 의해 ASA에 지정된 VLAN만 트래픽을 전달할 수 있습니다. ASA에 지정된 모든 VLAN을 보려면 **show vlan** 명령을 사용합니다. 아직 스위치에 의해 ASA에 지정되지 않은 VLAN을 위해 인터페이스를 추가할 경우 그 인터페이스는 중지(down) 상태가 됩니다. VLAN을 ASA에 지정하면 인터페이스는 작동(up) 상태로 바뀝니다. 인터페이스 상태에 대한 자세한 내용은 **show interface** 명령을 참조하십시오.

인터페이스 컨피그레이션 모드에서는 이름과 IP 주소를 할당하고 다른 여러 설정을 구성할 수 있습니다.

활성화된 인터페이스가 트래픽을 통과하도록 하려면 **nameif** 및 **ip address**(라우팅된 모드의 경우) 인터페이스 컨피그레이션 모드 명령을 구성합니다. ASA 5505 스위치 물리적 인터페이스의 경우 **switchport access vlan** 명령을 사용하여 VLAN 인터페이스에 물리적 인터페이스를 할당합니다.

인터페이스 설정을 변경한 경우, 기존 연결이 시간 초과될 때까지 기다리지 않고 새 보안 정보를 사용하려면 **clear local-host** 명령을 사용하여 연결을 해제합니다.

인터페이스에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

예

다음 예는 세 개의 VLAN 인터페이스를 구성합니다. 세 번째 home 인터페이스는 work 인터페이스로 트래픽을 전달할 수 없습니다.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
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 vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

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
```

다음 예는 다섯 개의 VLAN 인터페이스를 구성합니다. 그중 failover 인터페이스는 **failover lan** 명령을 사용해 별도로 구성합니다.

```
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 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 access vlan 200
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
allocate-interface	보안 컨텍스트에 인터페이스 및 하위 인터페이스를 할당합니다.
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

interface (vpn load-balancing)

VPN 로드 밸런싱 가상 클러스터에서 VPN 로드 밸런싱에 대해 기본이 아닌 공개 또는 비공개 인터페이스를 지정하려면 vpn 로드 밸런싱 모드에서 **interface** 명령을 사용합니다. 인터페이스 사양을 제거하고 기본 인터페이스로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

interface {**lbprivate** | **lbpublic**} *interface-name*

no interface {**lbprivate** | **lbpublic**}

구문 설명

interface-name	VPN 로드 밸런싱 클러스터에 대해 공개 또는 비공개 인터페이스로서 구성할 인터페이스의 이름.
lbprivate	이 명령으로 VPN 로드 밸런싱에 대해 비공개 인터페이스를 구성함을 지정합니다.
lbpublic	이 명령으로 VPN 로드 밸런싱에 대해 공개 인터페이스를 구성함을 지정합니다.

기본값

nterface 명령을 생략하면 **lbprivate** 인터페이스는 기본적으로 **inside**, **lbpublic** 인터페이스는 기본적으로 **outside**로 설정됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
vpn 로드 밸런싱	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

먼저 **vpn load-balancing** 명령을 사용해야 vpn 로드 밸런싱 컨피그레이션 모드로 들어갈 수 있습니다.

이 명령으로 지정하는 인터페이스를 구성하고 이름을 할당하려면 사전에 **interface**, **ip address** 및 **nameif** 명령을 사용해야 합니다.

예

다음은 클러스터의 공개 인터페이스를 "test"로 지정하고 클러스터의 비공개 인터페이스를 기본값(inside)으로 되돌리는 **interface** 명령을 포함하는 **vpn load-balancing** 명령 시퀀스의 예입니다.

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# no interface lbprivate
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
vpn load-balancing	VPN 로드 밸런싱 컨피그레이션 모드로 들어갑니다.

interface-policy

모니터링을 통해 인터페이스 장애가 감지되는 경우 장애 조치를 위한 정책을 지정하려면 장애 조치 그룹 컨피그레이션 모드에서 **interface-policy** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

구문 설명

num	백분율로 사용할 경우 1~100의 숫자를 지정하거나, 1부터 인터페이스 최대 수 사이의 숫자를 지정합니다.
%	(선택 사항) 숫자 *num*이 모니터링하는 인터페이스의 백분율임을 지정합니다.

기본값

유닛에 대해 **failover interface-policy** 명령을 구성한 경우 **interface-policy failover group** 명령의 기본값은 해당 값을 가정합니다. 그렇지 않은 경우 *num*은 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
장애 조치 그룹 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

num 인수와 선택적인 **%** 키워드 간에 공백이 없습니다.

장애가 발생한 인터페이스의 수가 구성된 정책과 일치하고 다른 ASA가 올바르게 작동하면, ASA는 스스로를 장애 상태로 표시하며 장애 조치가 발생할 수 있습니다(장애가 발생한 ASA가 액티브 상태인 경우). **monitor-interface** 명령으로 모니터링하도록 지정된 인터페이스만 정책을 기준으로 계산됩니다.

예

다음의 부분적인 예는 장애 조치 그룹에 대해 가능한 컨피그레이션을 보여줍니다.

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# interface-policy 25%
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
failover group	액티브/액티브 장애 조치에 대한 장애 조치 그룹을 정의합니다.
failover interface-policy	인터페이스 모니터링 정책을 구성합니다.
monitor-interface	장애 조치를 모니터링할 인터페이스를 지정합니다.

internal-password

클라이언트리스 SSL VPN 포털 페이지에서 추가 비밀번호 필드를 표시하려면 webvpn 컨피그레이션 모드에서 **internal-password** 명령을 사용합니다. 이 추가 비밀번호는 파일 서버에서 SSO가 허용되는 사용자를 인증하기 위해 ASA에서 사용합니다.

내부 비밀번호 사용 기능을 비활성화하려면 명령의 **no** 버전을 사용합니다.

internal-password enable

no internal password

구문 설명

enable	내부 비밀번호의 사용을 활성화합니다.

기본값

기본값은 disabled입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

활성화되면, 최종 사용자는 클라이언트리스 SSL VPN 세션에 로그인할 때 두 번째 비밀번호를 입력합니다. 클라이언트리스 SSL VPN 서버는 HTTPS를 사용하는 인증 서버에 SSO 인증 요청(사용자 이름 및 비밀번호 포함)을 전송합니다. 인증 서버는 인증 요청을 승인하는 경우 클라이언트리스 SSL VPN 서버에 SSO 인증 쿠키를 반환합니다. 이 쿠키는 사용자를 대신하여 ASA에 저장되며, SSO 서버로 보호되는 도메인 내의 안전한 웹사이트에 대해 사용자를 인증하는 데 사용됩니다.

내부 비밀번호 기능은 내부 비밀번호를 SSL VPN 비밀번호와 다르게 유지하려는 경우 유용합니다. 특히, ASA에 대한 인증에는 일회용 비밀번호를 사용하고 내부 사이트에는 또 다른 비밀번호를 사용할 수 있습니다.

예

다음 예는 내부 비밀번호를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# internal password enable
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
webvpn	클라이언트리스 SSL VPN 연결을 위해 특성을 구성할 수 있는 webvpn 컨피그레이션 모드로 들어갑니다.

interval maximum

DDNS 업데이트 메서드에 의한 업데이트 시도 간에 최대 간격을 구성하려면 DDNS-update-method 모드에서 **interval** 명령을 사용합니다. 실행 중인 컨피그레이션에서 DDNS 업데이트 메서드에 대한 간격을 제거하려면 이 명령의 **no** 형식을 사용합니다.

interval maximum *days hours minutes seconds*

no interval maximum *days hours minutes seconds*

구문 설명

days	업데이트 시도 간격의 일수를 0~364 범위로 지정합니다.
hours	업데이트 시도 간격의 시간(시간)을 0~23 범위로 지정합니다.
minutes	업데이트 시도 간격의 시간(분)을 0~59 범위로 지정합니다.
seconds	업데이트 시도 간격의 시간(초)을 0~59 범위로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ddns-update-method 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

일수, 시간, 분, 초를 모두 합산하여 총 간격이 산출됩니다.

예

다음 예는 3분 15초마다 업데이트를 시도하는 ddns-2라는 메서드를 구성합니다.

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# interval maximum 0 0 3 15
```

관련 명령

명령	설명
ddns	생성된 DDNS 메서드에 대해 DDNS 업데이트 메서드 유형을 지정합니다.
ddns update	DDNS 업데이트 메서드를 ASA 인터페이스 또는 DDNS 업데이트 호스트 이름과 연결합니다.
ddns update method	DNS 리소스 레코드의 동적 업데이트를 위한 메서드를 생성합니다.
dhcp-client update dns	DHCP 클라이언트에서 DHCP 서버에 전달할 업데이트 매개변수를 구성합니다.
dhcpd update dns	DHCP 서버에서 DDNS 업데이트를 수행하도록 지정합니다.

invalid-ack

잘못된 ACK가 포함된 패킷에 대한 작업을 설정하려면 tcp-map 컨피그레이션 모드에서 **invalid-ack** 명령을 사용합니다. 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 **set connection advanced-options** 명령을 사용하여 활성화되는 TCP 정규화 정책의 일부입니다.

invalid-ack {**allow** | **drop**}

no invalid-ack

구문 설명

allow	유효하지 않은 ACK가 포함된 패킷을 허용합니다.
drop	유효하지 않은 ACK가 포함된 패킷을 삭제합니다.

기본값

기본 작업은 잘못된 ACK가 포함된 패킷을 삭제하는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(4)/8.0(4)	이 명령이 추가되었습니다.

사용 지침

TCP 정규화를 활성화하려면 Modular Policy Framework를 사용하십시오.

1. **tcp-map** - TCP 정규화 작업을 식별합니다.
   a. **invalid-ack** - tcp-map 컨피그레이션 모드에서는 **invalid-ack** 명령 및 기타 많은 명령을 입력할 수 있습니다.
2. **class-map** - TCP 정규화를 수행할 트래픽을 식별합니다.
3. **policy-map** - 각 클래스 맵과 관련된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **set connection advanced-options** - 생성한 TCP 맵을 식별합니다.
4. **service-policy** - 정책 맵을 한 인터페이스에 또는 전체적으로 할당합니다.

유효하지 않은 ACK의 예는 다음과 같습니다.

- TCP 연결 SYN-ACK-received 상태에서 수신된 TCP 패킷의 ACK 번호가 다음번 전송 TCP 패킷의 시퀀스 번호와 정확히 같지 않으면 유효하지 않은 ACK입니다.
- 수신된 TCP 패킷의 ACK 번호가 다음번 전송 TCP 패킷의 시퀀스 번호보다 크면 유효하지 않은 ACK입니다.

참고 유효하지 않은 ACK가 포함된 TCP 패킷은 WAAS 연결에서 자동으로 허용됩니다.

예

다음 예는 잘못된 ACK가 포함된 패킷을 허용하도록 ASA를 설정합니다.

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# invalid-ack 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 정책에 대한 트래픽을 식별합니다.
policy-map	서비스 정책에서 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.

ip address

인터페이스(라우팅된 모드)에 대한 IP 주소 또는 BVI(Bridge Virtual Interface)나 관리 인터페이스(투명 모드)에 대한 IP 주소를 설정하려면 인터페이스 컨피그레이션 모드에서 **ip address** 명령을 사용합니다. IP 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ip address *ip_address* [*mask*] [**standby** *ip_address* | **cluster-pool** *poolname*]

no ip address [*ip_address*]

구문 설명

cluster-pool *poolname*	(선택 사항) ASA 클러스터링의 경우 **ip local pool** 명령으로 정의된 주소의 클러스터 풀을 설정합니다. *ip_address* 인수로 정의한 기본 클러스터 IP 주소는 현재 마스터 유닛에만 속합니다. 각 클러스터 멤버는 이 풀에서 로컬 IP 주소를 수신합니다. 각 유닛에 정확히 어떤 주소가 할당되는지 미리 확인할 수는 없습니다. 각 유닛에 사용된 주소를 보려면 **show ip local pool** *poolname* 명령을 입력합니다. 각 클러스터 멤버는 클러스터에 참가할 때 멤버 ID가 할당됩니다. ID는 풀에서 사용되는 로컬 IP를 결정합니다.
ip_address	인터페이스에 대한 IP 주소.
mask	(선택 사항) IP 주소의 서브넷 마스크. 마스크를 설정하지 않으면 ASA는 IP 주소 클래스에 대한 기본 마스크를 사용합니다.
standby *ip_address*	(선택 사항) 장애 조치의 경우 스탠바이 유닛에 대한 IP 주소를 설정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	라우팅된 모드의 경우, 이 명령은 글로벌 컨피그레이션 명령에서 인터페이스 컨피그레이션 모드 명령으로 변경되었습니다.
8.4(1)	투명 모드의 경우, 브리지 그룹이 추가되었습니다. 이제 전체가 아니라 BVI에 대해 IP 주소를 설정할 수 있습니다.
9.0(1)	ASA 클러스터링을 지원하도록 **cluster-pool** 키워드가 추가되었습니다.

사용 지침

이 명령은 또한 장애 조치용 스탠바이 주소를 설정합니다.

다중 컨텍스트 모드 지침

단일 컨텍스트 라우팅된 방화벽 모드에서 각 인터페이스 주소는 고유한 서브넷에 있어야 합니다. 다중 컨텍스트 모드에서 이 인터페이스가 공유 인터페이스에 있는 경우, 각 IP 주소는 고유해야 하지만 동일한 서브넷에 있어야 합니다. 인터페이스가 고유하면 원하는 경우 이 IP 주소를 다른 컨텍스트에서 사용할 수 있습니다.

투명 방화벽 지침

투명 방화벽은 IP 라우팅에 참여하지 않습니다. ASA에 필요한 유일한 IP 컨피그레이션은 BVI 주소를 설정하는 것입니다. ASA는 이 주소를 ASA에서 시작되는 트래픽(예: 시스템 메시지 또는 AAA 서버와의 통신)에 대한 소스 주소로 사용하기 때문에 이 주소가 필요합니다. 원격 관리 액세스에도 이 주소를 사용할 수 있습니다. 이 주소는 업스트림 및 다운스트림 라우터와 동일한 서브넷에 있어야 합니다. 다중 컨텍스트 모드의 경우, 각 컨텍스트 내에 관리 IP 주소를 설정합니다. 관리 인터페이스를 포함하는 모델의 경우 관리 목적으로 이 인터페이스에 대한 IP 주소를 설정할 수도 있습니다.

장애 조치 지침

스탠바이 IP 주소는 기본 IP 주소와 동일한 서브넷에 있어야 합니다.

ASA 클러스터링 지침

클러스터 인터페이스 모드를 individual로 구성한 후에야 개별 인터페이스에 대해 클러스터 풀을 설정할 수 있습니다(**cluster-interface mode individual** 명령). 관리 전용 인터페이스에 대한 유일한 예외는 다음과 같습니다.

- 관리 전용 인터페이스는 항상 개별 인터페이스로 구성할 수 있으며, Spanned EtherChannel 모드에서도 마찬가지입니다. 투명 방화벽 모드에서도 관리 인터페이스는 개별 인터페이스가 될 수 있습니다.
- Spanned EtherChannel 모드에서 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 경로를 사용해야 합니다.

예

다음 예는 두 인터페이스의 IP 주소 및 스탠바이 주소를 설정합니다.

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/3
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
ciscoasa(config-if)# no shutdown
```

다음 예에서는 브리지 그룹 1의 관리 주소와 대기 주소를 설정합니다.

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어갑니다.
ip address dhcp	DHCP 서버에서 IP 주소를 얻기 위해 인터페이스를 설정합니다.
show ip address	인터페이스에 할당된 IP 주소를 보여줍니다.

ip address dhcp

DHCP를 사용하여 인터페이스에 대한 IP 주소를 가져오려면 인터페이스 컨피그레이션 모드에서 **ip address dhcp** 명령을 사용합니다. 이 인터페이스에 대해 DHCP 클라이언트를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ip address dhcp [**setroute**]

no ip address dhcp

구문 설명

setroute	(선택 사항) ASA에서 DHCP 서버가 제공한 기본 경로를 사용할 수 있게 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 글로벌 컨피그레이션 명령에서 인터페이스 컨피그레이션 모드 명령으로 변경되었습니다. 외부 인터페이스만이 아니라 어떤 인터페이스에서든 이 명령을 활성화할 수 있습니다.

사용 지침

DHCP 임대를 재설정하고 새 임대를 요청하려면 이 명령을 다시 입력합니다.

ip address dhcp 명령을 입력하기 전에 **no shutdown** 명령을 사용하여 인터페이스를 활성화하지 않은 경우 일부 DHCP 요청이 전송되지 않을 수 있습니다.

참고 ASA는 시간 제한이 32초 미만인 임대를 거부합니다.

예

다음 예는 Gigabitethernet0/1 인터페이스에서 DHCP를 활성화합니다.

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address dhcp
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어갑니다.
ip address	인터페이스에 대한 IP 주소를 설정하거나, 투명 방화벽에 대한 관리 IP 주소를 설정합니다.
show ip address dhcp	DHCP 서버에서 얻은 IP 주소를 보여줍니다.

ip address pppoe

PPPoE를 활성화하려면 인터페이스 컨피그레이션 모드에서 **ip address pppoe** 명령을 사용합니다. PPPoE를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ip address [*ip_address* [*mask*]] **pppoe** [**setroute**]

no ip address [*ip_address* [*mask*]] **pppoe**

구문 설명

ip_address	PPPoE 서버에서 주소를 수신하는 대신 IP 주소를 수동으로 설정합니다.
mask	IP 주소의 네트워크 마스크를 지정합니다. 마스크를 설정하지 않으면 ASA는 IP 주소 클래스에 대한 기본 마스크를 사용합니다.
setroute	ASA에서 PPPoE 서버가 제공한 기본 경로를 사용할 수 있게 합니다. PPPoE 서버가 기본 경로를 전송하지 않으면 ASA는 게이트웨이로서 Access Concentrator의 주소로 기본 경로를 생성합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

PPPoE는 널리 사용되는 두 가지 표준인 이더넷과 PPP를 결합하여, 클라이언트 시스템에 IP 주소를 할당하는 인증된 방법을 제공합니다. ISP는 PPPoE를 구축하는데, 그 이유는 기존 원격 액세스 인프라를 사용하여 고속 광대역 액세스를 지원하며 고객이 사용하기에 더 쉽기 때문입니다.

PPPoE를 사용하여 IP 주소를 설정하려면 먼저 사용자 이름, 비밀번호 및 인증 프로토콜 설정을 위해 **vpdn** 명령을 구성해야 합니다. 둘 이상의 인터페이스(예: ISP에 대한 백업 링크용)에서 이 명령을 활성화하면, **pppoe client vpdn group** 명령을 사용해야 하는 경우 각 인터페이스를 서로 다른 VPDN 그룹에 할당할 수 있습니다.

MTU(maximum transmission unit) 크기는 이더넷 프레임 내에서 PPPoE 전송을 허용하기에 올바른 값인 1492바이트로 자동 설정됩니다.

PPPoE 세션을 재설정 및 다시 시작하려면 이 명령을 다시 입력합니다.

이 명령은 **ip address** 명령 또는 **ip address dhcp** 명령과 동시에 설정할 수 없습니다.

예

다음 예는 Gigabitethernet 0/1 인터페이스에서 PPPoE를 활성화합니다.

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address pppoe
ciscoasa(config-if)# no shutdown
```

다음 예는 PPPoE 인터페이스의 IP 주소를 수동으로 설정합니다.

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

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어갑니다.
ip address	인터페이스에 대한 IP 주소를 설정합니다.
pppoe client vpdn group	특정 VPDN 그룹에 이 인터페이스를 할당합니다.
show ip address pppoe	PPPoE 서버에서 얻은 IP 주소를 보여줍니다.
vpdn group	vpdn 그룹을 생성하고 PPPoE 클라이언트 설정을 구성합니다.

ip-address-privacy

IP 주소 비공개를 활성화하려면 매개변수 컨피그레이션 모드에서 **ip-address-privacy** 명령을 사용합니다. 매개변수 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ip-address-privacy

no ip-address-privacy

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 SIP 검사 정책 맵에서 SIP를 통해 IP 주소 비공개를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ip-address-privacy
```

관련 명령

명령	설명
policy-map type inspect	검사 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

ip audit attack

공격 시그니처를 확인하는 패킷에 대한 기본 작업을 설정하려면 글로벌 컨피그레이션 모드에서 **ip audit attack** 명령을 사용합니다. 기본 작업(연결 재설정)을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

구문 설명

action	(선택 사항) 기본 작업 집합을 정의하도록 지정합니다. 이 키워드 뒤에 작업을 지정하지 않으면 ASA는 작업을 수행하지 않습니다. **action** 키워드를 입력하지 않으면 ASA는 사용자가 입력한 것으로 간주하며, 컨피그레이션에 **action** 키워드가 나타납니다.
alarm	(기본값) 패킷이 시그니처와 일치함을 보여주는 시스템 메시지를 생성합니다.
drop	(선택 사항) 패킷을 삭제합니다.
reset	(선택 사항) 패킷을 삭제하고 연결을 닫습니다.

기본값

기본 작업은 경보(alarm) 전송입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

여러 작업을 지정할 수도 있고, 작업을 지정하지 않을 수도 있습니다. **ip audit name** 명령을 사용하여 감사 정책을 구성할 때 이 명령으로 설정한 작업을 재지정할 수 있습니다. **ip audit name** 명령으로 작업을 지정하지 않으면 이 명령으로 지정한 작업이 사용됩니다.

시그니처 목록은 **ip audit signature** 명령을 참조하십시오.

예

다음 예는 공격 시그니처와 일치하는 패킷에 대해 기본 작업을 alarm 및 reset으로 설정합니다. 내부 인터페이스에 대한 감사 정책은 이 기본값을 alarm만으로 재지정하는 반면, 외부 인터페이스에 대한 정책은 **ip audit attack** 명령으로 설정된 기본값을 사용합니다.

```
ciscoasa(config)# ip audit attack action alarm reset
ciscoasa(config)# ip audit name insidepolicy attack action alarm
ciscoasa(config)# ip audit name outsidepolicy attack
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

관련 명령

명령	설명
ip audit info	정보 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit interface	인터페이스에 감사 정책을 할당합니다.
ip audit name	패킷이 공격 시그니처 또는 정보 시그니처와 일치하는 경우 수행해야 할 작업을 식별하는 명명된 감사 정책을 생성합니다.
ip audit signature	시그니처를 비활성화합니다.
show running-config ip audit attack	**ip audit attack** 명령에 대한 컨피그레이션을 보여줍니다.

ip audit info

정보 시그니처를 확인하는 패킷에 대한 기본 작업을 설정하려면 글로벌 컨피그레이션 모드에서 **ip audit info** 명령을 사용합니다. 기본 작업(alarm 생성)을 복원하려면 이 명령의 **no** 형식을 사용합니다. 여러 작업을 지정할 수도 있고, 작업을 지정하지 않을 수도 있습니다.

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

구문 설명

action	(선택 사항) 기본 작업 집합을 정의하도록 지정합니다. 이 키워드 뒤에 작업을 지정하지 않으면 ASA는 작업을 수행하지 않습니다. **action** 키워드를 입력하지 않으면 ASA는 사용자가 입력한 것으로 간주하며, 컨피그레이션에 **action** 키워드가 나타납니다.
alarm	(기본값) 패킷이 시그니처와 일치함을 보여주는 시스템 메시지를 생성합니다.
drop	(선택 사항) 패킷을 삭제합니다.
reset	(선택 사항) 패킷을 삭제하고 연결을 닫습니다.

기본값

기본 작업은 경보(alarm) 생성입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ip audit name 명령을 사용하여 감사 정책을 구성할 때 이 명령으로 설정한 작업을 재지정할 수 있습니다. **ip audit name** 명령으로 작업을 지정하지 않으면 이 명령으로 지정한 작업이 사용됩니다.

시그니처 목록은 **ip audit signature** 명령을 참조하십시오.

예

다음 예는 정보 시그니처와 일치하는 패킷에 대해 기본 작업을 alarm 및 reset으로 설정합니다. 내부 인터페이스에 대한 감사 정책은 이 기본값을 alarm 및 drop으로 재지정하는 반면, 외부 인터페이스에 대한 정책은 **ip audit info** 명령으로 설정된 기본값을 사용합니다.

```
ciscoasa(config)# ip audit info action alarm reset
ciscoasa(config)# ip audit name insidepolicy info action alarm drop
ciscoasa(config)# ip audit name outsidepolicy info
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

관련 명령

명령	설명
ip audit attack	공격 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit interface	인터페이스에 감사 정책을 할당합니다.
ip audit name	패킷이 공격 시그니처 또는 정보 시그니처와 일치하는 경우 수행해야 할 작업을 식별하는 명명된 감사 정책을 생성합니다.
ip audit signature	시그니처를 비활성화합니다.
show running-config ip audit info	**ip audit info** 명령에 대한 컨피그레이션을 보여줍니다.

ip audit interface

인터페이스에 감사 정책을 할당하려면 글로벌 컨피그레이션 모드에서 **ip audit interface** 명령을 사용합니다. 인터페이스에서 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

구문 설명

interface_name	인터페이스 이름을 지정합니다.
policy_name	**ip audit name** 명령으로 추가한 정책의 이름. 각 인터페이스에 정보 정책 및 공격 정책을 할당할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 내부 및 외부 인터페이스에 감사 정책을 적용합니다.

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

관련 명령

명령	설명
ip audit attack	공격 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit info	정보 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit name	패킷이 공격 시그니처 또는 정보 시그니처와 일치하는 경우 수행해야 할 작업을 식별하는 명명된 감사 정책을 생성합니다.
ip audit signature	시그니처를 비활성화합니다.
show running-config ip audit interface	**ip audit interface** 명령에 대한 컨피그레이션을 보여줍니다.

ip audit name

패킷이 미리 정의된 공격 시그니처 또는 정보 시그니처와 일치하는 경우 수행할 작업을 지정하는 명명된 감사 정책을 만들려면 글로벌 컨피그레이션 모드에서 **ip audit name** 명령을 사용합니다. 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

구문 설명

action	(선택 사항) 작업 집합을 정의하도록 지정합니다. 이 키워드 뒤에 작업을 지정하지 않으면 ASA는 작업을 수행하지 않습니다. **action** 키워드를 입력하지 않으면 ASA는 **ip audit attack** 및 **ip audit info** 명령으로 설정한 기본 작업을 사용합니다.
alarm	(선택 사항) 패킷이 시그니처와 일치함을 보여주는 시스템 메시지를 생성합니다.
attack	공격 시그니처에 대한 감사 정책을 생성합니다. 패킷은 네트워크에 대한 공격의 일부일 수 있습니다(예: DoS 공격 또는 잘못된 FTP 명령).
drop	(선택 사항) 패킷을 삭제합니다.
info	정보 시그니처에 대한 감사 정책을 생성합니다. 패킷은 현재 네트워크를 공격하고 있지 않지만, 정보 수집 활동의 일부일 수 있습니다(예: 포트 스윕).
name	정책의 이름을 설정합니다.
reset	(선택 사항) 패킷을 삭제하고 연결을 닫습니다.

기본값

ip audit attack 및 **ip audit info** 명령을 사용하여 기본 작업을 변경하지 않는 경우, 공격 시그니처 및 정보 시그니처에 대한 기본 작업은 경보를 생성하는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

시그니처란 알려진 공격 패턴과 일치하는 활동입니다. 예를 들면 DoS 공격과 일치하는 시그니처가 있습니다. 정책을 적용하려면 **ip audit interface** 명령을 사용하여 인터페이스에 할당합니다. 각 인터페이스에 정보 정책 및 공격 정책을 할당할 수 있습니다.

시그니처 목록은 **ip audit signature** 명령을 참조하십시오.

트래픽이 시그니처와 일치하며 트래픽에 대해 작업을 수행하려는 경우 **shun** 명령을 사용하면 문제의 호스트에서 새 연결이 설정되는 것을 차단하고 기존 연결에서 오는 패킷을 허용하지 않을 수 있습니다.

예

다음 예는 공격 및 정보 시그니처에 대한 경보를 생성하기 위해 내부 인터페이스에 대한 감사 정책을 설정합니다. 한편, 외부 인터페이스에 대한 정책은 공격을 위한 연결을 재설정합니다.

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

관련 명령

명령	설명
ip audit attack	공격 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit info	정보 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit interface	인터페이스에 감사 정책을 할당합니다.
ip audit signature	시그니처를 비활성화합니다.
shun	특정 소스 및 수신 주소의 패킷을 차단합니다.

ip audit signature

감사 정책에 대한 시그니처를 비활성화하려면 글로벌 컨피그레이션 모드에서 **ip audit interface** 명령을 사용합니다. 시그니처를 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

구문 설명

disable	시그니처를 비활성화합니다.
signature_number	비활성화할 시그니처 번호를 지정합니다. 지원되는 시그니처 목록은 표 3-1을 참조하십시오.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

정상 트래픽이 계속해서 시그니처와 일치하는 경우 시그니처를 비활성화할 수 있으며, 다량의 경보를 피하기 위해 시그니처를 비활성화하는 위험을 감수할 수 있습니다. 표 3-1은 지원되는 시그니처 및 시스템 메시지 수를 나열합니다.

표 3-1 시그니처 ID 및 시스템 메시지 수

시그니처 ID	메시지 번호	시그니처 제목	시그니처 유형	설명
1000	400000	IP options-Bad Option List	정보	IP 데이터그램 헤더의 IP 옵션 목록이 불완전한 IP 데이터그램 또는 형식이 잘못된 IP 데이터그램을 수신하는 경우 트리거됩니다. IP 옵션 목록에는 다양한 네트워크 관리 또는 디버깅 작업을 수행하는 하나 이상의 옵션이 포함되어 있습니다.
1001	400001	IP options-Record Packet Route	정보	데이터그램에 대한 IP 옵션 목록에 옵션 7(Record Packet Route)이 포함되어 있는 IP 데이터그램을 수신하는 경우 트리거됩니다.

표 3-1 시그니처 ID 및 시스템 메시지 수(계속)

시그니처 ID	메시지 번호	시그니처 제목	시그니처 유형	설명
1002	400002	IP options-Timestamp	정보	데이터그램에 대한 IP 옵션 목록에 옵션 4(Timestamp)가 포함되어 있는 IP 데이터그램을 수신하는 경우 트리거됩니다.
1003	400003	IP options-Security	정보	데이터그램에 대한 IP 옵션 목록에 옵션 2(Security options)가 포함되어 있는 IP 데이터그램을 수신하는 경우 트리거됩니다.
1004	400004	IP options-Loose Source Route	정보	데이터그램에 대한 IP 옵션 목록에 옵션 3(Loose Source Route)이 포함되어 있는 IP 데이터그램을 수신하는 경우 트리거됩니다.
1005	400005	IP options-SATNET ID	정보	데이터그램에 대한 IP 옵션 목록에 옵션 8(SATNET stream identifier)이 포함되어 있는 IP 데이터그램을 수신하는 경우 트리거됩니다.
1006	400006	IP options-Strict Source Route	정보	데이터그램에 대한 IP 옵션 목록에 옵션 2(Strict Source Routing)가 포함되어 있는 IP 데이터그램을 수신하는 경우 트리거됩니다.
1100	400007	IP Fragment Attack	공격	오프셋 필드에 표시된 오프셋 값이 0보다 크고 5보다 작은 IP 데이터그램을 수신하는 경우 트리거됩니다.
1102	400008	IP Impossible Packet	공격	소스 주소와 수신 주소가 동일한 IP 패킷이 도달하는 경우 트리거됩니다. 이 서명은 소위 Land Attack을 캐치합니다.
1103	400009	IP Overlapping Fragments (Teardrop)	공격	동일한 IP 데이터그램 내에 포함된 두 개의 프래그먼트가 데이터그램 내에서 포지셔닝을 공유함을 나타내는 오프셋을 가지고 있는 경우 트리거됩니다. 이는 프래그먼트 B가 프래그먼트 A를 완전히 또는 부분적으로 덮어씀을 의미합니다. 일부 운영 체제는 이와 같이 중첩되는 프래그먼트를 제대로 처리하지 못하고 예외를 표시하거나, 중첩 프래그먼트를 수신할 경우 바람직하지 않은 방식으로 동작할 수 있습니다. Teardrop 공격이 DoS를 생성하는 것이 바로 이런 방식입니다.
2000	400010	ICMP Echo Reply	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 0(Echo Reply)으로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2001	400011	ICMP Host Unreachable	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 3(Host Unreachable)으로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2002	400012	ICMP Source Quench	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 4(Source Quench)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.

표 3-1 시그니처 ID 및 시스템 메시지 수(계속)

시그니처 ID	메시지 번호	시그니처 제목	시그니처 유형	설명
2003	400013	ICMP Redirect	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 5(Redirect)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2004	400014	ICMP Echo Request	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 8(Echo Request)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2005	400015	ICMP Time Exceeded for a Datagram	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 11(Time Exceeded for a Datagram)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2006	400016	ICMP Parameter Problem on Datagram	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 12(Parameter Problem on Datagram)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2007	400017	ICMP Timestamp Request	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 13(Timestamp Request)으로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2008	400018	ICMP Timestamp Reply	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 14(Timestamp Reply)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2009	400019	ICMP Information Request	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 15(Information Request)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2010	400020	ICMP Information Reply	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 16(ICMP Information Reply)으로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2011	400021	ICMP Address Mask Request	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 17(Address Mask Request)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2012	400022	ICMP Address Mask Reply	정보	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 ICMP 헤더의 유형 필드가 18(Address Mask Reply)로 설정된 IP 데이터그램을 수신하는 경우 트리거됩니다.
2150	400023	Fragmented ICMP Traffic	공격	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 더 많은 프래그먼트 플래그가 1(ICMP)로 설정되거나 오프셋 필드에 표시된 오프셋이 있는 IP 데이터그램을 수신하는 경우 트리거됩니다.

표 3-1 시그니처 ID 및 시스템 메시지 수(계속)

시그니처 ID	메시지 번호	시그니처 제목	시그니처 유형	설명
2151	400024	Large ICMP Traffic	공격	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고 IP 길이가 1024보다 큰 IP 데이터그램을 수신하는 경우 트리거됩니다.
2154	400025	Ping of Death Attack	공격	IP 헤더의 프로토콜 필드가 1(ICMP)로 설정되고, Last Fragment 비트가 설정되고, (IP 오프셋 * 8) + (IP 데이터 길이) > 65535, 즉 IP 오프셋(원래 패킷에서 이 프래그먼트의 시작 위치를 나타내며, 8바이트 유닛에 있음)과 패킷의 나머지를 합한 값이 IP 패킷에 대한 최대 크기보다 큰 IP 데이터그램을 수신하는 경우 트리거됩니다.
3040	400026	TCP NULL flags	공격	SYN, FIN, ACK 또는 RST 플래그 중 어떤 것도 설정되지 않은 단일 TCP 패킷이 특정 호스트로 전송된 경우 트리거됩니다.
3041	400027	TCP SYN+FIN flags	공격	SYN 및 FIN 플래그가 있는 단일 TCP 패킷이 설정되어 특정 호스트로 전송되는 경우 트리거됩니다.
3042	400028	TCP FIN only flags	공격	분리된 단일 TCP FIN 패킷이 특정 호스트의 특별 권한 포트(포트 번호 1024 미만)로 전송되는 경우 트리거됩니다.
3153	400029	FTP Improper Address Specified	정보	요청 호스트와 동일하지 않은 주소로 포트 명령이 실행되는 경우 트리거됩니다.
3154	400030	FTP Improper Port Specified	정보	데이터 포트가 <1024 또는 >65535로 지정된 포트 명령이 실행되는 경우 트리거됩니다.
4050	400031	UDP Bomb attack	공격	지정된 UDP 길이가 지정된 IP 길이보다 작은 경우 트리거됩니다. 형식이 잘못된 이 패킷 유형은 서비스 거부 시도와 결합됩니다.
4051	400032	UDP Snork attack	공격	소스 포트가 135, 7 또는 19이고 목적지 포트가 135인 UDP 패킷이 감지되는 경우 트리거됩니다.
4052	400033	UDP Chargen DoS attack	공격	소스 포트가 7이고 목적지 포트가 19인 UDP 패킷이 감지되는 경우 트리거됩니다.
6050	400034	DNS HINFO Request	정보	DNS 서버에서 HINFO 레코드에 액세스하려고 시도하는 경우 트리거됩니다.
6051	400035	DNS Zone Transfer	정보	소스 포트가 53인 일반 DNS 영역 전송 시 트리거됩니다.
6052	400036	DNS Zone Transfer from High Port	정보	소스 포트가 53이 아닌 잘못된 DNS 영역 전송 시 트리거됩니다.
6053	400037	DNS Request for All Records	정보	모든 레코드에 대한 DNS 요청 시 트리거됩니다.
6100	400038	RPC Port Registration	정보	대상 호스트에서 새 RPC 서비스 등록을 시도하는 경우 트리거됩니다.
6101	400039	RPC Port Unregistration	정보	대상 호스트에서 기존 RPC 서비스 등록 취소를 시도하는 경우 트리거됩니다.

표 3-1 시그니처 ID 및 시스템 메시지 수(계속)

시그니처 ID	메시지 번호	시그니처 제목	시그니처 유형	설명
6102	400040	RPC Dump	정보	대상 호스트에 대해 RPC 덤프 요청이 실행되는 경우 트리거됩니다.
6103	400041	Proxied RPC Request	공격	프록시 처리된 RPC 요청이 대상 호스트의 portmapper로 전송되는 경우 트리거됩니다.
6150	400042	ypserv (YP server daemon) Portmap Request	정보	YP server daemon(ypserv) 포트의 portmapper에 대해 요청이 실행되는 경우 트리거됩니다.
6151	400043	ypbind (YP bind daemon) Portmap Request	정보	YP bind daemon(ypbind) 포트의 portmapper에 대해 요청이 실행되는 경우 트리거됩니다.
6152	400044	yppasswdd (YP password daemon) Portmap Request	정보	YP password daemon(ypserv) 포트의 portmapper에 대해 요청이 실행되는 경우 트리거됩니다.
6153	400045	ypupdated (YP update daemon) Portmap Request	정보	YP update daemon(ypupdated) 포트의 portmapper에 대해 요청이 실행되는 경우 트리거됩니다.
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	정보	YP transfer daemon(ypxfrd) 포트의 portmapper에 대해 요청이 실행되는 경우 트리거됩니다.
6155	400047	mountd (mount daemon) Portmap Request	정보	mount daemon(mountd) 포트의 portmapper에 대해 요청이 실행되는 경우 트리거됩니다.
6175	400048	rexd (remote execution daemon) Portmap Request	정보	remote execution daemon(rexd) 포트의 portmapper에 대해 요청이 실행되는 경우 트리거됩니다.
6180	400049	rexd (remote execution daemon) Attempt	정보	rexd 프로그램에 대한 호출이 실행되는 경우 트리거됩니다. remote execution daemon은 원격 프로그램 실행을 담당하는 서버입니다. 이는 시스템 리소스에 대한 무단 액세스를 얻으려는 시도일 수 있습니다.
6190	400050	statd Buffer Overflow	공격	대규모 statd 요청이 전송되는 경우 트리거됩니다. 이는 버퍼를 오버플로하고 시스템 리소스에 대한 액세스를 얻으려는 시도일 수 있습니다.

예 다음 예는 시그니처 6100을 비활성화합니다.

```
ciscoasa(config)# ip audit signature 6100 disable
```

관련 명령

명령	설명
ip audit attack	공격 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit info	정보 시그니처와 일치하는 패킷에 대한 기본 작업을 설정합니다.
ip audit interface	인터페이스에 감사 정책을 할당합니다.
ip audit name	패킷이 공격 시그니처 또는 정보 시그니처와 일치하는 경우 수행해야 할 작업을 식별하는 명명된 감사 정책을 생성합니다.
show running-config ip audit signature	**ip audit signature** 명령에 대한 컨피그레이션을 보여줍니다.

ip-comp

LZS IP 압축을 활성화하려면 그룹 정책 컨피그레이션 모드에서 **ip-comp enable** 명령을 사용합니다. IP 압축을 비활성화하려면 **ip-comp disable** 명령을 사용합니다. 실행 중인 컨피그레이션에서 **ip-comp** 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ip-comp {**enable** | **disable**}

no ip-comp

구문 설명

disable	IP 압축을 비활성화합니다.
enable	IP 압축을 활성화합니다.

기본값

IP 압축이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령의 **no** 형식을 사용하면 다른 그룹 정책에서 값을 상속할 수 있습니다. 데이터 압축을 활성화하면 모뎀으로 연결하는 원격 전화 접속 사용자의 데이터 전송 속도가 빨라질 수 있습니다.

주의 데이터 압축을 사용하면 각 사용자 세션당 메모리 요구 사항 및 CPU 사용량이 늘어나며, 결과적으로 ASA의 전체적인 처리량이 줄어듭니다. 따라서 데이터 압축은 모뎀으로 연결하는 원격 사용자에 대해서만 활성화하는 것이 좋습니다. 모뎀 사용자를 위한 그룹 정책을 설계하고 이들에 대해서만 압축을 활성화하십시오.

엔드포인트가 IP 압축 트래픽을 생성하는 경우, 패킷의 부적절한 압축 해제를 방지하려면 IP 압축을 비활성화해야 합니다. 특정 LAN to LAN 터널에서 IP 압축을 활성화한 경우, 터널의 한쪽에서 다른 쪽으로 IP 압축 데이터를 전송하려고 시도할 때 호스트 A가 호스트 B와 통신할 수 없게 됩니다.

참고 "before-encryption"에 대해 **ip-comp** 명령이 활성화되고 IPsec 조각화가 구성된 경우에는 IPsec 압축(ip-comp_option 및 pre-encryption)을 사용할 수 없습니다. crypto chip으로 전송된 IP 헤더가 애매해지면(압축 때문에), 제공된 아웃바운드 패킷을 처리할 때 crypto chip에서 오류가 발생합니다. 양이 적은지(예: 600바이트) 확인하려면 MTU 수준을 검토해야 할 수 있습니다.

예 다음 예는 그룹 정책 "FirstGroup"에 대해 IP 압축을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-comp enable
```

ip local pool

IP 주소 풀을 구성하려면 매개변수 컨피그레이션 모드에서 **ip local pool** 명령을 사용합니다. 주소 풀을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

ip local pool *poolname first-address—last-address* [**mask** *mask*]

no ip local pool *poolname*

구문 설명

first-address	IP 주소 범위에서 시작 주소를 지정합니다.
last-address	IP 주소 범위에서 최종 주소를 지정합니다.
mask *mask*	(선택 사항) 주소 풀에 대해 서브넷 마스크를 지정합니다.
poolname	IP 주소 풀의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	ASA 클러스터링을 지원하려면 **ip address** 명령에서 클러스터 풀에 대해 IP 로컬 풀을 사용할 수 있습니다.

사용 지침

비표준 네트워크에 속하는 VPN 클라이언트 IP 주소가 할당된 경우 마스크 값을 제공해야 합니다. 기본 마스크를 사용하는 경우 데이터가 잘못 라우팅될 수 있습니다. 전형적인 예는 IP 로컬 풀이 10.10.10.0/255.255.255.0 주소를 포함하는 경우입니다(기본적으로 클래스 A 네트워크이기 때문). VPN 클라이언트가 서로 다른 인터페이스를 통해 10 네트워크 내에서 서로 다른 서브넷에 액세스해야 하는 경우 라우팅 문제가 발생할 수 있습니다. 예를 들어, 주소 10.10.100.1/255.255.255.0의 프린터는 인터페이스 2를 통해 이용할 수 있지만 10.10.10.0 네트워크는 VPN 터널을 통해 이용할 수 있으면, 인터페이스 1의 VPN 클라이언트는 프린터로 보내야 할 데이터를 어디로 라우팅해야 할지를 혼동할 수 있습니다. 10.10.10.0 및 10.10.100.0 서브넷 모두 10.0.0.0 클래스 A 네트워크에 속하므로 프린터 데이터는 VPN 터널을 통해 전송할 수 있습니다.

예

다음 예는 firstpool이라는 IP 주소 풀을 구성합니다. 시작 주소는 10.20.30.40이고 종료 주소는 10.20.30.50입니다. 네트워크 마스크는 255.255.255.0입니다.

```
ciscoasa(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

관련 명령

명령	설명
clear configure ip local pool	모든 IP 로컬 풀을 제거합니다.
show running-config ip local pool	IP 풀 컨피그레이션을 표시합니다. 특정 IP 주소 풀을 지정하려면 명령에 이름을 포함합니다.

ip-phone-bypass

IP Phone Bypass를 활성화하려면 그룹 정책 컨피그레이션 모드에서 **ip-phone-bypass enable** 명령을 사용합니다. 실행 중인 컨피그레이션에서 IP phone Bypass 특정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ip-phone-bypass {**enable** | **disable**}

no ip-phone-bypass

구문 설명

disable	IP Phone Bypass를 비활성화합니다.
enable	IP Phone Bypass를 활성화합니다.

기본값

IP Phone Bypass가 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

IP Phone Bypass를 비활성화하려면 **ip-phone-bypass disable** 명령을 사용합니다. 이 명령의 **no** 형식을 사용하면 다른 그룹 정책에서 IP Phone Bypass의 값을 상속하도록 허용할 수 있습니다.

IP Phone Bypass를 사용하면 하드웨어 클라이언트 뒤의 IP Phone을 사용자 인증 프로세스 없이 연결할 수 있습니다. 활성화할 경우 보안 유닛 인증은 계속 유효합니다.

사용자 인증을 활성화한 경우에만 IP Phone Bypass를 구성해야 합니다.

클라이언트의 인증을 면제하려면 **mac-exempt** 옵션도 구성해야 합니다. 자세한 내용은 **vpnclient mac-exempt** 명령을 참조하십시오.

예

다음 예는 그룹 정책 FirstGroup에 대해 IP Phone Bypass를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

관련 명령

명령	설명
user-authentication	하드웨어 클라이언트 뒤의 사용자가 연결 전에 ASA에 대해 스스로를 인증해야 합니다.

ips

검사를 위해 ASA에서 AIP SSM으로 트래픽을 전환하려면 클래스 컨피그레이션 모드에서 **ips** 명령을 사용합니다. 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

구문 설명

fail-close	AIP SSM이 실패하는 경우 트래픽을 차단합니다.
fail-open	AIP SSM이 실패하는 경우 트래픽을 허용합니다.
inline	패킷을 AIP SSM으로 전달합니다. IPS 작업의 결과 패킷이 삭제될 수 있습니다.
promiscuous	AIP SSM을 위해 패킷을 복제합니다. AIP SSM에서는 원래 패킷을 삭제할 수 없습니다.
sensor {*sensor_name* | *mapped_name*}	이 트래픽에 대한 가상 센서 이름을 설정합니다. AIP SSM에서 가상 센서를 사용하는 경우(버전 6.0 이상) 이 인수를 사용하여 센서 이름을 지정할 수 있습니다. 사용 가능한 센서 이름을 보려면 **ips ... sensor ?**를 입력합니다. 명령을 입력합니다. 사용 가능한 센서가 나열됩니다. **show ips** 명령을 사용할 수도 있습니다. ASA에서 다중 컨텍스트 모드를 사용하는 경우 컨텍스트에 할당한 센서만 지정할 수 있습니다(**allocate-ips** 참조). 컨텍스트에서 구성한 경우 *mapped_name* 인수를 사용합니다. 센서 이름을 지정하지 않으면 기본 센서가 트래픽에 사용됩니다. 다중 컨텍스트 모드에서는 컨텍스트에 대한 기본 센서를 지정할 수 있습니다. 단일 모드인 경우 또는 다중 모드에서 기본 센서를 지정하지 않은 경우 AIP SSM에 설정된 기본 센서가 트래픽에 사용됩니다. 아직 AIP SSM에 존재하지 않는 이름을 입력하면 오류 메시지가 표시되고 명령이 거부됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.0(2)	가상 센서 지원이 추가되었습니다.

사용 지침

ASA 5500 시리즈는, 완전한 기능을 갖춘 사전 대응형 침입 방지 서비스를 제공하여 웜과 네트워크 바이러스 등 악성 트래픽이 네트워크에 영향을 미치기 전에 차단하는 고급 IPS 소프트웨어를 실행하는 AIP SSM을 지원합니다. ASA에서 **ips** 명령을 구성하기 전 또는 후에 AIP SSM에서 보안 정책을 구성하십시오. ASA에서 AIP SSM으로 세션을 설정할 수도 있고(**session** 명령), 관리 인터페이스에서 SSH나 텔넷을 사용하여 AIP SSM에 직접 연결할 수도 있습니다. 또는 ASDM을 사용할 수 있습니다. AIP SSM 구성에 관한 자세한 정보는 *Command Line Interface를 이용한 Cisco Intrusion Prevention System Sensor 구성*를 참조하십시오.

ips 명령을 구성하려면 **class-map** 명령, **policy-map** 명령, **class** 명령을 차례로 구성해야 합니다.

AIP SSM은 ASA에서 별도의 애플리케이션을 실행합니다. 그러나 이 애플리케이션은 ASA 트래픽 흐름으로 통합됩니다. AIP SSM 자체에는 관리 인터페이스 외에 별도의 인터페이스가 포함되어 있지 않습니다. ASA의 트래픽 클래스에 **ips** 명령을 적용하면 트래픽이 다음과 같이 ASA에서 AIP SSM으로 흐릅니다.

1. 트래픽이 ASA로 들어갑니다.
2. 방화벽 정책이 적용됩니다.
3. 트래픽이 백플레인을 통해 AIP SSM으로 전송됩니다(**inline** 키워드 사용). 트래픽의 복사본만 AIP SSM으로 전송하는 방법에 대해서는 **promiscuous** 키워드를 참조하십시오.
4. AIP SSM이 보안 정책을 트래픽에 적용하고 적절한 작업을 수행합니다.
5. 유효한 트래픽은 백플레인을 통해 ASA로 다시 전송됩니다. AIP SSM은 자체 보안 정책에 따라 일부 트래픽을 차단할 수 있으며, 그러한 트래픽은 전달되지 않습니다.
6. VPN 정책이 적용됩니다(구성된 경우).
7. 트래픽이 ASA를 빠져나갑니다.

예

다음 예는 프로미스큐어스(promiscuous) 모드에서 모든 IP 트래픽을 AIP SSM으로 전환하고, 어떤 이유로든 AIP SSM 카드가 실패하면 모든 IP 트래픽을 차단합니다.

```
ciscoasa(config)# access-list IPS permit ip any any
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list IPS
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips promiscuous fail-close
ciscoasa(config-pmap-c)# service-policy my-ips-policy global
```

다음 예는 인라인 모드에서 10.1.1.0 및 10.2.1.0 네트워크로 향하는 모든 IP 트래픽을 AIP SSM으로 전환하고, 어떤 이유로든 AIP SSM 카드가 실패하면 모든 트래픽을 허용합니다. my-ips-class 트래픽에는 sensor1이 사용되고 my-ips-class2 트래픽에는 sensor2가 사용됩니다.

```
ciscoasa(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list my-ips-acl
ciscoasa(config)# class-map my-ips-class2
ciscoasa(config-cmap)# match access-list my-ips-acl2
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor1
ciscoasa(config-pmap)# class my-ips-class2
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor2
ciscoasa(config-pmap-c)# service-policy my-ips-policy interface outside
```

관련 명령

명령	설명
allocate-ips	보안 컨텍스트에 가상 센서를 할당합니다.
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
class-map	정책 맵에 사용할 트래픽을 식별합니다.
policy-map	트래픽 클래스 및 하나 이상의 작업을 결합한 정책을 구성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

ipsec-udp

IPsec over UDP를 활성화하려면 그룹 정책 컨피그레이션 모드에서 **ipsec-udp enable** 명령을 사용합니다. 현재 그룹 정책에서 IPsec over UDP 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipsec-udp {**enable** | **disable**}

no ipsec-udp

구문 설명

disable	IPsec over UDP를 비활성화합니다.
enable	IPsec over UDP를 활성화합니다.

기본값

IPsec over UDP는 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령의 **no** 형식을 사용하면 다른 그룹 정책에서 IPsec over UDP의 값을 상속하도록 허용할 수 있습니다.

IPsec over UDP(IPsec through NAT이라고도 함)에서는 Cisco VPN Client 또는 하드웨어 클라이언트가 NAT를 실행하는 ASA에 UDP를 통해 연결할 수 있습니다.

IPsec over UDP를 비활성화하려면 **ipsec-udp disable** 명령을 사용합니다.

IPsec over UDP를 사용하려면 **ipsec-udp-port** 명령도 구성해야 합니다.

IPsec over UDP를 사용하려면 Cisco VPN Client도 구성해야 합니다(기본적으로 사용하도록 구성되어 있음). VPN 3002는 IPsec over UDP 사용을 위한 컨피그레이션을 요구하지 않습니다.

IPsec over UDP는 독점적이고, 원격 액세스 연결에만 적용되며, 모드 컨피그레이션을 요구합니다. 즉 ASA는 SA 협상 중에 클라이언트와 컨피그레이션 매개변수를 교환합니다.

IPsec over UDP를 사용하는 경우 시스템 성능이 약간 저하될 수 있습니다.

VPN 클라이언트로서 운영되는 ASA5505에서는 ipsec-udp-port 명령이 지원되지 않습니다. 클라이언트 모드의 ASA 5505는 UDP 포트 500 및/또는 4500에서 IPsec 세션을 시작할 수 있습니다.

예

다음 예는 그룹 정책 FirstGroup에 대해 IPsec over UDP를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp enable
```

관련 명령

명령	설명
ipsec-udp-port	ASA가 UDP 트래픽을 수신 대기하는 포트를 지정합니다.

ipsec-udp-port

IPsec over UDP에 대한 UDP 포트 번호를 설정하려면 그룹 정책 컨피그레이션 모드에서 **ipsec-udp-port** 명령을 사용합니다. UDP 포트를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipsec-udp-port *port*

no ipsec-udp-port

구문 설명

port	4001~49151 범위의 정수를 사용하여 UDP 포트 번호를 식별합니다.

기본값

기본 포트는 10000입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령의 **no** 형식을 사용하면 다른 그룹 정책에서 IPsec over UDP 포트의 값을 상속하도록 허용할 수 있습니다.

IPsec 협상 시 ASA는 구성된 포트에서 수신 대기하며, 다른 필터 규칙이 UDP 트래픽을 삭제하는 경우에도 해당 포트에 대한 UDP 트래픽을 전달합니다.

이 기능을 활성화하여 여러 그룹 정책을 구성할 수 있으며, 각 그룹 정책에 서로 다른 포트 번호를 사용할 수 있습니다.

예

다음 예는 그룹 정책 FirstGroup에 대해 IPsec over UDP 포트를 포트 4025로 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp-port 4025
```

관련 명령

명령	설명
ipsec-udp	Cisco VPN Client 또는 하드웨어 클라이언트가 NAT를 실행하는 ASA에 UDP를 통해 연결할 수 있습니다.

ip verify reverse-path

Unicast RPF를 활성화하려면 글로벌 컨피그레이션 모드에서 **ip verify reverse-path** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

구문 설명

interface_name	Unicast RPF를 활성화할 인터페이스

기본값

이 기능은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Unicast RPF는 모든 패킷이 라우팅 테이블에 따라 올바른 소스 인터페이스와 일치하는 소스 IP 주소를 갖도록 보장함으로써 IP 스푸핑(실제 소스를 알아볼 수 없도록 패킷이 잘못된 소스 IP 주소를 사용함)을 방지합니다.

일반적으로 ASA는 패킷을 어디로 전달할지를 결정할 때 수신 주소만 확인합니다. Unicast RPF는 ASA에 소스 주소도 확인하도록 지시합니다. 따라서 이것을 RPF(Reverse Path Forwarding)라고 부릅니다. ASA의 통과를 허용할 모든 트래픽에 대해 ASA 라우팅 테이블은 소스 주소로 돌아가는 경로를 포함해야 합니다. 자세한 내용은 RFC 2267을 참조하십시오.

예를 들어 외부 트래픽의 경우 ASA는 Unicast RPF 보호를 충족하기 위해 기본 경로를 사용할 수 있습니다. 트래픽이 외부 인터페이스에서 들어오고 소스 주소가 라우팅 테이블에 알려지지 않은 경우, ASA는 기본 경로를 사용하여 외부 인터페이스를 소스 인터페이스로서 정확히 식별합니다.

트래픽이 라우팅 테이블에 알려진 주소에서 외부 인터페이스로 이동하는 경우 ASA는 패킷을 삭제합니다. 마찬가지로, 트래픽이 알려지지 않은 소스 주소로부터 내부 인터페이스로 이동하는 경우 일치하는 경로(기본 경로)가 외부 인터페이스임을 나타내기 때문에 ASA는 패킷을 삭제합니다.

Unicast RPF는 다음과 같이 구현됩니다.

- ICMP 패킷에는 세션이 없으므로 각 패킷이 점검됩니다.
- UDP 및 TCP에는 세션이 있으므로 초기 패킷에서 역방향 경로 조회를 요구합니다. 세션 중에 도착하는 후속 패킷은 세션의 일부로서 유지 관리되는 기존 상태를 사용하여 점검됩니다. 초기 패킷 이외의 패킷에서는 초기 패킷에 사용된 것과 동일한 인터페이스에 도착했는지를 확인합니다.

예

다음 예는 외부 인터페이스에서 Unicast RPF를 활성화합니다.

```
ciscoasa(config)# ip verify reverse-path interface outside
```

관련 명령

명령	설명
clear configure ip verify reverse-path	**ip verify reverse-path** 명령을 사용하여 설정한 컨피그레이션을 지웁니다.
clear ip verify statistics	Unicast RPF 통계를 지웁니다.
show ip verify statistics	Unicast RPF 통계를 보여줍니다.
show running-config ip verify reverse-path	**ip verify reverse-path** 명령을 사용하여 설정한 컨피그레이션을 표시합니다.

4 장

ipv6 address through ipv6-vpn-filter 명령

ipv6 address

인터페이스에서(라우팅된 모드) 또는 관리 주소에 대해(투명 모드) IPv6을 활성화하고 IPv6 주소를 구성하려면 **ipv6 address** 명령을 사용합니다. IPv6 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-prefix* | **cluster-pool** *poolname*] | *ipv6-prefix*/*prefix-length* **eui-64** | *ipv6-address* **link-local** [**standby** *ipv6-address*]}

no ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address* | **cluster-pool** *poolname*] | *ipv6-prefix*/*prefix-length* **eui-64** | *ipv6-address* **link-local** [**standby** *ipv6-address*]}

구문 설명

autoconfig	인터페이스에서 스테이트리스 자동 컨피그레이션을 활성화합니다. 인터페이스에서 스테이트리스 자동 컨피그레이션을 활성화하면, 라우터 광고 메시지에서 수신된 접두사를 기반으로 IPv6 주소가 구성됩니다. 스테이트리스 자동 컨피그레이션이 활성화될 경우, Modified EUI-64 인터페이스 ID를 기반으로 하는 링크-로컬 주소가 인터페이스에 대해 자동으로 생성됩니다. 투명 방화벽 모드에서 지원되지 않습니다. **참고** RFC 4862에서는 스테이트리스 자동 컨피그레이션에 구성된 호스트에서 라우터 광고 메시지를 보내지 않도록 지정하지만, 이 경우에는 ASA에서 라우터 광고 메시지를 전송합니다. 메시지를 보내지 않도록 하려면 **ipv6 nd suppress-ra** 명령을 참조하십시오.
cluster-pool *poolname*	(선택 사항) ASA 클러스터링의 경우 **ipv6 local pool** 명령으로 정의된 주소의 클러스터 풀을 설정합니다. 이 인수로 정의한 기본 클러스터 IP 주소는 현재 마스터 유닛에만 속합니다. 각 클러스터 멤버는 이 풀에서 로컬 IP 주소를 수신합니다. 각 유닛에 정확히 어떤 주소가 할당되는지 미리 확인할 수는 없습니다. 각 유닛에 사용된 주소를 보려면 **show ipv6 local pool** *poolname* 명령을 입력합니다. 각 클러스터 멤버는 클러스터에 참가할 때 멤버 ID가 할당됩니다. ID는 풀에서 사용되는 로컬 IP를 결정합니다.
ipv6-address/*prefix-length*	인터페이스에 전역 주소를 지정합니다. 전역 주소를 할당하면 인터페이스에 대한 링크-로컬 주소가 자동으로 생성됩니다.

ipv6-prefix/*prefix-length* **eui-64**	지정된 접두사를 Modified EUI-64 형식으로 인터페이스 MAC 주소에서 생성한 인터페이스 ID와 결합하여 인터페이스에 전역 주소를 할당합니다. 전역 주소를 할당하면 인터페이스에 대한 링크-로컬 주소가 자동으로 생성됩니다. *prefix-length* 인수에 대해 지정한 값이 64비트보다 크면 접두사 비트가 인터페이스 ID보다 우선합니다. 다른 호스트가 지정된 주소를 사용 중이면 오류 메시지가 표시됩니다. 스탠바이 주소를 지정하지 않아도 되며, 인터페이스 ID가 자동으로 생성됩니다. Modified EUI-64 형식 인터페이스 ID는 링크 계층 주소의 상위 3바이트(OUI 필드)와 하위 3바이트(일련 번호) 간에 16진수 FFFE를 삽입하여 48비트 링크 계층(MAC) 주소에서 파생됩니다. 선택한 주소가 고유한 이더넷 MAC 주소에서 온 것인지 확인하기 위해, 48비트 주소의 고유성을 나타내도록 상위 바이트의 다음-최하위(next-to-lowest) 순서 비트가 반전됩니다(universal/local 비트). 예를 들어, MAC 주소가 00E0.B601.3B7A인 인터페이스의 64비트 인터페이스 ID는 02E0:B6FF:FE01:3B7A가 될 수 있습니다.
ipv6-address **link-local**	링크-로컬 주소만 수동으로 구성합니다. 이 명령으로 지정한 *ipv6-address*는 인터페이스에 대해 자동으로 생성된 링크-로컬 주소를 재지정합니다. 링크-로컬 주소는 링크-로컬 접두사 FE80::/64 및 Modified EUI-64 형식의 인터페이스 ID로 구성됩니다. MAC 주소가 00E0.B601.3B7A인 인터페이스의 링크-로컬 주소는 FE80::2E0:B6FF:FE01:3B7A가 될 수 있습니다. 다른 호스트가 지정된 주소를 사용 중이면 오류 메시지가 표시됩니다.
standby *ipv6-address*	(선택 사항) standby는 장애 조치 쌍의 보조 유닛 또는 장애 조치 그룹에서 사용하는 인터페이스 주소를 지정합니다.

기본값

IPv6이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.
8.2(2)	스탠바이 주소 지원이 명령에 추가되었습니다.
8.4(1)	투명 모드의 경우, 브리지 그룹이 추가되었습니다. 전체가 아니라 BVI에 대해 IP 주소를 설정할 수 있습니다.
9.0(1)	ASA 클러스터링을 지원하도록 **cluster-pool** 키워드가 추가되었습니다.

사용 지침

인터페이스에 IPv6 주소를 구성하면 해당 인터페이스에서 IPv6이 활성화됩니다. IPv6 주소를 지정한 후 **ipv6 enable** 명령을 사용할 필요가 없습니다.

다중 컨텍스트 모드 지침

단일 컨텍스트 라우팅된 방화벽 모드에서 각 인터페이스 주소는 고유한 서브넷에 있어야 합니다. 다중 컨텍스트 모드에서 이 인터페이스가 공유 인터페이스에 있는 경우, 각 IP 주소는 고유해야 하지만 동일한 서브넷에 있어야 합니다. 인터페이스가 고유하면 원하는 경우 이 IP 주소를 다른 컨텍스트에서 사용할 수 있습니다.

투명 방화벽 지침

투명 방화벽은 IP 라우팅에 참여하지 않습니다. ASA에 필요한 유일한 IP 컨피그레이션은 BVI 주소를 설정하는 것입니다. ASA는 이 주소를 ASA에서 시작되는 트래픽(예: 시스템 메시지 또는 AAA 서버와의 통신)에 대한 소스 주소로 사용하기 때문에 이 주소가 필요합니다. 원격 관리 액세스에도 이 주소를 사용할 수 있습니다. 이 주소는 업스트림 및 다운스트림 라우터와 동일한 서브넷에 있어야 합니다. 다중 컨텍스트 모드의 경우, 각 컨텍스트 내에 관리 IP 주소를 설정합니다. 관리 인터페이스를 포함하는 모델의 경우 관리 목적으로 이 인터페이스에 대한 IP 주소를 설정할 수도 있습니다.

장애 조치 지침

스탠바이 IP 주소는 기본 IP 주소와 동일한 서브넷에 있어야 합니다.

ASA 클러스터링 지침

클러스터 인터페이스 모드를 individual로 구성한 후에야 개별 인터페이스에 대해 클러스터 풀을 설정할 수 있습니다(**cluster-interface mode individual**). 관리 전용 인터페이스에 대한 유일한 예외는 다음과 같습니다.

- 관리 전용 인터페이스는 항상 개별 인터페이스로 구성할 수 있으며, Spanned EtherChannel 모드에서도 마찬가지입니다. 투명 방화벽 모드에서도 관리 인터페이스는 개별 인터페이스가 될 수 있습니다.
- Spanned EtherChannel 모드에서 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 경로를 사용해야 합니다.

예

다음 예는 선택한 인터페이스에 대한 전역 주소로서 3FFE:C00:0:1::576/64를 할당합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

다음 예는 선택한 인터페이스에 대해 IPv6 주소를 자동으로 할당합니다.

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 address autoconfig
```

다음 예는 선택한 인터페이스에 IPv6 주소 3FFE:C00:0:1::/64를 할당하고, 주소의 낮은 순서 64비트로 EUI-64 인터페이스 ID를 지정합니다. 이 디바이스가 장애 조치 쌍의 일부이면 **standby** 키워드를 지정할 필요가 없습니다. Modified EUI-64 인터페이스 ID를 사용하면 스탠바이 주소가 자동으로 생성됩니다.

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

다음 예는 선택한 인터페이스에 대한 링크 수준 주소로서 FE80::260:3EFF:FE11:6670을 할당합니다.

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

다음 예는 선택한 인터페이스에 대한 전역 주소로서 3FFE:C00:0:1::576/64를 할당하고, 스탠바이 유닛의 해당 인터페이스에 대한 주소로서 3FFE:C00:0:1::575를 할당합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 3ffe:c00:0:1::576/64 standby 3ffe:c00:0:1::575
```

다음 예는 장애 조치 쌍의 기본 유닛에서 선택한 인터페이스에 대한 링크 수준 주소로서 FE80::260:3EFF:FE11:6670을 할당하고, 보조 유닛의 해당 인터페이스에 대한 링크 수준 주소로서 FE80::260:3EFF:FE11:6671을 할당합니다.

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

관련 명령

명령	설명
debug ipv6 interface	IPv6 인터페이스에 대한 디버깅 주소를 표시합니다.
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 상태를 표시합니다.

ipv6 dhcprelay enable

인터페이스에서 DHCPv6 릴레이 서비스를 활성화하려면 글로벌 컨피그레이션 모드에서 **ipv6 dhcprelay enable** 명령을 사용합니다. DHCPv6 릴레이 서비스를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 dhcprelay enable *interface*

no ipv6 dhcprelay enable *interface*

구문 설명

interface	대상에 대한 출력 인터페이스를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 인터페이스에서 DHCPv6 릴레이 서비스를 활성화할 수 있습니다. 이 서비스가 활성화되면 인터페이스에서 클라이언트로부터 들어오는 DHCPv6 메시지(또 다른 릴레이 에이전트에 의해 릴레이된 것일 수 있음)가 모든 구성된 나가는 링크를 통해 모든 구성된 릴레이 목적지로 전달됩니다. 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트가 사용하는 인터페이스(즉, 공유 인터페이스)에서 DHCP 릴레이 서비스를 활성화할 수 없습니다.

예

다음 예는 ASA 외부 인터페이스에서 IP 주소 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701의 DHCPv6 서버에 대해 DHCPv6 릴레이 에이전트를 구성하는 방법을 보여줍니다. 클라이언트 요청은 ASA 내부 인터페이스에서 오며, 바인딩 시간 제한 값은 90초입니다.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

관련 명령

명령	설명
ipv6 dhcprelay server	클라이언트 메시지가 전달되는 IPv6 DHCP 서버 수신 주소를 지정합니다.
ipv6 dhcprelay timeout	DHCPv6 서버에서 릴레이 바인딩 구조를 거쳐 DHCPv6 클라이언트에 전달하는 응답에 허용된 시간(초)을 설정합니다.

ipv6 dhcprelay server

클라이언트 메시지가 전달되는 IPv6 DHCP 서버 수신 주소를 지정하려면 글로벌 컨피그레이션 모드에서 **ipv6 dhcprelay server** 명령을 사용합니다. IPv6 DHCP 수신 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 dhcprelay server *ipv6-address* [*interface*]

no ipv6 dhcprelay server *ipv6-address* [*interface*]

구문 설명

interface	(선택 사항) 수신 주소에 대한 출력 인터페이스를 지정합니다.
ipv6-address	링크 범위 유니캐스트, 멀티캐스트, 사이트 범위 유니캐스트 또는 전역 IPv6 주소일 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 클라이언트 메시지가 전달되는 IPv6 DHCP 서버 수신 주소를 지정할 수 있습니다. 클라이언트 메시지는 출력 인터페이스가 연결된 링크를 통해 수신 주소에 전달됩니다. 지정된 주소가 링크 범위 주소일 경우 인터페이스를 지정해야 합니다. 미지정, 루프백, 노드-로컬 멀티캐스트 주소는 릴레이 목적지로 허용되지 않습니다. 컨텍스트당 최대 10개의 서버를 지정할 수 있습니다.

예

다음 예는 ASA 외부 인터페이스에서 IP 주소 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701의 DHCPv6 서버에 대해 DHCPv6 릴레이 에이전트를 구성하는 방법을 보여줍니다. 클라이언트 요청은 ASA 내부 인터페이스에서 오며, 바인딩 시간 제한 값은 90초입니다.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

관련 명령

명령	설명
ipv6 dhcprelay enable	인터페이스에서 IPv6 DHCP 릴레이 서비스를 활성화합니다.
ipv6 dhcprelay timeout	DHCPv6 서버에서 릴레이 바인딩 구조를 거쳐 DHCPv6 클라이언트에 전달하는 응답에 허용된 시간(초)을 설정합니다.

ipv6 dhcprelay timeout

DHCPv6 서버에서 릴레이 바인딩 구조를 거쳐 DHCPv6 클라이언트에 전달하는 응답에 허용된 시간(초)을 설정하려면 글로벌 컨피그레이션 모드에서 **ipv6 dhcprelay timeout** 명령을 사용합니다. 기본 설정으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 dhcprelay timeout *seconds*

no ipv6 dhcprelay timeout *seconds*

구문 설명

seconds	DHCPv6 릴레이 주소 협상에 대해 허용된 시간(초)을 설정합니다. 유효한 값의 범위는 1~3600입니다.

기본값

기본값은 60초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 DHCPv6 서버에서 릴레이 주소 처리를 위해 릴레이 바인딩을 거쳐 DHCPv6 클라이언트에 전달하는 응답에 허용된 시간(초)을 설정합니다.

예

다음 예는 ASA 외부 인터페이스에서 IP 주소 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701의 DHCPv6 서버에 대해 DHCPv6 릴레이 에이전트를 구성하는 방법을 보여줍니다. 클라이언트 요청은 ASA 내부 인터페이스에서 오며, 바인딩 시간 제한 값은 90초입니다.

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

관련 명령

명령	설명
ipv6 dhcprelay server	클라이언트 메시지가 전달되는 IPv6 DHCP 서버 수신 주소를 지정합니다.
ipv6 dhcprelay enable	클라이언트 메시지가 전달되는 IPv6 DHCP 서버 수신 주소를 지정합니다.

ipv6 enable

명시적 IPv6 주소를 아직 구성하지 않은 상태에서 IPv6 프로세싱을 활성화하려면 글로벌 컨피그레이션 모드에서 **ipv6 enable** 명령을 사용합니다. 명시적 IPv6 주소로 구성되지 않은 인터페이스에서 IPv6 프로세싱을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 enable

no ipv6 enable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

IPv6이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—
글로벌 컨피그레이션	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

ipv6 enable 명령은 인터페이스에서 IPv6 링크-로컬 유니캐스트 주소를 자동으로 구성하며, 또한 IPv6 프로세싱용 인터페이스를 활성화합니다.

no ipv6 enable 명령은 명시적 IPv6 주소로 구성된 인터페이스에서 IPv6 프로세싱을 비활성화하지 않습니다.

예

다음 예는 선택한 인터페이스에서 IPv6 프로세싱을 활성화합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

관련 명령

명령	설명
ipv6 address	인터페이스에 대한 IPv6 주소를 구성하고 인터페이스에서 IPv6 프로세싱을 활성화합니다.
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 enforce-eui64

로컬 링크의 IPv6 주소에서 Modified EUI-64 형식의 인터페이스 식별자를 강제로 사용하도록 하려면 글로벌 컨피그레이션 모드에서 **ipv6 enforce-eui64** 명령을 사용합니다. Modified EUI-64 주소 형식의 강제 사용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 enforce-eui64 *if_name*

no ipv6 enforce-eui64 *if_name*

구문 설명

if_name	Modified EUI-64 주소 형식의 강제 사용을 활성화하는 인터페이스의 이름(**nameif** 명령으로 지정)을 지정합니다.

기본값

Modified EUI-64 형식의 강제 사용을 비활성화합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

이 명령이 인터페이스에서 활성화된 경우, 그 인터페이스에서 수신한 IPv6 패킷의 소스 주소를 소스 MAC 주소와 비교하여 검증함으로써 인터페이스 식별자가 Modified EUI-64 형식을 사용하는지 확인합니다. IPv6 패킷에서 인터페이스 식별자에 Modified EUI-64 형식을 사용하지 않을 경우 패킷은 폐기되고 다음 syslog 메시지가 생성됩니다.

```
%ASA-3-325003: EUI-64 source address check failed.
```

주소 형식 검증은 흐름이 생성되는 경우에만 수행됩니다. 기존 흐름의 패킷은 검사하지 않습니다. 또한 이 주소 검증은 로컬 링크의 호스트에 대해서만 수행할 수 있습니다. 라우터 뒤에 있는 호스트로부터 받은 패킷은 주소 형식 검증을 통과하지 못해 폐기됩니다. 그 소스 MAC 주소가 호스트 MAC 주소가 아닌 라우터 MAC 주소이기 때문입니다.

Modified EUI-64 형식 인터페이스 식별자는 링크 계층 주소의 상위 3바이트(OUI 필드)와 하위 3바이트(일련 번호) 간에 16진수 FFFE를 삽입하여 48비트 링크 계층(MAC) 주소에서 파생됩니다. 선택한 주소가 고유한 이더넷 MAC 주소에서 온 것인지 확인하기 위해, 48비트 주소의 고유성을 나타내도록 상위 바이트의 다음-최하위(next-to-lowest) 순서 비트가 반전됩니다(universal/local 비트). 예를 들어, MAC 주소가 00E0.B601.3B7A인 인터페이스의 64비트 인터페이스 ID는 02E0:B6FF:FE01:3B7A가 될 수 있습니다.

예

다음 예는 내부 인터페이스에서 수신하는 IPv6 주소에 대해 Modified EUI-64 형식의 강제 사용을 활성화합니다.

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

관련 명령

명령	설명
ipv6 address	인터페이스에서 IPv6 주소를 구성합니다.
ipv6 enable	인터페이스에서 IPv6을 활성화합니다.

ipv6 icmp

인터페이스에서 ICMP 액세스 규칙을 구성하려면 글로벌 컨피그레이션 모드에서 **ipv6 icmp** 명령을 사용합니다. ICMP 액세스 규칙을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

구문 설명

any	임의의 IPv6 주소를 지정하는 키워드. IPv6 접두사 ::/0의 약어.
deny	선택한 인터페이스에서 지정한 ICMP 트래픽을 차단합니다.
host	주소가 특정 호스트를 가리킴을 나타냅니다.
icmp-type	ICMP 메시지 유형이 액세스 규칙에 의해 필터링되도록 지정합니다. 값은 유효한 ICMP 유형 번호(0~255)이거나 다음 ICMP 유형 리터럴 중 하나일 수 있습니다. • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	액세스 규칙이 적용되는 인터페이스의 이름입니다(**nameif** 명령으로 지정).
ipv6-address	인터페이스에 ICMPv6 메시지를 전송하는 호스트의 IPv6 주소입니다.
ipv6-prefix	인터페이스에 ICMPv6 메시지를 전송하는 IPv6 네트워크입니다.
permit	지정한 ICMP 트래픽을 선택한 인터페이스에서 허용합니다.
prefix-length	IPv6 접두사의 길이입니다. 이 값은 주소에서 얼마나 많은 상위 연속 비트가 접두사의 네트워크 부분을 구성하는지 나타냅니다. 슬래시(/)가 접두사 길이 앞에 와야 합니다.

기본값

정의된 ICMP 액세스 규칙이 없으면 모든 ICMP 트래픽이 허용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

IPv6의 ICMP는 IPv4의 ICMP와 동일하게 작동합니다. ICMPv6은 오류 메시지(예: ICMP 대상에 도달할 수 없다는 메시지) 및 정보 메시지(예: ICMP 에코 요청 및 응답 메시지)를 생성합니다. 또한 IPv6 인접 디바이스 검색 프로세스 및 경로 MTU 검색에서 IPv6의 ICMP 패킷이 사용됩니다.

IPv6 지원 인터페이스에서 허용되는 최소 MTU는 1280바이트입니다. 그러나 인터페이스에서 IPsec이 사용되는 경우, IPsec 암호화의 오버헤드 때문에 MTU 값을 1380 미만으로 설정해서는 안 됩니다. 인터페이스를 1380바이트 미만으로 설정하면 패킷이 삭제될 수 있습니다.

인터페이스에 대해 정의된 ICMP 규칙이 없으면 모든 IPv6 ICMP 트래픽이 허용됩니다.

인터페이스에 대해 정의된 ICMP 규칙이 있으면, 암시적인 모두 거부 규칙에 이어 먼저 일치하는 것이 먼저 적용되는 방식으로 규칙이 처리됩니다. 예를 들어, 첫 번째 일치 규칙이 허용 규칙이면 ICMP 패킷이 처리됩니다. 첫 번째 일치 규칙이 거부 규칙이거나 ICMP 패킷이 해당 인터페이스에서 어떤 규칙과도 일치하지 않는 경우 ASA는 ICMP 패킷을 폐기하고 syslog 메시지를 생성합니다.

따라서 ICMP 규칙을 입력하는 순서는 중요합니다. 특정 네트워크의 모든 ICMP 트래픽을 거부하는 규칙을 입력하고 그 뒤에 해당 네트워크의 특별한 호스트에서 오는 ICMP 트래픽을 허용하는 규칙을 입력하면 호스트 규칙은 처리되지 않습니다. ICMP 트래픽은 네트워크 규칙에 의해 차단됩니다. 그러나 호스트 규칙을 먼저 입력하고 그 뒤에 네트워크 규칙을 입력하면, 호스트 ICMP 트래픽은 허용되고 해당 네트워크의 다른 모든 ICMP 트래픽은 차단됩니다.

ipv6 icmp 명령은 ASA 인터페이스에서 종료되는 ICMP 트래픽에 대한 액세스 규칙을 구성합니다. Pass-through ICMP 트래픽에 대한 액세스 규칙을 구성하려면 **ipv6 access-list** 명령을 참조하십시오.

예

다음 예는 외부 인터페이스에서 모든 ping 요청을 거부하고 모든 packet-too-big 메시지를 허용합니다(경로 MTU 검색을 지원하기 위해).

```
ciscoasa(config)# ipv6 icmp deny any echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

다음 예는 호스트 2000:0:0:4::2 또는 접두사 2001::/64의 호스트가 외부 인터페이스에 대해 ping하도록 허용합니다.

```
ciscoasa(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
ciscoasa(config)# ipv6 icmp permit 2001::/64 echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

관련 명령

명령	설명
ipv6 access-list	액세스 목록을 구성합니다.

ipv6 local pool

IPv6 주소 풀을 구성하려면 매개변수 컨피그레이션 모드에서 **ipv6 local pool** 명령을 사용합니다. 풀을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

no ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

구문 설명

ipv6_address	풀에 대한 시작 IPv6 주소를 지정합니다.
number_of_addresses	범위: 1~16384
pool_name	이 IPv6 주소 풀에 할당할 이름을 지정합니다.
prefix_length	범위: 0~128

기본값

기본적으로 IPv6 로컬 주소 풀은 구성되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.
9.0(1)	ASA 클러스터링을 지원하려면 **ipv6 address** 명령에서 클러스터 풀에 대해 IPv6 로컬 풀을 사용할 수 있습니다.

사용 지침

VPN의 경우 IPv6 로컬 풀을 할당하려면 터널 그룹에서 **ipv6-local-pool** 명령을 사용하거나 그룹 정책에서 **ipv6-address-pools** 명령을 사용합니다(이 명령의 "s"에 유의). 그룹 정책의 ipv6-address-pools 설정은 터널 그룹의 ipv6-address-pools 설정을 재지정합니다.

예

다음 예는 원격 클라이언트에 주소를 할당하는 데 사용할 firstipv6pool이라는 IPv6 주소 풀을 구성합니다.

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
ciscoasa(config)#
```

관련 명령

명령	설명
ipv6-address-pool	IPv6 주소 풀을 VPN 터널 그룹 정책과 연결합니다.
ipv6-address-pools	IPv6 주소 풀을 VPN 그룹 정책과 연결합니다.
clear configure ipv6 local pool	구성된 모든 IPv6 로컬 풀을 지웁니다.
show running-config ipv6	IPv6에 대한 컨피그레이션을 보여줍니다.

ipv6 nd dad attempts

중복 주소 감지 중에 인터페이스에서 전송할 연속 인접 디바이스 요청 메시지의 수를 구성하려면 컨피그레이션 모드에서 **ipv6 nd dad attempts** 명령을 사용합니다. 전송할 중복 주소 감지 메시지 수의 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts *value*

구문 설명

value	0~600의 숫자입니다. 0을 입력하면 지정된 인터페이스에서 중복 주소 감지가 비활성화됩니다. 1을 입력하면 후속 전송 없이 단일 전송이 구성됩니다. 기본값은 메시지 1개입니다.

기본값

기본 시도 횟수는 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

중복 주소 감지가 새로운 유니캐스트 IPv6 주소의 고유성을 먼저 확인한 후 주소가 인터페이스에 할당됩니다(중복 주소 감지 수행 중에는 새로운 주소가 임시 상태를 유지). 중복 주소 감지는 인접 디바이스 요청 메시지를 사용하여 유니캐스트 IPv6 주소의 고유성을 확인합니다. 인접 디바이스 요청 메시지가 전송되는 빈도는 **ipv6 nd ns-interval** 명령을 사용하여 구성합니다.

관리상 가동 중지된 인터페이스에서는 중복 주소 감지가 중지됩니다. 인터페이스가 관리상 가동 중지된 동안에는 인터페이스에 할당된 유니캐스트 IPv6 주소가 대기 상태로 설정됩니다.

인터페이스가 관리상 가동 상태로 복귀하면 중복 주소 감지가 해당 인터페이스에서 자동으로 다시 시작됩니다. 관리상 가동 상태로 복귀하는 인터페이스는 인터페이스의 모든 유니캐스트 IPv6 주소에 대한 중복 주소 감지를 재시작합니다.

참고 중복 주소 감지는 인터페이스의 링크-로컬 주소에서 수행되는 반면 나머지 IPv6 주소의 상태는 여전히 임시 상태로 설정됩니다. 링크-로컬 주소에서 중복 주소 감지가 완료된 후 나머지 IPv6 주소에서도 중복 주소 감지가 수행됩니다.

중복 주소 감지가 중복 주소를 식별하면, 해당 주소는 상태가 DUPLICATE로 설정되고 사용되지 않습니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 비활성화되고 다음과 유사한 오류 메시지가 표시됩니다.

```
%ASA-4-DUPLICATE: Duplicate address FE80::1 on outside
```

중복 주소가 인터페이스의 전역 주소인 경우, 해당 주소는 사용되지 않고 다음과 유사한 오류 메시지가 표시됩니다.

```
%ASA-4-DUPLICATE: Duplicate address 3000::4 on outside
```

주소 상태가 DUPLICATE로 설정된 동안 중복 주소와 연결된 모든 컨피그레이션 명령은 구성된 상태를 유지합니다.

인터페이스의 링크-로컬 주소가 변경된 경우 새로운 링크-로컬 주소에서 중복 주소 감지가 수행되고 인터페이스와 연결된 모든 다른 IPv6 주소가 다시 생성됩니다(중복 주소 감지는 새로운 링크-로컬 주소에서만 수행됨).

예

다음 예는 인터페이스의 임시 IPv6 주소에서 중복 주소 감지가 수행 중일 때 전송할 연속 인접 디바이스 요청 메시지 수를 5로 구성합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 5
```

다음 예는 선택한 인터페이스에서 중복 주소 감지를 비활성화합니다.

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 nd dad attempts 0
```

관련 명령

명령	설명
ipv6 nd ns-interval	인터페이스에서 IPv6 인접 디바이스 요청 전송 사이의 간격을 구성합니다.
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 nd managed-config-flag

IPv6 라우터 광고 패킷에서 Managed Address Config 플래그를 설정하도록 ASA를 구성하려면 컨피그레이션 모드에서 **ipv6 nd managed config-flag** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd managed-config-flag

no ipv6 managed-config-flag

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

파생된 스테이트리스 자동 컨피그레이션 주소 이외의 주소를 가져오려면 스테이트풀 주소 컨피그레이션 프로토콜(DHCPv6)을 사용해야 함을 나타내기 위해 IPv6 자동 컨피그레이션 클라이언트 호스트는 이 플래그를 사용할 수 있습니다.

예

다음 예는 인터페이스 GigabitEthernet 0/0에 대한 IPv6 라우터 광고 패킷에서 Managed Address Config 플래그를 설정합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

관련 명령

명령	설명
ipv6 nd other-config-flag	IPv6 라우터 광고 패킷에서 다른 Config 플래그를 설정하도록 ASA를 구성합니다.

ipv6 nd ns-interval

인터페이스에서 IPv6 인접 디바이스 요청 재전송 사이의 간격을 구성하려면 컨피그레이션 모드에서 **ipv6 nd ns-interval** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

구문 설명

value	IPv6 인접 디바이스 요청 전송 사이의 간격(밀리초). 유효한 값은 1000~3600000밀리초입니다. 기본값은 1000밀리초입니다.

기본값

기본값은 인접 디바이스 요청 전송 간 1000밀리초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

이 값은 인터페이스에서 전송된 모든 IPv6 라우터 광고에 포함됩니다.

예

다음 예는 GigabitEthernet 0/0에 대한 IPv6 인접 디바이스 요청 전송 간격을 9000밀리초로 구성합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

관련 명령

명령	설명
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 nd other-config-flag

IPv6 라우터 광고 패킷에서 기타 Config 플래그를 설정하도록 ASA를 구성하려면 컨피그레이션 모드에서 **ipv6 nd other-config-flag** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd other-config-flag

no ipv6 other-config-flag

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

DNS 서버 정보 등 주소 외의 컨피그레이션 정보를 가져오려면 스테이트풀 주소 컨피그레이션 프로토콜(DHCPv6)을 사용해야 함을 나타내기 위해 IPv6 자동 컨피그레이션 클라이언트 호스트는 이 플래그를 사용할 수 있습니다.

예

다음 예는 인터페이스 GigabitEthernet 0/0에 대한 IPv6 라우터 광고 패킷에서 기타 Config 플래그를 설정합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

관련 명령

명령	설명
ipv6 nd managed-config-flag	IPv6 라우터 광고 패킷에서 Managed Address Config 플래그를 설정하도록 ASA를 구성합니다.

ipv6 nd prefix

IPv6 라우터 광고에 어떤 IPv6 접두사를 포함할지를 구성하려면 인터페이스 컨피그레이션 모드에서 **ipv6 nd prefix** 명령을 사용합니다. 접두사를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd prefix *ipv6-prefix*/*prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

no ipv6 nd prefix *ipv6-prefix*/*prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

구문 설명

at *valid-date preferred-date*	수명 및 기본 설정이 만료되는 날짜와 시간. 접두사는 지정된 날짜와 시간에 도달할 때까지 유효합니다. 날짜는 *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* 형식으로 표현됩니다.
default	기본값이 사용됩니다.
infinite	(선택 사항) 유효한 수명이 만료되지 않습니다.
ipv6-prefix	라우터 광고를 포함할 IPv6 네트워크 번호. 이 인수의 형식은 콜론 간에 16비트 값을 사용하는 16진수로 주소가 지정되는 RFC 2373의 규정을 따라야 합니다.
no-advertise	(선택 사항) 지정된 접두사가 IPv6 자동 컨피그레이션에 사용되지 않을 것임을 로컬 링크의 호스트에 알려줍니다.
no-autoconfig	(선택 사항) 지정된 접두사를 IPv6 자동 컨피그레이션에 사용할 수 없음을 로컬 링크의 호스트에 알려줍니다.
off-link	(선택 사항) 지정된 접두사가 온-링크 결정에 사용되지 않음을 알려줍니다.
preferred-lifetime	지정된 IPv6 접두사가 기본 접두사로서 광고되는 시간(초). 유효한 값은 0부터 4294967295초입니다. 최대값은 무한대에 해당하며 **infinite** 키워드로 지정할 수도 있습니다. 기본값은 604800(7일)입니다.
prefix-length	IPv6 접두사의 길이입니다. 이 값은 주소에서 얼마나 많은 상위 연속 비트가 접두사의 네트워크 부분을 구성하는지 나타냅니다. 슬래시(/)가 접두사 길이 앞에 와야 합니다.
valid-lifetime	지정된 IPv6 접두사가 유효한 접두사로서 광고되는 시간. 유효한 값은 0부터 4294967295초입니다. 최대값은 무한대에 해당하며 **infinite** 키워드로 지정할 수도 있습니다. 기본값은 2592000(30일)입니다.

기본값

IPv6 라우터 광고가 시작되는 인터페이스에 구성된 모든 접두사는 2592000초(30일)의 유효 수명 및 604800초(7일)의 기본 수명, 그리고 "onlink" 및 "autoconfig" 플래그 설정으로 광고됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 접두사 광고 여부를 포함하여 접두사별로 개별 매개변수를 제어할 수 있습니다.

기본적으로 **ipv6 address** 명령을 사용하여 인터페이스에서 주소로 구성된 접두사는 라우터 광고에서 광고됩니다. **ipv6 nd prefix** 명령을 사용하여 접두사를 구성할 경우 해당 접두사만 광고됩니다.

default 키워드는 모든 접두사에 대한 기본 매개변수 설정에 사용할 수 있습니다.

날짜는 접두사의 만료를 지정하도록 설정할 수 있습니다. 유효 수명과 기본 수명은 실시간으로 계산됩니다. 만료 날짜가 되면 접두사가 더 이상 광고되지 않습니다.

onlink가 "on"인 경우(기본값) 지정된 접두사가 링크에 할당됩니다. 지정된 접두사를 포함한 주소로 트래픽을 보내는 노드는 대상을 링크에서 로컬로 도달 가능한 것으로 간주합니다.

자동 컨피그레이션이 "on"인 경우(기본값) 지정된 접두사를 IPv6 자동 컨피그레이션에 사용할 수 있음을 호스트에 알려주는 것입니다.

예

다음 예는 지정된 인터페이스에서 전송되는 라우터 광고에 IPv6 접두사 2001:200::/35와 함께 유효한 수명 1000초, 기본 수명 900초를 포함합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

관련 명령

명령	설명
ipv6 address	인터페이스에서 IPv6 주소를 구성하고 IPv6 프로세싱을 활성화합니다.
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 nd ra-interval

인터페이스에서 IPv6 라우터 광고 전송 사이의 간격을 구성하려면 컨피그레이션 모드에서 **ipv6 nd ra-interval** 명령을 사용합니다. 기본 간격을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd ra-interval [**msec**] *value*

no ipv6 nd ra-interval [[**msec**] *value*]

구문 설명

msec	(선택 사항) 값이 밀리초 단위로 입력됨을 나타냅니다. 이 키워드가 없으면 값은 초 단위로 입력됩니다.
value	IPv6 라우터 광고 전송 사이의 간격. 유효한 값의 범위는 3~1800초 또는 **msec** 키워드가 있는 경우 500~1800000밀리초입니다. 기본값은 200초입니다.

기본값

200초

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA가 **ipv6 nd ra-lifetime** 명령을 사용하여 기본 라우터로 구성된 경우, 전송 사이의 간격은 IPv6 라우터 광고 수명보다 작거나 같아야 합니다. 다른 IPv6 노드와의 동기화를 방지하려면 사용되는 실제 값을 지정된 값의 20% 범위로 임의로 조정하십시오.

예

다음 예는 선택한 인터페이스에 대하여 IPv6 라우터 광고 간격을 201초로 설정합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

관련 명령

명령	설명
ipv6 nd ra-lifetime	IPv6 라우터 광고의 수명을 구성합니다.
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 nd ra-lifetime

인터페이스에서 IPv6 라우터 광고의 "라우터 수명" 값을 구성하려면 인터페이스 컨피그레이션 모드에서 **ipv6 nd ra-lifetime** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

구문 설명

seconds	이 인터페이스의 기본 라우터로서 ASA의 유효성. 유효한 값은 0~9000초입니다. 기본값은 1800초입니다. 0은 ASA를 선택한 인터페이스에서 기본 라우터로 간주하지 않아야 함을 나타냅니다.

기본값

1800초

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

"라우터 수명"은 인터페이스에서 전송된 모든 IPv6 라우터 광고에 포함됩니다. 이 값은 이 인터페이스에서 기본 라우터로서 ASA의 유용성을 나타냅니다.

0이 아닌 값은 ASA를 이 인터페이스의 기본값으로 간주해야 함을 나타냅니다. 0이 아닌 "라우터 수명" 값은 라우터 광고 간격보다 작으면 안 됩니다.

0인 값은 이 인터페이스에서 ASA를 기본 라우터로 간주하지 않아야 함을 나타냅니다.

예

다음 예는 선택한 인터페이스에 대하여 IPv6 라우터 광고 수명을 1801초로 설정합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 1801
```

관련 명령

명령	설명
ipv6 nd ra-interval	인터페이스에서 IPv6 라우터 광고 전송 사이의 간격을 구성합니다.
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 nd reachable-time

도달 가능성 확인 이벤트가 발생한 후 원격 IPv6 노드를 도달 가능한 것으로 간주하는 시간을 구성하려면 인터페이스 컨피그레이션 모드에서 **ipv6 nd reachable-time** 명령을 사용합니다. 기본 시간을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

구문 설명

value	원격 IPv6 노드가 도달 가능한 것으로 간주되는 시간(밀리초). 유효한 값은 0~3600000밀리초입니다. 기본값은 0입니다. *value* 인수로 0을 사용하는 경우 도달 가능 시간은 undetermined로 전송됩니다. 도달 가능한 시간 값을 설정하고 추적하는 것은 수신 디바이스에 달려 있습니다.

기본값

제로 밀리초

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

구성된 시간을 통해 사용할 수 없는 인접 디바이스를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 인접 디바이스를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.

ASA에서 사용하는 도달 가능한 시간을 보려면(이 명령을 0으로 설정한 경우의 실제 값 포함) **show ipv6 interface** 명령을 사용하여 IPv6 인터페이스에 대한 정보(사용되는 ND reachable 시간 포함)를 표시합니다.

예

다음 예는 선택한 인터페이스에 대해 IPv6 도달 가능 시간을 1700000밀리초로 구성합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd reachable-time 1700000
```

관련 명령

명령	설명
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 nd suppress-ra

LAN 인터페이스에서 IPv6 라우터 광고 전송을 억제하려면 인터페이스 컨피그레이션 모드에서 **ipv6 nd suppress-ra** 명령을 사용합니다. LAN 인터페이스에서 IPv6 라우터 광고 전송을 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

IPv6 유니캐스트 라우팅이 활성화되면 LAN 인터페이스에서 라우터 광고가 자동으로 전송됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

비 LAN 인터페이스 유형(예: serial 또는 tunnel 인터페이스)에서 IPv6 라우터 광고 전송을 활성화하려면 **no ipv6 nd suppress-ra** 명령을 사용합니다.

예

다음 예는 선택한 인터페이스에서 IPv6 라우터 광고를 억제합니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd suppress-ra
```

관련 명령

명령	설명
show ipv6 interface	IPv6에 대해 구성된 인터페이스의 사용성 상태를 표시합니다.

ipv6 neighbor

IPv6 인접 디바이스 검색 캐시에서 고정 엔트리를 구성하려면 글로벌 컨피그레이션 모드에서 **ipv6 neighbor** 명령을 사용합니다. 인접 디바이스 검색 캐시에서 고정 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

구문 설명

if_name	**nameif** 명령으로 지정하는 내부 또는 외부 인터페이스 이름입니다.
ipv6_address	로컬 데이터 링크 주소에 해당하는 IPv6 주소입니다.
mac_address	로컬 데이터 라인(하드웨어 MAC) 주소입니다.

기본값

고정 엔트리는 IPv6 인접 디바이스 검색 캐시에 구성되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

ipv6 neighbor 명령은 **arp** 명령과 유사합니다. 지정된 IPv6 주소에 대한 엔트리가 인접 디바이스 검색 캐시에 존재하는 경우(IPv6 인접 디바이스 검색 프로세스를 통해 학습) 이 엔트리는 고정 엔트리로 자동 변환됩니다. 이 엔트리는 컨피그레이션 저장을 위해 **copy** 명령이 사용될 때 컨피그레이션에 저장됩니다.

show ipv6 neighbor 명령을 사용하여 IPv6 인접 디바이스 검색 캐시의 고정 엔트리를 봅니다.

clear ipv6 neighbors 명령은 IPv6 인접 디바이스 검색 캐시에서 고정 엔트리를 제외한 모든 엔트리를 삭제합니다. **no ipv6 neighbor** 명령은 인접 디바이스 검색 캐시에서 특정 고정 엔트리를 삭제합니다. 이 명령은 동적 엔트리(IPv6 인접 디바이스 검색 프로세스에서 학습한 엔트리)를 캐시에서 삭제하지 않습니다. **no ipv6 enable** 명령을 사용하여 인터페이스에서 IPv6을 비활성화하면 고정 엔트리를 제외하고 해당 인터페이스에 대한 모든 IPv6 인접 디바이스 검색 캐시 엔트리가 삭제됩니다(엔트리 상태가 INCMP [Incomplete]로 변경됨).

IPv6 인접 디바이스 검색 캐시의 고정 엔트리는 인접 디바이스 검색 프로세스로 인해 변경되지 않습니다.

예

다음 예는 IPv6 주소가 3001:1::45A이고 MAC 주소가 0002.7D1A.9472인 내부 호스트에 대한 고정 엔트리를 인접 디바이스 검색 캐시에 추가합니다.

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

관련 명령

명령	설명
clear ipv6 neighbors	고정 엔트리를 제외하고, IPv6 인접 디바이스 검색 캐시의 모든 엔트리를 삭제합니다.
show ipv6 neighbor	IPv6 인접 디바이스 캐시 정보를 표시합니다.

ipv6 ospf

IPv6에 대해 OSPFv3 인터페이스 컨피그레이션을 활성화하려면 글로벌 컨피그레이션 모드에서 **ipv6 ospf** 명령을 사용합니다. IPv6에 대해 OSPFv3 인터페이스 컨피그레이션을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

no ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

구문 설명

cost	인터페이스에서 패킷을 전송하는 비용을 명시적으로 지정합니다.
database-filter	OSPFv3 인터페이스에 발신되는 LSA를 필터링합니다.
dead-interval *seconds*	인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간을 초 단위로 설정합니다. 이 값은 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다. 기본값은 **ipv6 ospf hello-interval** 명령으로 설정된 간격 집합의 4배입니다.
flood-reduction	인터페이스에 대한 LSA의 플러딩 감소를 지정합니다.
hello-interval *seconds*	인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. 이 값은 특정 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다. 기본 간격은 이더넷 인터페이스의 경우 10초이고, 비 브로드캐스트 인터페이스의 경우 30초입니다.
mtu-ignore	DBD 패킷이 수신될 때 OSPF MTU 불일치 감지를 비활성화합니다. OSPF MTU 불일치 감지는 기본적으로 활성화되어 있습니다.
neighbor	비 브로드캐스트 네트워크에 대한 OSPFv3 라우터 상호 연결을 구성합니다.
network	OSPF 네트워크 유형을 기본값 이외의 유형으로 설정하며, 이 경우 네트워크 유형에 따라 달라집니다.
priority	네트워크의 전용 라우터를 결정하는 데 도움이 되는 라우터 우선순위를 설정합니다. 유효한 값의 범위는 0~255입니다.
process-id	활성화할 OSPFv3 프로세스를 지정합니다. 유효한 값의 범위는 1~65535입니다.
retransmit-interval *seconds*	인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다. 이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 5초입니다.
transmit-delay *seconds*	인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 설정합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 1초입니다.

기본값

기본적으로 모든 IPv6 주소가 포함됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

OSPFv3 영역을 만들려면 우선 OSPFv3 라우팅 프로세스를 활성화해야 합니다.

예

다음 예는 OSPFv3 인터페이스 컨피그레이션을 활성화합니다.

```
ciscoasa(config)# ipv6 ospf 3
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf area

IPv6에 대한 OSPFv3 영역을 만들려면 글로벌 컨피그레이션 모드에서 **ipv6 ospf area** 명령을 사용합니다. IPv6에 대한 OSPFv3 영역 컨피그레이션을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf area [*area-num*] [**instance**]

no ipv6 ospf area [*area-num*] [**instance**]

구문 설명

area-num	활성화할 OSPFv3 영역을 지정합니다.
instance	인터페이스에 할당할 영역 인스턴스 ID를 지정합니다.

기본값

기본적으로 모든 IPv6 주소가 포함됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

각 인터페이스에서 OSPFv3 라우팅을 별도로 구성해야 합니다. 인터페이스당 OSPFv3 영역을 하나만 가질 수 있으며, ASA용 OSPFv3은 인터페이스당 하나의 인스턴스만 지원합니다. 각 인터페이스는 서로 다른 영역 인스턴스 ID를 사용합니다. 영역 인스턴스 ID는 OSPF 패킷의 수신에만 영향을 미치며, 일반 OSPF 인터페이스 및 가상 링크에 적용됩니다.

예

다음 예는 OSPFv3 인터페이스 컨피그레이션을 활성화합니다.

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf cost

인터페이스에서 패킷을 전송하는 비용을 명시적으로 지정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf cost** 명령을 사용합니다. 인터페이스에서 패킷을 전송하는 비용을 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf cost *interface-cost*

no ipv6 ospf cost *interface-cost*

구문 설명

interface-cost	링크 상태 메트릭으로 표시되는 무부호 정수 값을 지정하며, 입력 가능한 값의 범위는 1~65535입니다.

기본값

기본 비용은 대역폭을 기준으로 합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에 대한 패킷 비용을 명시적으로 지정하려면 이 명령을 사용합니다.

예

다음 예는 패킷 비용을 65로 설정합니다.

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf database-filter all out

OSPFv3 인터페이스에 대한 나가는 LSA를 필터링하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf database-filter all out** 명령을 사용합니다. 인터페이스에 대한 LSA의 전달을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf database-filter all out

no ipv6 ospf database-filter all out

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

모든 나가는 LSA는 인터페이스에 플러딩됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

OSPFv3 인터페이스에 대한 나가는 LSA를 필터링하려면 이 명령을 사용합니다.

예

다음 예는 지정된 인터페이스에 대한 나가는 LSA를 필터링합니다.

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf dead-interval

인접 디바이스에서 라우터가 다운되었음을 선언하기까지 hello 패킷이 표시되지 않는 기간을 설정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf dead-interval** 명령을 사용합니다. 기본 시간으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval *seconds*

구문 설명

seconds	간격을 초 단위로 지정합니다. 이 값은 네트워크의 모든 노드에서 동일해야 합니다. 유효한 값의 범위는 1~65535입니다.

기본값

기본값은 **ipv6 ospf hello-interval** 명령으로 설정된 간격 집합의 4배입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인접 디바이스에서 라우터가 다운되었음을 알리기까지 hello 패킷이 표시되지 않는 기간을 지정하려면 이 명령을 사용합니다.

예

다음 예는 Dead 간격을 60으로 설정합니다.

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf encryption

인터페이스의 암호화 유형을 지정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf encryption** 명령을 사용합니다. 인터페이스에서 암호화 유형을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

no ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

구문 설명

authentication-algorithm	사용할 암호화 알고리즘을 지정합니다. 유효한 값은 다음 중 하나입니다. • **md5** - 메시지 다이제스트 5(MD5)를 활성화합니다. • **sha1** - SHA-1을 활성화합니다.
encryption-algorithm	ESP와 함께 사용할 암호화 알고리즘을지정합니다. 유효한 값은 다음과 같습니다. • **aes-cdc** - AES-CDC 암호화를 활성화합니다. • **3des** - 3DES 암호화를 활성화합니다. • **des** - DES 암호화를 활성화합니다. • **null** - 암호화 없이 ESP를 지정합니다.
esp	ESP(Encapsulating Security Payload)를 지정합니다.
ipsec	IP 보안 프로토콜을 지정합니다.
key	메시지 다이제스트의 계산에 사용되는 숫자를 지정합니다. MD5 인증을 사용할 경우, 키는 32자 길이의 16진수 숫자(16바이트)여야 합니다. SHA-1 인증을 사용할 경우, 키는 40자 길이의 16진수 숫자(20바이트)여야 합니다.
key-encryption-type	(선택 사항) 키 암호화 유형을 다음 값 중 하나로 지정합니다. • **0** - 키가 암호화되지 않습니다. • **7** - 키가 암호화됩니다.
null	영역 인증을 재지정합니다.
spi *spi*	SPI(Security Policy Index) 값을 지정합니다. *spi* 값은 256~4294967295 범위의 십진수로 입력해야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에 대한 암호화 유형을 지정하려면 이 명령을 사용합니다.

예

다음 예는 인터페이스에서 SHA-1 암호화를 활성화합니다.

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf flood-reduction

인터페이스에 대한 LSA의 플러딩 감소를 지정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf flood-reduction** 명령을 사용합니다. 인터페이스에 대한 LSA의 플러딩 감소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf flood-reduction

no ipv6 ospf flood-reduction

구문 설명

이 명령에는 인수나 키워드가 없습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에 대한 LSA의 플러딩 감소를 지정하려면 이 명령을 사용합니다.

예

다음 예는 인터페이스에 대한 LSA의 플러딩 감소를 활성화합니다.

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 20.20.200.30 255.255.255.0 standby 20.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf hello-interval

인접 디바이스에서 라우터가 다운되었음을 선언하기까지 hello 패킷이 표시되지 않는 기간을 설정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf dead-interval** 명령을 사용합니다. 기본 시간으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval *seconds*

구문 설명

seconds	간격을 초 단위로 지정합니다. 이 값은 네트워크의 모든 노드에서 동일해야 합니다. 유효한 값의 범위는 1~65535입니다.

기본값

기본 간격이 이더넷을 사용하는 경우에는 10초, 비 브로드캐스트를 사용하는 경우에는 30초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인접 디바이스에서 라우터가 다운되었음을 알리기까지 hello 패킷이 표시되지 않는 기간을 지정하려면 이 명령을 사용합니다.

예

다음 예는 Dead 간격을 60으로 설정합니다.

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf mtu-ignore

ASA에서 DBD(Database Descriptor) 패킷을 수신할 때 OSPFv3 MTU(Maximum Transmission Unit) 불일치 감지를 비활성화하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf mtu-ignore** 명령을 사용합니다. ASA에서 DBD 패킷을 수신할 때 MTU 불일치 감지를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

OSPFv3 MTU 불일치 감지는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA에서 DBD 패킷을 수신할 때 OSPFv3 MTU 불일치 감지를 비활성화하려면 이 명령을 사용합니다.

예

다음 예는 ASA에서 DBD 패킷을 수신할 때 OSPFv3 MTU 불일치 감지를 비활성화합니다.

```
ciscoasa(config)# interface serial 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf mtu-ignore
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6 ospf neighbor

비 브로드캐스트 네트워크에 대한 OSPFv3 라우터 상호 연결을 구성하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf neighbor** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

구문 설명

cost *number*	(선택 사항) 1~65535의 정수 형식으로 인접 디바이스에 비용을 할당합니다. 비용이 특별히 구성되지 않은 인접 디바이스는 **ipv6 ospf cost** 명령을 기반으로 인터페이스의 비용을 가정하게 됩니다.
database-filter	(선택 사항) OSPF 인접 디바이스에 대한 나가는 LSA(링크 상태 광고)를 필터링합니다.
ipv6-address	인접 디바이스의 링크 로컬 IPv6 주소입니다. 이 인수의 형식은 콜론 간에 16비트 값을 사용하는 16진수로 주소가 지정되는 RFC 2373의 규정을 따라야 합니다.
poll-interval *seconds*	(선택 사항) 폴링 간격 시간(초)을 나타내는 숫자 값. RFC 2328에서는 이 값을 hello 간격보다 훨씬 크게 설정할 것을 권장합니다. 기본값은 120초(2분)입니다. point-to-multipoint 인터페이스에는 이 키워드가 적용되지 않습니다.
priority *number*	(선택 사항) 지정된 IPv6 접두사와 연결된 비 브로드캐스트 인접 디바이스의 라우터 우선순위 값을 나타내는 숫자. 기본값은 0입니다.

기본값

기본값은 네트워크 유형에 따라 다릅니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	•	•	•	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

비 브로드캐스트 네트워크에 대한 OSPFv3 라우터 상호 연결을 구성하려면 이 명령을 사용합니다.

예

다음 예는 OSPFv3 인접 라우터를 구성합니다.

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
ipv6 ospf priority	특정 네트워크의 지정된 라우터를 결정합니다.

ipv6 ospf network

OSPFv3 네트워크 유형을 기본값 이외의 유형으로 구성하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf network** 명령을 사용합니다. 기본 유형으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

no ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

구문 설명

broadcast	네트워크 유형을 broadcast로 설정합니다.
point-to-point non-broadcast	네트워크 유형을 point-to-point non-broadcast로 설정합니다.

기본값

기본값은 네트워크 유형에 따라 다릅니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

OSPFv3 네트워크 유형을 기본값 이외의 유형으로 구성하려면 이 명령을 사용합니다.

예

다음 예는 OSPFv3 네트워크를 브로드캐스트 네트워크로 설정합니다.

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf network broadcast
ciscoasa(config-if)# encapsulation frame-relay
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
ipv6 ospf priority	특정 네트워크의 지정된 라우터를 결정합니다.

ipv6 ospf priority

특정 네트워크에 대해 지정된 라우터를 결정하는 데 도움이 되는 라우터 우선순위를 설정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf priority** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf priority *number-value*

no ipv6 ospf priority *number-value*

구문 설명

number-value	라우터의 우선순위를 지정하는 숫자 값을 설정합니다. 유효한 값의 범위는 0~255입니다.

기본값

기본 우선순위는 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

라우터의 우선순위를 설정하려면 이 명령을 사용합니다.

예

다음 예는 라우터의 우선순위를 4로 설정합니다.

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ipv6 ospf priority 4
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
ipv6 ospf retransmit-interval	인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 지정합니다.

ipv6 ospf retransmit-interval

인터페이스에 속하는 인접성에 대해 LSA 재전송 사이의 시간을 지정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf retransmit-interval** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval *seconds*

구문 설명

seconds	재전송 사이의 시간(초)을 지정합니다. 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1~65535초입니다.

기본값

기본값은 5초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 지정하려면 이 명령을 사용합니다.

예

다음 예는 재전송 간격을 8초로 설정합니다.

```
ciscoasa(config)# interface ethernet 2
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf retransmit-interval 8
```

관련 명령

명령	설명
ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
ipv6 ospf priority	특정 네트워크의 지정된 라우터를 결정합니다.

ipv6 ospf transmit-delay

인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 설정하려면 인터페이스 컨피그레이션 모드에서 **ipv6 ospf transmit-delay** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

ipv6 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay *seconds*

구문 설명

seconds	링크 상태 업데이트를 전송하는 데 필요한 시간(초)을 지정합니다. 유효한 값의 범위는 1~65535초입니다.

기본값

기본값은 1초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 설정하려면 이 명령을 사용합니다.

예

다음 예는 재전송 지연을 3초로 설정합니다.

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf transmit-delay 3
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 삭제합니다.
ipv6 ospf priority	특정 네트워크의 지정된 라우터를 결정합니다.

ipv6 route

IPv6 라우팅 테이블에 IPv6 경로를 추가하려면 글로벌 컨피그레이션 모드에서 **ipv6 route** 명령을 사용합니다. IPv6 기본 경로를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

no ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

구문 설명

administrative-distance	(선택 사항) 경로의 관리 거리입니다. 기본값은 1입니다. 이 경우 고정 경로가 연결된 경로를 제외한 다른 모든 유형의 경로에 우선합니다.
if_name	경로가 구성되는 인터페이스의 이름입니다.
ipv6-address	지정된 네트워크에 도달하기 위해 사용할 수 있는 next hop의 IPv6 주소입니다.
ipv6-prefix	고정 경로의 대상인 IPv6 네트워크입니다. 이 인수의 형식은 콜론 간에 16비트 값을 사용하는 16진수로 주소가 지정되는 RFC 2373의 규정을 따라야 합니다.
prefix-length	IPv6 접두사의 길이입니다. 이 값은 주소에서 얼마나 많은 상위 연속 비트가 접두사의 네트워크 부분을 구성하는지 나타냅니다. 슬래시(/)가 접두사 길이 앞에 와야 합니다.
tunneled	(선택 사항) VPN 트래픽에 대한 기본 터널 게이트웨이로 경로를 지정합니다.

기본값

기본적으로 관리 거리는 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(1)	투명 방화벽 모드 지원이 추가되었습니다.

사용 지침

IPv6 라우팅 테이블의 내용을 보려면 **show ipv6 route** 명령을 사용합니다.

표준 기본 경로를 가지고 터널링된 트래픽을 위한 별도의 기본 경로를 정의할 수 있습니다. **tunneled** 옵션으로 기본 경로를 생성하면 학습 경로나 고정 경로를 이용하여 라우팅할 수 없는 ASA에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다. 터널에서 발생하는 트래픽에 대해 이 경로는 다른 구성된 또는 학습된 기본 경로를 재지정합니다.

tunneled 옵션을 포함한 기본 경로에는 다음 제한 사항이 적용됩니다.

- 터널링 경로의 이그레스 인터페이스에서 유니캐스트 RPF(**ip verify reverse-path** 명령)를 활성화하지 마십시오. 터널링 경로의 이그레스 인터페이스에서 uRPF를 활성화하면 세션이 실패합니다.
- 터널링 경로의 이그레스 인터페이스에서 TCP 인터셉트를 활성화하지 마십시오. 그렇게 할 경우 세션이 실패하게 됩니다.
- VoIP 검사 엔진(CTIQBE, H.323, GTP, MGCP, RTSP, SIP 또는 SKINNY), DNS 검사 엔진 또는 DCE RPC 검사 엔진을 터널링 경로에 사용하지 마십시오. 이러한 검사 엔진은 터널링 경로를 무시합니다.

tunneled 옵션으로 두 개 이상의 기본 경로를 정의할 수 없습니다. 터널링 트래픽에 대한 ECMP는 지원되지 않습니다.

예

다음 예제에서는 네트워크 7fff::0/32의 패킷을 3FFE:1100:0:CC00::1에 위치한 관리 거리가 110인 내부 인터페이스의 네트워킹 디바이스로 라우팅합니다.

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

관련 명령

명령	설명
debug ipv6 route	IPv6 라우팅 테이블 업데이트 및 경로 캐시 업데이트에 대한 디버깅 메시지를 표시합니다.
show ipv6 route	IPv6 라우팅 테이블의 현재 내용을 표시합니다.

ipv6 router ospf

OSPFv3 라우팅 프로세스를 만들고 IPv6 라우터 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **ipv6 router ospf** 명령을 사용합니다.

ipv6 router ospf *process-id*

구문 설명

process-id	로컬에서 할당되며 1~65535 범위의 양의 정수인 내부 ID를 지정합니다. 이 번호는 IPv6 라우팅 프로세스용 OSPFv3을 활성화할 때 관리상 할당되는 번호입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

ipv6 router ospf 명령은 ASA에서 실행 중인 OSPFv3 라우팅 프로세스를 위한 글로벌 컨피그레이션 명령입니다. **ipv6 router ospf** 명령을 입력하면 명령 프롬프트가 (config-rtr)#으로 표시되는데, 이는 IPv6 라우터 컨피그레이션 모드에 있음을 나타냅니다.

no ipv6 router ospf 명령을 사용할 경우, 필요한 정보를 제공하지 않는 한 선택적인 인수를 지정할 필요가 없습니다. **no ipv6 router ospf** 명령은 *process-id* 인수로 지정한 OSPFv3 라우팅 프로세스를 종료합니다. *process-id* 값은 ASA에서 로컬로 할당합니다. 각 OSPFv3 라우팅 프로세스에 고유한 값을 할당해야 합니다. 최대 2개의 프로세스를 사용할 수 있습니다.

다음의 OSPFv3 관련 옵션으로 OSPFv3 라우팅 프로세스를 구성하려면 IPv6 라우터 컨피그레이션 모드에서 **ipv6 router ospf** 명령을 사용합니다.

- **area** - OSPFv3 영역 매개변수를 구성합니다. 지원되는 매개변수에는 십진수 숫자(0~4294967295)로 된 영역 ID 및 IP 주소 형식(**A.B.C.D**)으로 된 영역 ID가 포함됩니다.
- **default** - 명령을 기본값으로 설정합니다. **originate** 매개변수는 기본 경로를 배포합니다.
- **default-information** - 기본 정보의 배포를 제어합니다.
- **distance** - 경로 유형을 기준으로 OSPFv3 경로 관리 영역을 정의합니다. 지원되는 매개변수에는 관리 영역 값(1~254) 및 OSPF 영역에 대한 **ospf**가 포함됩니다.
- **exit** - IPv6 라우터 컨피그레이션 모드로 들어갑니다.

- **ignore** - 라우터에 Type 6 Multicast OSPF(MOSPF)에 대한 링크 상태 광고(LSA)가 수신될 경우, **lsa** 매개변수를 사용하여 syslog 메시지가 전송되는 것을 억제합니다.
- **log-adjacency-changes** - OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다. **detail** 매개변수를 사용하면 모든 상태 변경 사항이 기록됩니다.
- **passive-interface** - 다음 매개변수로 인터페이스에서 라우팅 업데이트를 억제합니다.
  - **GigabitEthernet** - GigabitEthernet IEEE 802.3z 인터페이스를 지정합니다 .
  - **Management** - 관리 인터페이스를 지정합니다 .
  - **Port-channel** - 인터페이스의 이더넷 채널을 지정합니다 .
  - **Redundant** - 이중화 인터페이스를 지정합니다 .
  - **default** - 모든 인터페이스에서 라우팅 업데이트를 억제합니다 .
- **redistribute** - 다음 매개변수에 따라 하나의 라우팅 도메인에서 다른 도메인으로 경로를 재배포하도록 구성합니다.
  - **connected** - 연결된 경로를 지정합니다 .
  - **ospf** - OSPF 경로를 지정합니다 .
  - **static** - 고정 경로를 지정합니다 .
- **router-id** - 다음 매개변수를 사용하여 지정된 프로세스에 대한 고정 라우터 ID를 생성합니다.
  - **A.B.C.D** - OSPF 라우터 ID 를 IP 주소 형식으로 지정합니다 .
  - **cluster-pool** - Layer 3 클러스터링이 구성될 때 IP 주소 풀을 구성합니다 .
- **summary-prefix** - IPv6 주소 요약을 0~128 사이의 유효한 값으로 구성합니다. **X:X:X:X::X/** 매개변수는 IPv6 접두사를 지정합니다.
- **timers** - 다음 매개변수를 사용하여 라우팅 타이머를 조정합니다.
  - **lsa** - OSPF LSA 타이머를 지정합니다 .
  - **pacing** - OSPF 속도 타이머를 지정합니다 .
  - **throttle** - OSPF 속도 제한 타이머를 지정합니다 .

예

다음 예는 OSPFv3 라우팅 프로세스를 활성화하고 IPv6 라우터 컨피그레이션 모드로 들어갑니다.

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)#
```

관련 명령

명령	설명
clear ipv6 ospf	OSPFv3 라우팅 프로세스에서 모든 IPv6 설정을 제거합니다.
debug ospfv3	OSPFv3 라우팅 프로세스의 문제 해결을 위한 디버깅 정보를 제공합니다.

ipv6-address-pool(tunnel-group general attributes mode)

원격 클라이언트에 주소를 할당하기 위한 IPv6 주소 풀 목록을 지정하려면 tunnel-group general-attributes 컨피그레이션 모드에서 **ipv6-address-pool** 명령을 사용합니다. IPv6 주소 풀을 없애려면 이 명령의 **no** 형식을 사용합니다.

ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

구문 설명

interface_name	(선택 사항) 주소 풀에 사용할 인터페이스를 지정합니다.
ipv6_address_pool	**ipv6 local pool** 명령으로 구성한 주소 풀의 이름을 지정합니다. 최대 6개의 로컬 주소 풀을 지정할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group general attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

이러한 각 명령을 인터페이스당 하나씩 여러 번 입력할 수 있습니다. 인터페이스를 지정하지 않으면, 명시적으로 참조되지 않은 모든 인터페이스에 대한 기본값이 지정됩니다.

group-policy **ipv6-address-pools** 명령의 IPv6 주소 풀 설정은 tunnel group **ipv6-address-pool** 명령의 IPv6 주소 풀 설정을 재지정합니다.

풀을 지정하는 순서는 중요합니다. ASA는 이러한 풀에서 명령에 풀이 나타나는 순서대로 주소를 할당합니다.

예

tunnel-group general-attributes 컨피그레이션 모드에서 입력하는 다음 예는 IPsec 원격 액세스 터널 그룹 테스트용 원격 클라이언트에 주소를 할당하기 위한 IPv6 주소 풀의 목록을 지정합니다.

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general-attributes
ciscoasa(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
ipv6addrpool3
ciscoasa(config-tunnel-general)#
```

관련 명령

명령	설명
ipv6-address-pools	그룹 정책용 IPv6 주소 풀 설정을 구성합니다. 이러한 설정은 터널 그룹용 설정을 재지정합니다.
ipv6 local pool	VPN 원격 액세스 터널에 사용할 IP 주소 풀을 구성합니다.
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 컨피그레이션을 보여줍니다.
tunnel-group	터널 그룹을 구성합니다.

ipv6-address-pools

원격 클라이언트에 주소를 할당하는 데 사용할 최대 6개 IPv6 주소 풀의 목록을 지정하려면 group-policy 특성 컨피그레이션 모드에서 **ipv6-address-pools** 명령을 사용합니다. 그룹 정책에서 특성을 제거하고 다른 그룹 정책 소스로부터의 상속을 활성화하려면 이 명령의 **no** 형식을 사용합니다.

ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

ipv6-address-pools none

no ipv6-address-pools none

구문 설명

ipv6_address_pool	**ipv6 local pool** 명령으로 구성한 최대 6개 IPv6 주소 풀의 이름을 지정합니다. IPv6 주소 풀 이름을 구분하는 데에는 공백을 사용합니다.
none	구성된 IPv6 주소 풀이 없음을 지정하고, 다른 그룹 정책 소스로부터의 상속을 비활성화합니다.
value	주소를 할당하는 데 사용할 최대 6개 IPv6 주소 풀의 목록을 지정합니다.

기본값

기본적으로 IPv6 주소 풀 특성은 구성되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Group-policy 특성 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

IPv6 주소 풀을 구성하려면 **ipv6 local pool** 명령을 사용합니다.

ipv6-address-pools 명령에서 풀을 지정하는 순서는 중요합니다. ASA는 이러한 풀에서 명령에 풀이 나타나는 순서대로 주소를 할당합니다.

ipv6-address-pools none 명령은 다른 정책 소스(예: DefaultGrpPolicy)에서 상속하는 이러한 특성을 비활성화합니다. **no ipv6-address-pools none** 명령은 컨피그레이션에서 **ipv6-address-pools none** 명령을 제거하고, 상속을 허용하는 기본값을 복원합니다.

예

group-policy 특성 컨피그레이션 모드에서 입력하는 다음 예는 원격 클라이언트에 주소를 할당하는 데 사용할 firstipv6pool이라는 IPv6 주소 풀을 구성한 다음, 해당 풀을 GroupPolicy1과 연결합니다.

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# ipv6-address-pools value firstipv6pool
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
ipv6 local pool	VPN 그룹 정책에 사용할 IPv6 주소 풀을 구성합니다.
clear configure group-policy	구성된 모든 그룹 정책을 지웁니다.
show running-config group-policy	모든 그룹 정책 또는 특정 그룹 정책에 대한 컨피그레이션을 보여줍니다.

ipv6-split-tunnel-policy

IPv6 스플릿 터널링 정책을 설정하려면 group-policy 컨피그레이션 모드에서 **ipv6-split-tunnel-policy** 명령을 사용합니다. 실행 중인 컨피그레이션에서 ipv6-split-tunnel-policy 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

구문 설명

excludespecified	트래픽이 암호화 없이 통과할 네트워크 목록을 정의합니다. 이 기능은 터널을 통해 회사 네트워크에 연결하는 원격 사용자가 로컬 네트워크(예: 프린터)의 디바이스에 액세스하려는 경우 유용합니다.
ipv6-split-tunnel-policy	터널링 트래픽을 위한 규칙을 설정 중임을 나타냅니다.
tunnelall	어떤 트래픽도 암호화 없이는 통과할 수 없음을 또는 ASA 이외의 다른 목적지로는 이동할 수 없음을 지정합니다. 원격 사용자는 회사 네트워크를 통해 인터넷 네트워크에 도달하며 로컬 네트워크에는 액세스할 수 없습니다.
tunnelspecified	지정한 네트워크에서 나오거나 네트워크로 들어가는 모든 트래픽을 터널링합니다. 이 옵션은 스플릿 터널링을 활성화합니다. 이 옵션을 이용하면 터널링할 네트워크 주소 목록을 생성할 수 있습니다. 다른 모든 주소로 향하는 데이터는 암호화 없이 이동하며, 원격 사용자의 인터넷 서비스 공급자에 의해 라우팅됩니다.

기본값

IPv6 스플릿 터널링은 기본적으로 비활성화되어 있습니다(**tunnelall**).

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

IPv6 스플릿 터널링은 기본적으로 보안 기능이 아니라 트래픽 관리 기능입니다. 실제로 최적의 보안을 유지하려면 IPv6 스플릿 터널링을 활성화하지 않는 것이 좋습니다.

이 명령은 다른 그룹 정책으로부터 IPv6 스플릿 터널링의 값을 상속하도록 허용합니다.

IPv6 스플릿 터널링을 사용하면 원격 액세스 VPN 클라이언트는 IPsec 또는 SSL IPv6 터널을 통과하는 경우 암호화된 형식으로, 네트워크 인터페이스에서는 암호화되지 않은 형식으로 패킷을 조건부로 전달할 수 있습니다. IPv6 스플릿 터널링이 활성화되면 IPsec 또는 SSL VPN 터널 엔드포인트의 다른 쪽에 있는 목적지로 바인딩되지 않은 패킷은 암호화하거나, 터널을 통해 전송하거나, 암호 해독하거나, 최종 목적지로 라우팅할 필요가 없습니다.

이 명령은 특정 네트워크에 IPv6 스플릿 터널링 정책을 적용합니다.

예

다음 예는 FirstGroup이라는 그룹 정책에 대해 지정된 네트워크만을 터널링하는 스플릿 터널링 정책을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

관련 명령

명령	설명
split-tunnel-network-list none	스플릿 터널링용 액세스 목록이 없음을 나타냅니다. 모든 트래픽이 터널을 통과합니다.
split-tunnel-network-list value	터널링을 요구하는 네트워크와 그렇지 않은 네트워크를 구분하기 위해 ASA에서 사용하는 액세스 목록을 식별합니다.

ipv6-vpn-address-assign

원격 액세스 클라이언트에 IPv6 주소를 할당하는 방법을 지정하려면 글로벌 컨피그레이션 모드에서 **ipv6-vpn-addr-assign** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 구성된 모든 VPN 주소 할당 방법을 ASA에서 제거하려면 인수 없이 이 명령의 **no** 형식을 사용합니다.

ipv6-vpn-addr-assign {**aaa** | **local** }

no ipv6-vpn-addr-assign {**aaa** | **local** }

구문 설명

aaa	ASA는 외부 또는 내부(LOCAL) AAA(인증, 권한 부여 및 어카운팅)에서 사용자 단위로 주소를 검색합니다. IP 주소가 구성된 인증 서버를 사용하는 경우 이 방법을 사용하는 것이 좋습니다.
local	ASA가 내부에서 구성된 주소 풀로부터 IPv6 주소를 배포합니다.

기본값

AAA 및 local vpn 주소 할당 옵션이 모두 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA는 원격 액세스 클라이언트에 IPv6 주소를 할당하는 데 AAA 또는 local 방법 중 하나를 사용할 수 있습니다. 둘 이상의 주소 할당 방법을 구성하면 ASA는 IPv6 주소를 찾을 때까지 각 옵션을 검색합니다.

예

다음 예는 주소 할당 방법으로서 AAA를 구성하는 방법을 보여줍니다.

예
```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

다음 예는 주소 할당 방법으로 로컬 주소 풀을 사용하도록 구성하는 방법을 보여줍니다.

예
```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

관련 명령

명령	설명
ipv6 local pool	VPN 그룹 정책에 사용할 IPv6 주소 풀을 구성합니다.
show running-config group-policy	모든 그룹 정책 또는 특정 그룹 정책에 대한 컨피그레이션을 보여줍니다.
vpn-addr-assign	원격 액세스 클라이언트에 IPv4 주소를 할당하기 위한 방법을 지정합니다.

ipv6-vpn-filter

VPN 연결에 사용할 IPv6 ACL의 이름을 지정하려면 group-policy 컨피그레이션 또는 사용자 이름 컨피그레이션 모드에서 **ipv6-vpn-filter** 명령을 사용합니다. **ipv6-vpn-filter none** 명령을 사용하여 만드는 null 값을 포함하여 ACL을 제거하려면 이 명령의 no 형식을 사용합니다.

ipv6-vpn-filter {**value** *IPV6-ACL-NAME* | **none**}

no ipv6-vpn-filter

구문 설명

none	액세스 목록이 없음을 나타냅니다. Null 값을 설정하여 액세스 목록을 허용하지 않습니다. 다른 그룹 정책으로부터의 액세스 목록 상속을 차단합니다.
value *IPV6-ACL-NAME*	전에 구성된 액세스 목록의 이름을 제공합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.
9.0(1)	**ipv6-vpn-filter** 명령이 사용 중단되었습니다. IPv4 및 IPv6 엔트리와 함께 통합 필터를 구성하려면 **vpn-filter** 명령을 사용해야 합니다. **vpn-filter** 명령으로 지정한 액세스 목록에 IPv6 엔트리가 없는 경우에만 이 IPv6 필터가 사용됩니다.
9.1(4)	**ipv6-vpn-filter** 명령이 비활성화되었고, 명령의 "no" 형식만 허용됩니다. IPv4 및 IPv6 엔트리용 통합 필터를 구성하려면 **vpn-filter** 명령을 사용해야 합니다. IPv6 ACL을 지정하는 데 실수로 이 명령을 사용하면 연결이 종료됩니다.

사용 지침

클라이언트리스 SSL VPN은 **ipv6-vpn-filter** 명령으로 정의한 ACL을 사용하지 않습니다.

no 옵션은 다른 그룹 정책으로부터 값을 상속하도록 허용합니다. 값의 상속을 차단하려면 **ipv6-vpn-filter none** 명령을 사용합니다.

이 사용자 또는 그룹 정책에 대한 각종 트래픽 유형을 허용하거나 거부하도록 ACL을 구성합니다. 그런 다음 **ipv6-vpn-filter** 명령을 사용하여 이러한 ACL을 적용합니다.

예

다음 예는 FirstGroup이라는 그룹 정책에 대해 ipv6_acl_vpn이라는 액세스 목록을 호출하는 필터를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipv6-vpn-filter value ipv6_acl_vpn
```

관련 명령

명령	설명
access-list	액세스 목록을 만들거나 다운로드 가능한 액세스 목록을 사용합니다.
vpn-filter	VPN 연결에 사용할 IPv4 또는 IPv6 ACL의 이름을 지정합니다.

5 장

isakmp am-disable부터 issuer-name까지의 명령

isakmp am-disable

인바운드 어그레시브 모드 연결을 비활성화하려면 글로벌 컨피그레이션 모드에서 **isakmp am-disable** 명령을 사용합니다. 인바운드 어그레시브 모드 연결을 활성화하려면 이 명령의 **no** 형식을 사용합니다.

isakmp am-disable

no isakmp am-disable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본값은 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp am-disable** 명령이 이 명령을 대체했습니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 인바운드 어그레시브 모드 연결을 비활성화합니다.

```
ciscoasa(config)# isakmp am-disable
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp disconnect-notify

피어에게 연결 끊김을 알리는 기능을 활성화하려면 글로벌 컨피그레이션 모드에서 **isakmp disconnect-notify** 명령을 사용합니다. 연결 끊김 알림을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

isakmp disconnect-notify

no isakmp disconnect-notify

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본값은 활성화되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp disconnect-notify** 명령이 이 명령을 대체했습니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 피어에게 연결 끊김을 알리는 기능을 활성화합니다.

```
ciscoasa(config)# isakmp disconnect-notify
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp enable

IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화하려면 글로벌 컨피그레이션 모드에서 **isakmp enable** 명령을 사용합니다. 인터페이스에서 ISAKMP를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

isakmp enable *interface-name*

no isakmp enable *interface-name*

구문 설명

interface-name	ISAKMP 협상을 활성화 또는 비활성화할 인터페이스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp enable** 명령이 이 명령을 대체했습니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 내부 인터페이스에서 ISAKMP를 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# no isakmp enable inside
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp identity

Phase 2 ID를 피어에게 전송하도록 설정하려면 글로벌 컨피그레이션 모드에서 **isakmp identity** 명령을 사용합니다. 기본 설정으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

no isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

구문 설명

address	ISAKMP 아이덴티티 정보를 교환하는 호스트의 IP 주소를 사용합니다.
auto	사전 공유 키용 IP 주소 또는 인증서용 인증 DN 중 어떤 연결 유형인지에 따라 ISKMP 협상을 결정합니다.
hostname	ISAKMP 아이덴티티 정보를 교환하는 호스트의 정규화된 도메인 이름을 사용합니다(기본값). 이 이름은 호스트 이름 및 도메인 이름으로 구성됩니다.
key-id *key_id_string*	원격 피어에서 사전 공유 키를 조회하는 데 사용하는 문자열을 지정합니다.

기본값

기본 ISAKMP 아이덴티티는 **isakmp identity hostname** 명령입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp identity** 명령이 이 명령을 대체했습니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 연결 유형에 따라 IPsec 피어와 통신할 수 있도록 인터페이스에서 ISAKMP 협상을 활성화합니다.

```
ciscoasa(config)# isakmp identity auto
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp ipsec-over-tcp

IPsec over TCP를 활성화하려면 글로벌 컨피그레이션 모드에서 **isakmp ipsec-over-tcp** 명령을 사용합니다. IPsec over TCP를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

구문 설명

port *port1...port10*	(선택 사항) 디바이스가 IPsec over TCP 연결을 허용하는 포트를 지정합니다. 포트를 최대 10개까지 지정할 수 있습니다. 포트 번호의 범위는 1~65535입니다. 기본 포트 번호는 10000입니다.

기본값

기본값은 활성화되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp ipsec-over-tcp** 명령이 이 명령을 대체했습니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 포트 45에서 IPsec over TCP를 활성화합니다.

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp keepalive

IKE keepalive를 구성하려면 tunnel-group ipsec-attributes 구성 모드에서 **isakmp keepalive** 명령을 사용합니다. 기본 임계값 및 재시도 값과 함께 keepalive 파라미터를 재활성화하려면 이 명령의 **no** 형식을 사용합니다.

isakmp keepalive [threshold *seconds* **| infinite] [retry** *seconds*] [**disable]**

no isakmp keepalive disable [threshold *seconds* **| infinite] [retry** *seconds*] [**disable]**

구문 설명

disable	기본적으로 활성화되어 있는 IKE keepalive 프로세싱을 비활성화합니다.
infinite	ASA에서 keepalive 모니터링을 시작하지 않습니다.
retry *seconds*	keepalive 응답을 수신하지 못했을 경우 재시도 사이의 간격을 초 단위로 지정합니다. 범위는 2~10초입니다. 기본값은 2초입니다.
threshold *seconds*	keepalive 모니터링을 시작하기 전 피어가 유휴 상태로 머물 수 있는 기간을 초 단위로 지정합니다. 범위는 10~3600초입니다. 기본값은 LAN-to-LAN 그룹에서는 10초, 원격 액세스 그룹에서는 300초입니다.

기본값

원격 액세스 그룹의 경우 기본값은 임계값 300초, 재시도 2초입니다.

LAN-to-LAN 액세스 그룹의 경우 기본값은 임계값 10초, 재시도 2초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Tunnel-group ipsec-attributes 구성	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

모든 터널 그룹에서 IKE keepalive는 기본 임계값 및 재시도 값과 함께 기본적으로 활성화되어 있습니다. 이 특성은 IPsec 원격 액세스 그룹 및 IPsec LAN-to-LAN 터널 그룹 유형에만 적용할 수 있습니다.

예

다음 예는 tunnel-group ipsec-attributes 구성 모드에서 입력하여 IKE DPD를 구성하고, 임계값을 15로 설정하고, IP 주소 209.165.200.225의 IPsec LAN-to-LAN 터널 그룹의 재시도 간격을 10으로 지정합니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
ciscoasa(config-tunnel-ipsec)#
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 구성을 보여줍니다.
tunnel-group ipsec-attributes	이 그룹에 대한 터널 그룹 IPsec 특성을 구성합니다.

isakmp nat-traversal

NAT traversal을 전체적으로 활성화하려면, 글로벌 컨피그레이션 모드에서 ISAKMP가 활성화되어 있는지 확인한 다음(**isakmp enable** 명령으로 활성화할 수 있음) **isakmp nat-traversal** 명령을 사용합니다. NAT traversal이 활성화되어 있는 경우 다시 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

구문 설명

natkeepalive	NAT keepalive 간격을 10~3600초 범위로 설정합니다. 기본값은 20초입니다.

기본값

기본적으로 NAT traversal(**isakmp nat-traversal** 명령)은 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp nat-traversal** 명령이 이 명령을 대체했습니다.

사용 지침

PAT(Port Address Translation)를 비롯한 NAT(Network Address Translation)는 여러 네트워크에서 사용되고 있습니다. 여기서는 IPsec도 사용되지만, NAT 디바이스 간 IPsec 패킷의 성공적 이동을 방해하는 여러 비호환성 문제가 있습니다. NAT traversal을 사용하면 ESP 패킷이 하나 이상의 NAT 디바이스를 통과할 수 있습니다.

ASA는 http://www.ietf.org/html.charters/ipsec-charter.html에서 이용 가능한 IETF "UDP Encapsulation of IPsec Packets" 초안의 버전 2 및 버전 3에 설명된 대로 NAT traversal을 지원하며, NAT traversal은 동적 및 고정 crypto 맵에서 모두 지원됩니다.

이 명령은 ASA에서 NAT-T를 전체적으로 활성화합니다. crypto-map 엔트리를 비활성화하려면 **crypto map set nat-t-disable** 명령을 사용합니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 ISAKMP를 활성화한 다음, 30초의 간격으로 NAT traversal을 활성화합니다.

```
ciscoasa(config)# isakmp enable
ciscoasa(config)# isakmp nat-traversal 30
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp policy authentication

IKE 정책 내에서 인증 방법을 지정하려면 글로벌 컨피그레이션 모드에서 **isakmp policy authentication** 명령을 사용합니다. ISAKMP 인증 방법을 제거하려면 **clear configure** 명령을 사용합니다.

isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

구문 설명

crack	인증 방법으로 IKE CRACK(Challenge/Response for Authenticated Cryptographic Keys)을 지정합니다.
pre-share	인증 방법으로 사전 공유 키를 지정합니다.
priority	IKE 정책을 고유하게 식별하고 정책에 우선순위를 할당합니다. 1~65,534 범위의 정수를 사용합니다. 1은 가장 높은 우선순위이고 65,534는 가장 낮은 우선순위입니다.
rsa-sig	인증 방법으로 RSA 서명을 사용합니다. RSA 서명은 IKE 협상에 대한 부인 방지를 제공합니다. 즉, 사용자는 피어와 IKE 협상을 수행했는지 여부를 제3자에게 입증할 수 있습니다.

기본값

기본 ISAKMP 정책 인증은 **pre-share** 옵션입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

IKE 정책은 IKE 협상을 위한 파라미터의 집합을 정의합니다. RSA 서명을 지정하는 경우 CA(Certification Authority)에서 인증서를 받을 수 있도록 ASA 및 해당 피어를 구성해야 합니다. 사전 공유 키를 지정하는 경우 ASA 및 해당 피어 내에서 이러한 사전 공유 키를 별도로 구성해야 합니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 IKE 정책 내에서 RSA 서명의 인증 방법을 우선순위 번호 40으로 사용하도록 설정합니다.

```
ciscoasa(config)# isakmp policy 40 authentication rsa-sig
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp policy encryption

IKE 정책 내에서 암호화 알고리즘을 사용하도록 지정하려면 글로벌 컨피그레이션 모드에서 **isakmp policy encryption** 명령을 사용합니다. 암호와 알고리즘을 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

구문 설명

3des	IKE 정책에서 Triple DES 암호화 알고리즘을 사용하도록 지정합니다.
aes	IKE 정책에서 사용할 암호화 알고리즘을 128비트 키의 AES로 지정합니다.
aes-192	IKE 정책에서 사용할 암호화 알고리즘을 192비트 키의 AES로 지정합니다.
aes-256	IKE 정책에서 사용할 암호화 알고리즘을 256비트 키의 AES로 지정합니다.
des	IKE 정책에서 사용할 암호화 알고리즘을 56비트 DES-CBC로 지정합니다.
priority	IKE 정책을 고유하게 식별하고 정책에 우선순위를 할당합니다. 1~65,534 범위의 정수를 사용합니다. 1은 가장 높은 우선순위이고 65,534는 가장 낮은 우선순위입니다.

기본값

기본 ISAKMP 정책 암호화는 **3des**입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp policy encryption** 명령이 이 명령을 대체했습니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 IKE 정책 내에서 128비트 키의 AES 암호화 알고리즘을 우선순위 번호 25로 사용하도록 설정합니다.

```
ciscoasa(config)# isakmp policy 25 encryption aes
```

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 IKE 정책 내에서 3DES 알고리즘을 우선순위 번호 40으로 사용하도록 설정합니다.

```
ciscoasa(config)# isakmp policy 40 encryption 3des
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp policy group

IKE 정책용 Diffie-Hellman group을 지정하려면 글로벌 컨피그레이션 모드에서 **isakmp policy group** 명령을 사용합니다. Diffie-Hellman group 식별자를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

isakmp policy *priority* **group** {**1** | **2** | **5**}

no isakmp policy *priority* **group**

구문 설명

group 1	IKE 정책에서 768비트 Diffie-Hellman group이 사용되도록 지정합니다. 이것이 기본값입니다.
group 2	IKE 정책에서 1024비트 Diffie-Hellman group 2가 사용되도록 지정합니다.
group 5	IKE 정책에서 1536비트 Diffie-Hellman group 5가 사용되도록 지정합니다.
priority	IKE(Internet Key Exchange) 정책을 고유하게 식별하고 정책에 우선순위를 할당합니다. 1~65,534 범위의 정수를 사용합니다. 1은 가장 높은 우선순위이고 65,534는 가장 낮은 우선순위입니다.

기본값

기본값은 group 2입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다. Group 7이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp policy group** 명령이 이 명령을 대체했습니다.
8.0(4)	**group 7** 명령 옵션은 사용이 중단되었습니다. group 7을 구성하려고 시도하면 오류 메시지가 표시되고 group 5가 대신 사용됩니다.

사용 지침

IKE 정책은 IKE 협상 중 사용할 파라미터의 집합을 정의합니다.

세 가지 그룹 옵션, 즉 768비트(DH Group 1), 1024비트(DH Group 2), 1536비트(DH Group 5)가 있습니다. 1024비트 및 1536비트 Diffie-Hellman Group은 더 강력한 보안을 제공하지만, CPU 실행 시간도 더 많이 요구합니다.

참고 Cisco VPN Client 버전 3.x 이상에서 DH group 2를 구성하려면 ISAKMP 정책이 필요합니다. (DH group 1을 구성한 경우 Cisco VPN Client를 연결할 수 없습니다.)

AES 지원은 VPN-3DES 전용으로 라이센스된 ASA에서만 이용할 수 없습니다. AES가 제공하는 키는 크기가 크기 때문에, ISAKMP 협상에는 group 1이나 group 2 대신 Diffie-Hellman(DH) group 5를 사용해야 합니다. 이렇게 하려면 **isakmp policy priority group 5** 명령을 사용하면 됩니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 IKE 정책에 대해 group 2, 즉 1024비트 Diffie Hellman을 우선순위 번호 40으로 사용하도록 설정합니다.

```
ciscoasa(config)# isakmp policy 40 group 2
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp policy hash

IKE 정책용 해시 알고리즘을 지정하려면 글로벌 컨피그레이션 모드에서 **isakmp policy hash** 명령을 사용합니다. 해시 알고리즘을 기본값 SHA-1로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

isakmp policy *priority* **hash** {**md5** | **sha**}

no isakmp policy *priority* **hash**

구문 설명

md5	IKE 정책에서 해시 알고리즘으로 MD5(HMAC 변형)를 사용하도록 지정합니다.
priority	IKE 정책을 고유하게 식별하고 정책에 우선순위를 할당합니다. 1~65,534 범위의 정수를 사용합니다. 1은 가장 높은 우선순위이고 65,534는 가장 낮은 우선순위입니다.
sha	IKE 정책에서 해시 알고리즘으로 SHA-1(HMAC 변형)을 사용하도록 지정합니다.

기본값

기본 해시 알고리즘은 SHA-1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp policy hash** 명령이 이 명령을 대체했습니다.

사용 지침

IKE 정책은 IKE 협상 중 사용할 파라미터의 집합을 정의합니다.

SHA-1 및 MD5의 두 가지 해시 알고리즘 옵션이 있습니다. MD5의 다이제스트가 더 작으며, 속도는 SHA-1보다 약간 더 빠른 것으로 간주됩니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 IKE 정책 내에서 우선순위 번호 40으로 MD5 해시 알고리즘을 사용하도록 지정합니다.

```
ciscoasa(config)# isakmp policy 40 hash md5
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp policy lifetime

만료 전에 IKE 보안 연결의 수명을 지정하려면 글로벌 컨피그레이션 모드에서 **isakmp policy lifetime** 명령을 사용합니다. 보안 연결 수명을 기본값 86,400초(1일)로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

구문 설명

priority	IKE 정책을 고유하게 식별하고 정책에 우선순위를 할당합니다. 1~65,534 범위의 정수를 사용합니다. 1은 가장 높은 우선순위이고 65,534는 가장 낮은 우선순위입니다.
seconds	각 보안 연결이 만료되기까지의 시간을 지정합니다. 유한 수명을 지정하려면 120~2147483647초 사이의 정수를 지정합니다. 무한 수명을 지정하려면 0초를 사용합니다.

기본값

기본값은 86,400초(1일)입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp policy lifetime** 명령이 이 명령을 대체했습니다.

사용 지침

IKE는 협상 시작 시, 자체 세션에 대한 보안 파라미터에 합의하려고 시도합니다. 그런 다음 각 피어의 보안 연결은 합의된 파라미터를 참조합니다. 수명이 만료될 때까지 피어는 보안 연결을 유지합니다. 보안 연결이 만료되기 전에는 후속 IKE 협상에서도 이를 사용할 수 있습니다. 그러면 새 IPsec 보안 연결을 설정할 때 시간을 절약할 수 있습니다. 현재 보안 연결이 만료되기 전 피어는 새 보안 연결을 협상합니다.

수명이 더 긴 경우 ASA는 미래의 IPsec 보안 연결을 더욱 신속히 설정합니다. 암호화 강도는 몇 분마다 한 번씩 매우 빠른 리키(rekey) 시간을 사용하지 않고도 보안을 보장할 만큼 충분이 강력합니다. 기본값을 사용하는 것이 좋지만, 피어가 수명을 제안하지 않는 경우 무한 수명을 지정할 수 있습니다.

참고 IKE 보안 연결이 무한 수명으로 설정되어 있지만 피어가 유한 수명을 제안하는 경우, 피어의 협상된 유한 수명이 사용됩니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 IKE 정책 내에서 우선순위 번호 40으로 IKE 보안 연결의 수명을 50,400초(14시간)로 설정합니다.

```
ciscoasa(config)# isakmp policy 40 lifetime 50400
```

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 IKE 보안 연결을 무한 수명으로 설정합니다.

```
ciscoasa(config)# isakmp policy 40 lifetime 0
```

관련 명령

clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

isakmp reload-wait

모든 활성 세션이 자발적으로 종료되기까지 기다린 후 ASA를 재부팅하는 기능을 활성화하려면 글로벌 컨피그레이션 모드에서 **isakmp reload-wait** 명령을 사용합니다. 활성 세션 종료 대기 기능을 비활성화하고 ASA의 재부팅을 진행하려면 이 명령의 **no** 형식을 사용합니다.

isakmp reload-wait

no isakmp reload-wait

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령은 사용이 중단되었습니다. **crypto isakmp reload-wait** 명령이 이 명령을 대체했습니다.

예

다음 예는 글로벌 컨피그레이션 모드에서 입력하여 모든 활성 세션이 만료되기까지 기다린 후 재부팅하도록 ASA에 지시합니다.

```
ciscoasa(config)# isakmp reload-wait
```

관련 명령

명령	설명
clear configure isakmp	모든 ISAKMP 구성을 지웁니다.
clear configure isakmp policy	모든 ISAKMP 정책 구성을 지웁니다.
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 구성을 표시합니다.

issuer

SAML 유형의 SSO 서버에 어설션(assertions)을 전송하는 보안 디바이스를 지정하려면 특정 SAML 유형에 대한 webvpn-sso-saml 구성 모드에서 **issuer** 명령을 사용합니다. 발급자 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다.

issuer *identifier*

no issuer [*identifier*]

구문 설명

identifier	보안 디바이스 이름(대개 디바이스의 호스트 이름)을 지정합니다. 식별자는 영숫자 65자 미만이어야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Webvpn-sso-saml 구성	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

WebVPN에서만 사용 가능한 SSO가 지원되므로, 사용자는 사용자 이름과 비밀번호를 한 번만 입력하여 서로 다른 서버의 서로 다른 서비스에 안전하게 액세스할 수 있습니다. 현재 ASA는 SAML POST 유형의 SSO 서버 및 SiteMinder 유형의 SSO 서버를 지원합니다.

이 명령은 SAML 유형의 SSO 서버에만 적용됩니다.

예

다음 예는 보안 디바이스에 대한 발급자 이름을 asa1.example.com으로 지정합니다.

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# issuer asa1.example.com
ciscoasa(config-webvpn-sso-saml#
```

관련 명령

명령	설명
assertion-consumer-url	보안 디바이스에서 SAML 유형의 SSO 서버 어설션 소비자 서비스에 연락하는 데 사용할 URL을 지정합니다.
request-timeout	실패한 SSO 인증 시도 시간 제한(초 단위)을 지정합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso-server	단일 로그인 서버를 만듭니다.
trustpoint	SAML 유형의 브라우저 어설션에 서명하는 데 사용할 인증서를 포함하는 신뢰 지점 이름을 지정합니다.

issuer-name

발급된 모든 인증서의 발급자 이름 DN을 지정하려면 로컬 CA(인증 기관) 서버 구성 모드에서 **issuer-name** 명령을 사용합니다. 인증서 인증 기관에서 주체 DN을 제거하려면 이 명령의 **no** 형식을 사용합니다.

issuer-name *DN-string*

no issuer-name *DN-string*

구문 설명

DN-string	인증서의 고유 이름을 지정합니다. 이는 자체 서명된 CA 인증서의 주체 이름 DN이기도 합니다. 쉼표를 사용하여 특성-값 쌍을 구분합니다. 쉼표를 포함하는 값을 따옴표로 묶습니다. 발급자 이름은 영숫자 500자 미만이어야 합니다.

기본값

기본 발급자 이름은 cn=*hostame.domain-name*(예: cn=asa.example.com)입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
CA 서버 컨피스레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.3(1)	이 명령이 추가되었습니다.
8.0(2)	*DN-string* 값에 쉼표를 포함하도록 따옴표에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 로컬 CA 서버에서 생성된 인증서에 나타나는 발급자 이름을 지정합니다. 발급자 이름을 기본 CA 이름과 다르게 지정하려면 이 선택적인 명령을 사용합니다.

참고 CA 서버를 활성화하고 **no shutdown** 명령을 실행하여 인증서를 생성한 후에는 발급자 이름 구성을 변경할 수 없습니다.

예

다음 예는 인증서 인증을 구성합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco
systems, inc."
ciscoasa(config-ca-server)#
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리를 허용하는 ca 서버 컨피스레이션 모드 명령에 대한 액세스를 제공합니다.
keysize	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 지정합니다.
lifetime	CA 인증서 및 발급된 인증서의 수명을 지정합니다.
show crypto ca server	로컬 CA의 특성을 표시합니다.
show crypto ca server cert-db	로컬 CA 서버 인증서를 표시합니다.

파트 **2**

J~M 명령

6 장

java-trustpoint through kill 명령

java-trustpoint

지정된 신뢰 지점 위치에서 PKCS12 인증서 및 키 지정 자료를 사용할 수 있도록 WebVPN Java 객체 서명 기능을 구성하려면 webvpn 컨피그레이션 모드에서 **java-trustpoint** 명령을 사용합니다. Java 객체 서명에 대한 신뢰 지점을 제거하려면 이 명령의 **no** 형식을 사용합니다.

java-trustpoint *trustpoint*

no java-trustpoint

구문 설명

trustpoint	**crypto ca import** 명령으로 구성할 신뢰 지점 위치를 지정합니다.

기본값

기본적으로 Java 객체 서명에 대한 신뢰 지점은 none으로 설정됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(2)	이 명령이 추가되었습니다.

사용 지침

신뢰 지점은 CA(인증 기관) 또는 ID 키 쌍을 나타낸 것입니다. **java-trustpoint** 명령의 경우, 지정된 신뢰 지점에는 애플리케이션 서명 엔트리의 X.509 인증서, 그 인증서에 해당하는 RSA 개인 키, 그리고 루트 CA까지 확장되는 인증 기관 체인을 포함해야 합니다. 이렇게 하려면 일반적으로 **crypto ca import** 명령을 사용하여 PKCS12 형식의 번들을 가져오면 됩니다. 신뢰할 수 있는 CA에서 PKCS12 번들을 가져올 수도 있고, openssl과 같은 오픈 소스 툴을 사용하여 기존 X.509 인증서 및 RSA 개인 키에서 번들을 만들 수도 있습니다.

참고 패키지(예: CSD 패키지)와 함께 포함되어 있는 Java 객체에 서명하는 데에는 업로드된 인증서를 사용할 수 없습니다.

예

다음 예는 먼저 새 신뢰 지점을 구성한 다음, 이를 WebVPN Java 객체 서명에 맞게 구성합니다.

```
ciscoasa(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
ciscoasa(config)#
```

다음 예는 WebVPN Java 객체 서명을 위한 새 신뢰 지점을 구성합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config)# java-trustpoint mytrustpoint
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ca import	PKCS12 데이터를 사용하여 신뢰 지점을 위한 인증서 및 키 쌍을 가져옵니다.

join-failover-group

장애 조치 그룹에 컨텍스트를 할당하려면 컨텍스트 컨피그레이션 모드에서 **join-failover-group** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

join-failover-group *group_num*

no join-failover-group *group_num*

구문 설명

group_num	장애 조치 그룹 번호를 지정합니다.

기본값

장애 조치 그룹 1

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
컨텍스트 컨피그레이션	• 예	• 예	—	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

관리자 컨텍스트는 항상 장애 조치 그룹 1에 할당됩니다. 장애 조치 그룹 및 컨텍스트 연결을 표시하려면 **show context detail** 명령을 사용할 수 있습니다.

장애 조치 그룹에 컨텍스트를 할당하기 전에 시스템 컨텍스트에서 **failover group** 명령을 사용하여 장애 조치 그룹을 만들어야 합니다. 컨텍스트가 활성 상태인 유닛에서 이 명령을 입력합니다. 기본적으로, 할당되지 않은 컨텍스트는 장애 조치 그룹 1의 멤버입니다. 따라서 전에 장애 조치 그룹에 컨텍스트를 할당하지 않았다면 활성 상태의 장애 조치 그룹 1이 있는 유닛에서 이 명령을 입력해야 합니다.

시스템에서 장애 조치 그룹을 제거하려면 먼저 **no join-failover-group** 명령을 사용하여 장애 조치 그룹에서 모든 컨텍스트를 제거해야 합니다.

예

다음 예는 ctx1이라는 컨텍스트를 장애 조치 그룹 2에 할당합니다.

```
ciscoasa(config)# context ctx1
ciscoasa(config-context)# join-failover-group 2
ciscoasa(config-context)# exit
```

관련 명령

명령	설명
context	지정된 컨텍스트에 대한 컨텍스트 컨피그레이션 모드로 들어갑니다.
failover group	액티브/액티브 장애 조치에 대한 장애 조치 그룹을 정의합니다.
show context detail	이름, 클래스, 인터페이스, 장애 조치 그룹 연결, 컨피그레이션 파일 URL을 비롯한 컨텍스트 세부 정보를 표시합니다.

jumbo-frame reservation

지원되는 모델에 대한 점보 프레임을 활성화하려면 글로벌 컨피그레이션 모드에서 **jumbo-frame reservation** 명령을 사용합니다. 점보 프레임을 비활성화하려면 이 명령을 **no** 형식으로 사용합니다.

참고 이 설정을 변경하면 ASA를 재부팅해야 합니다.

jumbo-frame reservation

no jumbo-frame reservation

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

점보 프레임 예약은 기본적으로 비활성화되어 있습니다.

ASASM에서는 기본적으로 점보 프레임이 지원되므로 이 명령을 사용할 필요가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.1(1)	이 명령이 ASA 5580용으로 추가되었습니다.
8.2(5)/8.4(1)	ASA 5585-X에 대한 지원이 추가되었습니다.
8.6(1)	ASA 5512-X~ASA 5555-X에 대한 지원이 추가되었습니다.

사용 지침

점보 프레임은 표준 최대 크기인 1518바이트(Layer 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷으로 최대 크기가 9216바이트입니다. 점보 프레임에는 별도의 메모리가 필요하며, 이에 따라 액세스 목록 등 다른 기능을 최대한 사용하는 데 제한이 따를 수 있습니다.

Management *n*/*n* 인터페이스에서는 점보 프레임이 지원되지 않습니다.

점보 프레임을 전송해야 하는 각 인터페이스의 MTU는 기본값 1500보다 높은 값으로 설정해야 합니다. 예를 들어, **mtu** 명령을 사용하여 값을 9000으로 설정합니다. ASASM은 기본적으로 점보 프레임을 지원하므로 **jumbo-frame** reservation 명령을 설정할 필요가 없습니다. MTU를 원하는 값으로 설정하면 됩니다.

또한 점보 프레임을 사용할 경우에는 TCP용 MSS(maximum segment size) 값을 설정해야 합니다. MSS는 MTU보다 120바이트 적어야 합니다. 예를 들어 MTU를 9000으로 구성하는 경우 MSS는 8880으로 구성해야 합니다. MSS는 **sysopt connection tcpmss** 명령으로 구성할 수 있습니다.

장애 조치 쌍이 점보 프레임을 지원하도록 하려면 기본 유닛과 보조 유닛 모두 재부팅해야 합니다. 다운타임을 피하려면 다음을 수행합니다.

- 활성 유닛에서 명령을 실행합니다.
- 활성 유닛에서 실행 중인 컨피그레이션을 저장합니다.
- 기본 유닛과 보조 유닛을 한 번에 하나씩 재부팅합니다.

예

다음 예에서는 점보 프레임 예약을 활성화하고, 컨피그레이션을 저장하며, ASA를 다시 로드합니다.

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

관련 명령

명령	설명
mtu	인터페이스의 최대 전송 유닛을 지정합니다.
show jumbo-frame reservation	**jumbo-frame reservation** 명령의 현재 컨피그레이션을 보여줍니다.

kcd-server

ASA가 Active Directory 도메인에 가입하도록 하려면 webvpn 컨피그레이션 모드에서 **kcd-server** 명령을 사용합니다. ASA에 대해 지정된 동작을 제거하려면 이 명령의 **no** 형식을 사용합니다.

kcd-server *aaa-server-group_name* **user** *username* **password** *password*

no kcd-server

구문 설명

user	서비스 레벨 권한이 있는 Active Directory 사용자를 지정합니다.
password	지정된 사용자에 대한 비밀번호를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

사용 지침

ASA가 Active Directory 도메인에 가입하도록 하려면 webvpn 컨피그레이션 모드에서 **kcd-server** 명령을 사용합니다. 도메인 컨트롤러 이름 및 영역은 **aaa-server-groupname** 명령으로 지정합니다. AAA 서버 그룹은 Kerberos 서버 유형이어야 합니다. **username** 및 **password** 옵션은 관리자 권한이 있는 사용자에게는 해당되지 않지만, 도메인 컨트롤러에서 서비스 레벨 권한이 있는 사용자에게는 적용해야 합니다. 이 명령을 실행하면 성공 또는 실패 상태가 표시됩니다. **show webvpn kcd** 명령을 사용하여 결과를 볼 수도 있습니다.

ASA 환경의 KCD(Kerberos Constrained Delegation)는 WebVPN 사용자에게 Kerberos로 보호되는 모든 웹 서비스에 대한 SSO(단일 로그인) 액세스를 제공합니다. ASA는 사용자(서비스 티켓) 대신 자격 증명을 유지 관리하며, 이 티켓을 사용해 서비스에 대해 사용자를 인증합니다.

kcd-server 명령이 작동하도록 하려면, ASA가 *source* 도메인(ASA가 상주하는 도메인)과 *target* 또는 *resource* 도메인(웹 서비스가 상주하는 도메인) 간에 신뢰 관계를 형성해야 합니다. ASA는 고유한 형식을 사용하여 소스에서 대상 도메인으로 인증 경로를 교차하고, 서비스에 액세스하려는 원격 액세스 사용자를 대신하여 필요한 티켓을 획득합니다.

이 경로를 교차 영역 인증이라고 합니다. 교차 영역 인증의 각 단계에서 ASA는 특정 도메인에 있는 자격 증명 및 후속 도메인과의 신뢰 관계에 의존합니다.

교차 영역 인증을 위해 ASA를 구성하려면 **ntp**, **hostname**, **dns domain-lookup, dns server-group** 명령을 사용하여 Active Directory 도메인에 가입해야 합니다.

예

다음 예는 **kcd-server** 명령의 사용 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server kcd-grp protocol kerberos
ciscoasa(config-aaa-server-group)# aaa-server kcd-grp host DC
ciscoasa(config-aaa-server-group)# kerberos-realm EXAMPLE.COM
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# kcd-server kcd-grp user Administrator password Cisco123
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)#
```

다음은 교차 영역 인증의 컨피그레이션 예입니다. 여기서 Domain Controller는 10.1.1.10(내부 인터페이스를 통해 도달 가능)이고 도메인 이름은 PRIVATE.NET입니다. 또한 도메인 컨트롤러에서 Service Account 사용자 이름 및 비밀번호는 dcuser와 dcuser123!입니다.

```
ciscoasa(config)# config t

-----Create an alias for the Domain Controller-------------

ciscoasa(config)# name 10.1.1.10 DC

----Configure the Name server-----------------------------

ciscoasa(config)# ntp server DC

----Enable a DNS lookup by configuring the DNS server and Domain name --------------

ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server DC
ciscoasa(config-dns-server-group)# domain-name private.net

----Configure the AAA server group with Server and Realm------------------------------

ciscoasa(config)# aaa-server KerberosGroup protocol Kerberos
ciscoasa(config-asa-server-group)# aaa-server KerberosGroup (inside) host DC
ciscoasa(config-asa-server-group)# Kerberos-realm PRIVATE.NET

----Configure the Domain Join-------------------------------

ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# kcd-server KerberosGroup username dcuser password dcuser123!
ciscoasa(config)#
```

관련 명령

명령	설명
aaa-server	AAA 서버 매개변수를 구성할 수 있는 aaa-server 컨피그레이션 모드로 들어갑니다.
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
clear configure aaa-server	컨피그레이션에서 모든 AAA 명령문을 제거합니다.
dns	도메인 이름 서버를 지정합니다.
domain-name	서버의 도메인 이름을 지정합니다.
hostname	호스트 이름을 지정합니다.
ntp	전송 프로토콜을 지정합니다.
show aaa-kerberos	모든 AAA Kerberos 서버에 대한 서버 통계를 표시합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

keepout

새 사용자 세션에 대한 로그인 페이지 대신 관리자가 정의한 메시지를 표시하려면(ASA에서 유지 관리 또는 문제 해결이 진행되는 동안) webvpn 컨피그레이션 모드에서 **keepout** 명령을 사용합니다. 전에 설정한 keepout 페이지를 제거하려면 이 명령의 **no** 형식을 사용합니다.

keepout

no keepout *string*

구문 설명

string	큰따옴표의 영숫자 문자열

기본값

keepout 페이지 없음

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

이 명령을 활성화하면 클라이언트리스 WebVPN 포털 페이지를 사용할 수 없게 됩니다. 포털의 로그인 페이지 대신 포털을 사용할 수 없다는 내용의 관리자 정의 메시지가 표시됩니다. 클라이언트리스 액세스는 비활성화하되 AnyConnect 액세스는 여전히 허용하려면 **keepout** 명령을 사용합니다. 유지 관리가 진행되는 동안에는 이 명령을 사용하여 포털을 사용할 수 없음을 나타낼 수도 있습니다.

예

다음 예는 keepout 페이지 구성 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# keepout "The system is unavailable until 7:00 a.m. EST."
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
webvpn	클라이언트리스 SSL VPN 연결을 위해 특성을 구성할 수 있는 webvpn 컨피그레이션 모드로 들어갑니다.

kerberos-realm

이 Kerberos 서버에 대한 영역 이름을 지정하려면 aaa-server host 컨피그레이션 모드에서 **kerberos-realm** 명령을 사용합니다. 영역 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다.

kerberos-realm *string*

no kerberos-realm

구문 설명

string	대/소문자를 구분하는 최대 64자의 영숫자 문자열. 문자열에서 공백은 허용되지 않습니다. **참고** Kerberos 영역 이름에는 숫자 및 대문자만 사용할 수 있습니다. ASA는 *string* 인수에서 소문자를 허용하지만 소문자를 대문자로 변환하지는 않습니다. 대문자만 사용하도록 유의하십시오.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Kerberos 서버에 대해서만 유효합니다.

Kerberos 영역의 Windows 2000 Active Directory 서버에서 실행할 때 *string* 인수의 값은 Microsoft Windows **set USERDNSDOMAIN** 명령의 출력과 일치해야 합니다. 다음 예에서는 EXAMPLE.COM이 Kerberos 영역 이름입니다.

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

string 인수에는 숫자 및 대문자만 사용할 수 있습니다. **kerberos-realm** 명령은 대/소문자를 구분하며 ASA는 소문자를 대문자로 변환하지 않습니다.

예

다음 예는 **kerberos-realm** 명령을 사용하여, AAA 서버 호스트를 구성하는 컨텍스트에서 kerberos 영역을 "EXAMPLE.COM"으로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 AAA server host 컨피그레이션 하위 모드로 들어갑니다.
clear configure aaa-server	컨피그레이션에서 모든 AAA 명령문을 제거합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

key(aaa-server host)

AAA 서버에 대해 NAS를 인증하는 데 사용되는 서버 암호 값을 지정하려면 aaa-server host 컨피그레이션 모드에서 **key** 명령을 사용합니다. aaa-server host 컨피그레이션 모드는 aaa-server protocol 컨피그레이션 모드에서 액세스할 수 있습니다. 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

key *key*

no key

구문 설명

key	최대 127자 길이의 영숫자 키워드

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

key 값은 대/소문자를 구분하는 최대 127자의 영숫자 키워드로 TACACS+ 서버의 키와 같은 값입니다. 127자를 넘는 문자는 무시됩니다. 키는 클라이언트와 서버 간 데이터를 암호화하기 위해 클라이언트와 서버 간에 사용됩니다. 키는 클라이언트 시스템과 서버 시스템에서 모두 동일해야 합니다. 키에는 공백을 포함할 수 없지만 다른 특수 문자는 허용됩니다. 키(서버 암호) 값은 AAA 서버를 기준으로 ASA를 인증합니다.

이 명령은 RADIUS 및 TACACS+ 서버에 대해서만 유효합니다.

예

다음 예는 호스트 "1.2.3.4"에서 "svrgrp1"이라는 TACACS+ AAA 서버를 구성하고, 시간 제한 간격을 9초로 설정하고, 재시도 간격을 7초로 설정하며, 키를 "myexclusivemumblekey"로 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
clear configure aaa-server	컨피그레이션에서 모든 AAA 명령문을 제거합니다.
show running-config aaa-server	AAA 서버 컨피그레이션을 표시합니다.

key(cluster group)

클러스터 제어 링크에서 컨트롤 트래픽용 인증 키를 설정하려면 cluster group 컨피그레이션 모드에서 **key** 명령을 사용합니다. 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

key *shared_secret*

no key [*shared_secret*]

구문 설명

shared_secret	1~63자로 된 ASCII 문자열로 공유 암호를 설정합니다. 공유 비밀은 키를 생성하는 데 사용됩니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

예

다음 예는 공유 암호를 설정합니다.

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용할 경우 ASA에서는 cLACP를 사용하여 EtherChannel과 인접 스위치의 협상을 수행합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드로 들어갑니다.
cluster-interface	클러스터 제어 링크 인터페이스를 지정합니다.
cluster interface-mode	클러스터 인터페이스 모드를 설정합니다.
conn-rebalance	연결 리밸런싱을 활성화합니다.
console-replicate	슬레이브 유닛에서 마스터 유닛으로의 콘솔 복제를 활성화합니다.
enable (cluster group)	클러스터링을 활성화합니다.
health-check	유닛 검사 모니터링 및 인터페이스 상태 모니터링이 포함된 클러스터 상태 검사 기능을 활성화합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스의 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택을 위해 이 유닛의 우선순위를 설정합니다.

key config-key password-encryption

암호화 키 생성에 사용할 패스프레이즈를 설정하려면 글로벌 컨피그레이션 모드에서 **key config-key password-encryption** 명령을 사용합니다. 패스프레이즈로 암호화한 비밀번호를 해독하려면 이 명령의 **no** 형식을 사용합니다.

key config-key password-encryption [*new pass phrase* [*old pass phrase*]]

no key config-key password-encryption [*current pass phrase*]

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 활성화하면 암호화 키 생성에 사용되는 패스프레이즈를 설정할 수 있습니다. 패스프레이즈를 처음 구성하는 경우에는 현재 비밀번호를 입력할 필요가 없습니다. 그렇지 않은 경우에는 현재 비밀번호를 입력해야 합니다. 새 패스프레이즈는 8~128자여야 합니다. 패스프레이즈에는 백스페이스와 큰따옴표를 제외한 모든 문자를 사용할 수 있습니다.

write erase 명령 뒤에 **reload** 명령을 사용하면 마스터 패스프레이즈가 제거됩니다(손실된 경우).

예

다음 예는 암호화 키를 생성하는 데 사용되는 패스프레이즈를 설정합니다.

```
ciscoasa(config)# key config-key password-encryption
```

관련 명령

명령	설명
password encryption aes	비밀번호 암호화를 활성화합니다.
write erase	이 명령 뒤에 **reload** 명령을 사용하는 경우, 손실된 마스터 패스프레이즈를 제거합니다.

key-hash

온보드 SCP(Secure Copy) 클라이언트용 서버에 해시된 SSH 호스트 키를 수동으로 추가하려면 서버 컨피그레이션 모드에서 **key-hash** 명령을 사용합니다. 먼저 **ssh pubkey-chain** 명령을 입력하여 서버 컨피그레이션 모드에 액세스할 수 있습니다. 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

key-hash {**md5** | **sha256**} *fingerprint*

no key-hash {**md5** | **sha256**} *fingerprint*

구문 설명

fingerprint	해시된 키를 입력합니다.
{**md5** | **sha256**}	사용되는 해시 유형을 설정합니다(MD5 또는 SHA-256). ASA는 컨피그레이션에서 항상 SHA-256을 사용합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
서버 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.1(5)	이 명령이 추가되었습니다.

사용 지침

온보드 SCP 클라이언트를 사용하여 파일을 ASA로 복사하거나 ASA에서 복사해올 수 있습니다. ASA에서는 연결되는 각 SCP 서버의 SSH 호스트 키를 저장합니다. 원한다면 ASA 데이터베이스에서 직접 서버와 키를 추가하거나 삭제할 수 있습니다.

각 서버에 대해 SSH 호스트의 **key-string**(공개 키) 또는 **key-hash**(해시된 값)를 지정할 수 있습니다. **key-hash**는 이미 해시된 키를 입력합니다(MD5 또는 SHA-256 키 사용). 예를 들면 **show** 명령 출력에서 복사한 키입니다.

예

다음 예에서는 서버 10.86.94.170을 위해 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
```

관련 명령

명령	설명
copy	파일을 ASA로 또는 ASA에서 복사합니다.
key-hash	해시된 SSH 호스트 키를 입력합니다.
key-string	공개 SSH 호스트 키를 입력합니다.
ssh pubkey-chain	서버 및 서버의 키를 ASA 데이터베이스에서 수동으로 추가하거나 삭제합니다.
ssh stricthostkeycheck	온보드 SCP(Secure Copy) 클라이언트를 검사하도록 SSH 호스트 키를 설정합니다.

keypair

인증할 공개 키의 키 쌍을 지정하려면 crypto ca trustpoint 컨피그레이션 모드에서 **keypair** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

keypair *name*

no keypair

구문 설명

name	키 쌍의 이름을 지정합니다.

기본값

기본 설정은 키 쌍을 포함하지 않는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 trustpoint central을 위한 crypto ca trustpoint 컨피그레이션 모드로 들어가며 trustpoint central에 대해 인증할 키 쌍을 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# keypair exchange
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다.
crypto key generate dsa	DSA 키를 생성합니다.
crypto key generate rsa	RSA 키를 생성합니다.
default enrollment	enrollment 매개변수를 기본값으로 되돌립니다.

keysize

사용자 인증서 등록 시 CA(인증 기관) 서버에서 생성하는 공개 키 및 개인 키의 크기를 지정하려면 ca-server 컨피그레이션 모드에서 **keysize** 명령을 사용합니다. keysize를 기본 길이인 1024비트로 복원하려면 이 명령의 **no** 형식을 사용합니다.

keysize {**512** | **768** | **1024** | **2048**}

no keysize

구문 설명

512	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 512비트로 지정합니다.
768	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 768비트로 지정합니다.
1024	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 1024비트로 지정합니다.
2048	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 2048비트로 지정합니다.

기본값

기본적으로 키 쌍의 각 키 길이는 1024비트입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-server 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

예

다음 예는 로컬 CA 서버의 사용자를 위해 생성되는 모든 공개 및 개인 키 쌍에 대해 2048비트의 키 크기를 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server))# keysize 2048
ciscoasa(config-ca-server)#
```

다음 예는 로컬 CA 서버의 사용자를 위해 생성되는 모든 공개 및 개인 키 쌍에 대해 키 크기를 기본 길이인 1024비트로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no keysize
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 ca-server 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다.
issuer-name	인증서 인증 기관의 주체 이름 DN을 지정합니다.
subject-name-default	CA 서버에서 발급하는 모든 사용자 인증서에서 사용자 이름과 함께 일반 주체 이름 DN을 사용하도록 지정합니다.

keysize server

CA keypair의 크기를 구성하기 위해 CA(인증 기관) 서버에서 생성하는 공개 키 및 개인 키의 크기를 지정하려면 ca-server 컨피그레이션 모드에서 **keysize server** 명령을 사용합니다. keysize를 기본 길이인 1024비트로 복원하려면 이 명령의 **no** 형식을 사용합니다.

keysize server{**512** | **768** | **1024** | **2048**}

no keysize server

구문 설명

512	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 512비트로 지정합니다.
768	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 768비트로 지정합니다.
1024	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 1024비트로 지정합니다.
2048	인증서 등록 시 생성되는 공개 키와 개인 키의 크기를 2048비트로 지정합니다.

기본값

기본적으로 키 쌍의 각 키 길이는 1024비트입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-server 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

예

다음 예는 CA 인증서에 대해 2048비트의 키 크기를 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server))# keysize server 2048
ciscoasa(config-ca-server)#
```

다음 예는 키 크기를 CA 인증서용 기본 길이인 1024비트로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no keysize server
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 ca-server 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다.
issuer-name	인증서 인증 기관의 주체 이름 DN을 지정합니다.
keysize	사용자 인증서용 키 쌍 크기를 지정합니다.
subject-name-default	CA 서버에서 발급하는 모든 사용자 인증서에서 사용자 이름과 함께 일반 주체 이름 DN을 사용하도록 지정합니다.

key-string

온보드 SCP(Secure Copy) 클라이언트용 서버에 공개 SSH 호스트 키를 수동으로 추가하려면 서버 컨피그레이션 모드에서 **key-string** 명령을 사용합니다. 먼저 **ssh pubkey-chain** 명령을 입력하여 서버 컨피그레이션 모드에 액세스할 수 있습니다. 다음 명령은 키 문자열에 대한 프롬프트를 표시합니다. 문자열을 컨피그레이션에 저장하면 SHA-256을 사용하여 해시된 후 **key-hash** 명령으로 저장됩니다. 따라서 문자열을 제거하려면 **no key-hash** 명령을 사용합니다.

key-string
key_string

구문 설명

key_string	공개 키를 입력합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
서버 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.1(5)	이 명령이 추가되었습니다.

사용 지침

온보드 SCP 클라이언트를 사용하여 파일을 ASA로 복사하거나 ASA에서 복사해올 수 있습니다. ASA에서는 연결되는 각 SCP 서버의 SSH 호스트 키를 저장합니다. 원한다면 ASA 데이터베이스에서 직접 서버와 키를 추가하거나 삭제할 수 있습니다.

각 서버에 대해 SSH 호스트의 **key-string**(공개 키) 또는 **key-hash**(해시된 값)를 지정할 수 있습니다. *key_string*은 원격 피어의 Base64 인코딩 RSA 공개 키입니다. 열린 SSH 클라이언트에서, 즉 .ssh/id_rsa.pub 파일에서 공개 키 값을 얻을 수 있습니다. Base64 인코딩 공개 키를 전송하면 그 키가 SHA-256을 통해 해시됩니다.

예

다음 예에서는 서버 10.7.8.9를 위해 호스트 문자열 키를 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
```

다음 예는 저장된 해시된 키를 보여줍니다.

```
ciscoasa(config-ssh-pubkey-server)# show running-config ssh
ssh scopy enable
ssh stricthostkeycheck
ssh pubkey-chain
  server 10.7.8.9
    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
```

관련 명령

명령	설명
copy	파일을 ASA로 또는 ASA에서 복사합니다.
key-hash	해시된 SSH 호스트 키를 입력합니다.
key-string	공개 SSH 호스트 키를 입력합니다.
ssh pubkey-chain	서버 및 서버의 키를 ASA 데이터베이스에서 수동으로 추가하거나 삭제합니다.
ssh stricthostkeycheck	온보드 SCP(Secure Copy) 클라이언트를 검사하도록 SSH 호스트 키를 설정합니다.

kill

텔넷 세션을 종료하려면 특별 권한 EXEC 모드에서 **kill** 명령을 사용합니다.

kill *telnet_id*

구문 설명

telnet_id	텔넷 세션 ID를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

kill 명령을 사용하면 텔넷 세션을 종료할 수 있습니다. 텔넷 세션 ID를 보려면 **who** 명령을 사용합니다. 사용자가 텔넷 세션을 종료하면 ASA는 모든 활성 명령의 종료를 허용한 후 경고 없이 연결을 삭제합니다.

예

다음 예는 ID "2"의 텔넷 세션을 종료하는 방법을 보여줍니다. 먼저 활성 텔넷 세션의 목록을 표시하도록 **who** 명령을 입력합니다. 그런 다음 **kill 2** 명령을 입력하여 ID "2"인 텔넷 세션을 종료합니다.

```
ciscoasa# who
2: From 10.10.54.0

ciscoasa# kill 2
```

관련 명령

명령	설명
telnet	ASA에 대한 텔넷 액세스를 구성합니다.
who	활성 텔넷 세션의 목록을 표시합니다.

7 장

l2tp tunnel hello through log-adjacency-changes 명령

l2tp tunnel hello

L2TP over IPsec 연결에서 hello 메시지 사이의 간격을 지정하려면 글로벌 컨피그레이션 모드에서 **l2tp tunnel hello** 명령을 지정합니다. 간격을 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

구문 설명

interval	hello 메시지 사이의 간격(초). 기본값은 60초입니다. 범위는 10~300초입니다.

기본값

기본값은 60초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

l2tp tunnel hello 명령을 사용하면 ASA는 L2TP 연결의 물리적 계층에서 문제를 감지할 수 있습니다. 기본값은 60초입니다. 낮은 값을 구성할수록 문제가 발생하는 연결이 더 일찍 끊어집니다.

예

다음 예는 hello 메시지의 간격을 30초로 구성합니다.

```
ciscoasa(config)# l2tp tunnel hello 30
```

관련 명령

명령	설명
show vpn-sessiondb detail remote filter protocol L2TPOverIPsec	L2TP 연결의 세부 정보를 표시합니다.
vpn-tunnel-protocol l2tp-ipsec	특정 터널 그룹의 터널링 프로토콜로서 L2TP를 활성화합니다.

lacp max-bundle

EtherChannel 채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 지정하려면 인터페이스 컨피그레이션 모드에서 **lacp max-bundle** 명령을 사용합니다. 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

lacp max-bundle *number*

no lacp max-bundle

구문 설명

number	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 9.2(1)의 경우 1~8로 지정하고, 그 이상의 경우 최대 16으로 지정합니다. 스위치에서 16개의 액티브 인터페이스를 지원하지 않을 경우, 이 명령을 8 이하로 설정합니다.

명령 기본값

(9.1 이하) 기본값 8

(9.2(1) 이상) 기본값 16

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.
9.2(1)	액티브 인터페이스의 개수가 8에서 16으로 증가했습니다.

사용 지침

포트 채널 인터페이스에 대해 이 명령을 입력합니다. 채널 그룹당 최대 액티브 인터페이스 개수는 8입니다. 값을 줄이려면 이 명령을 사용합니다.

예

다음 예는 EtherChannel에서 최대 인터페이스 개수를 4로 설정합니다.

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp port-priority	채널 그룹에서 물리적 인터페이스의 우선순위를 설정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel load-balance	로드 밸런싱 알고리즘을 구성합니다.
port-channel min-bundle	포트 채널 인터페이스를 액티브 상태로 설정하는 데 필요한 액티브 인터페이스의 최소 개수를 지정합니다.
show lacp	트래픽 통계, 시스템 식별자, 인접 디바이스 세부사항 같은 LACP 정보가 표시됩니다.
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령을 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel load-balance	정해진 매개변수 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

lacp port-priority

EtherChannel에서 물리적 인터페이스의 우선순위를 설정하려면 인터페이스 컨피그레이션 모드에서 **lacp port-priority** 명령을 사용합니다. 우선순위를 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

lacp port-priority *number*

no lacp port-priority

구문 설명

number	우선순위를 설정합니다(1~65535). 숫자가 높을수록 우선순위는 낮아집니다.

명령 기본값

기본값은 32768일입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

사용 지침

물리적 인터페이스에 대해 이 명령을 입력합니다. 사용할 수 있는 인터페이스보다 더 많은 인터페이스가 할당된 경우, ASA에서는 이 설정을 사용하여 어떤 인터페이스가 액티브이고 스탠바이인지 확인합니다. 포트 우선순위 설정이 모든 인터페이스에 대해 동일한 경우, 인터페이스 ID(슬롯/포트)로 우선순위가 결정됩니다. 가장 낮은 인터페이스 ID의 우선순위가 가장 높습니다. 예를 들어, GigabitEthernet 0/0은 GigabitEthernet 0/1보다 우선순위가 더 높습니다.

인터페이스 ID가 더 큰 인터페이스에 우선순위를 부여하여 액티브 상태로 만들려면 이 명령을 더 낮은 값으로 설정합니다. 예를 들어, GigabitEthernet 1/3을 GigabitEthernet 0/7보다 우선순위가 높은 액티브 상태로 만들려면 0/7 인터페이스의 기본값인 32768과 대조적으로, 1/3 인터페이스의 **lacp port-priority** 값을 12345로 설정합니다.

EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선순위가 충돌할 경우, 시스템 우선순위를 통해 어느 포트 우선순위를 사용해야 할지 결정됩니다. **lacp system-priority** 명령을 참조하십시오.

LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다. LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 컨피그레이션 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다.

예

다음 예는 GigabitEthernet 0/0 및 0/1보다 먼저 EtherChannel의 일부로서 사용되도록 GigabitEthernet 0/2에 대해 포트 우선순위를 더 낮게 설정합니다.

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 지정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel load-balance	로드 밸런싱 알고리즘을 구성합니다.
port-channel min-bundle	포트 채널 인터페이스를 액티브 상태로 설정하는 데 필요한 액티브 인터페이스의 최소 개수를 지정합니다.
show lacp	트래픽 통계, 시스템 식별자, 인접 디바이스 세부사항 같은 LACP 정보가 표시됩니다.
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령을 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel load-balance	정해진 매개변수 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

lacp system-priority

EtherChannels의 경우 ASA에 대해 LACP 시스템 우선순위를 전체적으로 설정하려면 글로벌 컨피그레이션 모드에서 **lacp system-priority** 명령을 사용합니다. 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

lacp system-priority *number*

no lacp system-priority

구문 설명

number	LACP 시스템 우선순위를 1~65535까지 설정합니다. 기본값은 32768일입니다. 숫자가 높을수록 우선순위는 낮아집니다. 이 명령어는 ASA에 전체적으로 적용됩니다.

명령 기본값

기본값은 32768일입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

사용 지침

EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선순위가 충돌할 경우, 시스템 우선순위를 통해 어느 포트 우선순위를 사용해야 할지 결정됩니다. EtherChannel 내의 인터페이스 우선순위에 대한 자세한 내용은 **lacp port-priority** 명령을 참조하십시오.

예

다음 예는 시스템 우선순위를 기본값보다 높게(더 낮은 숫자로) 설정합니다.

```
ciscoasa(config)# lacp system-priority 12345
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 지정합니다.
lacp port-priority	채널 그룹에서 물리적 인터페이스의 우선순위를 설정합니다.
port-channel load-balance	로드 밸런싱 알고리즘을 구성합니다.
port-channel min-bundle	포트 채널 인터페이스를 액티브 상태로 설정하는 데 필요한 액티브 인터페이스의 최소 개수를 지정합니다.
show lacp	트래픽 통계, 시스템 식별자, 인접 디바이스 세부사항 같은 LACP 정보가 표시됩니다.
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령을 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel load-balance	정해진 매개변수 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

ldap attribute-map

사용자 정의 특성 이름을 Cisco LDAP 특성 이름에 매핑할 수 있도록 LDAP 특성 맵을 만들고 이름을 지정하려면 글로벌 컨피그레이션 모드에서 **ldap attribute-map** 명령을 사용합니다. 맵을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

구문 설명

map-name	LDAP 특성 맵을 위한 사용자 정의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

ldap attribute-map 명령을 사용하면 고유한 특성 이름과 값을 Cisco 특성 이름에 매핑할 수 있습니다. 그런 다음 결과 특성 맵을 LDAP 서버에 바인딩할 수 있습니다. 일반적인 단계는 다음과 같습니다.

1. 글로벌 컨피그레이션 모드에서 **ldap attribute-map** 명령을 사용하여 채워지지 않은 특성 맵을 생성합니다. 이 명령을 실행하면 ldap-attribute-map 컨피그레이션 모드로 들어갑니다.
2. ldap-attribute-map 컨피그레이션 모드에서 **map-name** 및 **map-value** 명령을 사용하여 특성 맵을 채웁니다.
3. aaa-server host 모드에서 **ldap-attribute-map** 명령을 사용하여 특성 맵을 LDAP 서버에 바인딩합니다. 이 명령에서 ldap 뒤에 하이픈이 있음에 유의하십시오.

참고 특성 매핑 기능을 올바르게 사용하려면 Cisco LDAP 특성의 이름 및 값 그리고 사용자 정의 특성의 이름 및 값을 모두 알고 있어야 합니다.

예

글로벌 컨피그레이션 모드에서 입력하는 다음 명령 예는 myldapmap이라는 LDAP 특성 맵을 만든 후 내용을 채우거나 LDAP 서버에 바인딩합니다.

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)#
```

관련 명령

명령	설명
ldap-attribute-map(aaa-server host 모드)	LDAP 특성 맵을 LDAP 서버에 바인딩합니다.
map-name	사용자 정의 LDAP 특성 이름을 Cisco LDAP 특성 이름에 매핑합니다.
map-value	사용자 정의 특성 값을 Cisco 특성 이름에 매핑합니다.
show running-config ldap attribute-map	실행 중인 특정 LDAP 특성 맵 또는 실행 중인 모든 특성 맵을 표시합니다.
clear configure ldap attribute-map	모든 LDAP 특성 맵을 제거합니다.

ldap-attribute-map

기존 매핑 컨피그레이션을 LDAP 호스트에 바인딩하려면 aaa-server host 컨피그레이션 모드에서 **ldap-attribute-map** 명령을 사용합니다. 바인딩을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

구문 설명

map-name	LDAP 특성 매핑 컨피그레이션을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

Cisco 정의 LDAP 특성 이름이 편이성 또는 기타 요건에 맞지 않으면 고유한 특성 이름을 만들고, 이를 Cisco 특성에 매핑한 다음, 그 결과의 특성 컨피그레이션을 LDAP 서버에 바인딩할 수 있습니다. 일반적인 단계는 다음과 같습니다.

1. 글로벌 컨피그레이션 모드에서 **ldap attribute-map** 명령을 사용하여 채워지지 않은 특성 맵을 생성합니다. 이 명령을 실행하면 ldap-attribute-map 컨피그레이션 모드로 들어갑니다. 이 명령에서 "ldap" 뒤에 하이픈이 없음에 유의하십시오.
2. ldap-attribute-map 컨피그레이션 모드에서 **map-name** 및 **map-value** 명령을 사용하여 특성 매핑 컨피그레이션을 채웁니다.
3. aaa-server host 모드에서 **ldap-attribute-map** 명령을 사용하여 특성 맵 컨피그레이션을 LDAP 서버에 바인딩합니다.

예

aaa-server host 컨피그레이션 모드에서 입력하는 다음 명령 예는 myldapmap이라는 기존의 특성 맵을 ldapsvr1이라는 LDAP 서버에 바인딩합니다.

```
ciscoasa(config)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map myldapmap
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
ldap attribute-map(글로벌 컨피그레이션 모드))	사용자 정의 특성 이름을 Cisco LDAP 특성 이름에 매핑하기 위한 LDAP 특성 맵을 생성하고 이름을 지정합니다.
map-name	Cisco LDAP 특성 이름을 이용해 사용자 정의 LDAP 특성 이름을 매핑합니다.
map-value	사용자 정의 특성 값을 Cisco 특성에 매핑합니다.
show running-config ldap attribute-map	실행 중인 특정 ldap 특성 매핑 컨피그레이션 또는 실행 중인 모든 특성 매핑 컨피그레이션을 표시합니다.
clear configure ldap attribute-map	모든 LDAP 특성 맵을 제거합니다.

ldap-base-dn

서버가 권한 부여 요청을 받으면 검색을 시작해야 하는 LDAP 계층 구조의 위치를 지정하려면 aaa-server host 컨피그레이션 모드에서 **ldap-base-dn** 명령을 사용합니다. aaa-server host 컨피그레이션 모드는 aaa-server protocol 컨피그레이션 모드에서 액세스할 수 있습니다. 이 사양을 제거하고 목록의 위부터 시작되도록 검색을 재설정하려면 이 명령의 **no** 형식을 사용합니다.

ldap-base-dn *string*

no ldap-base-dn

구문 설명

string	서버가 권한 부여 요청을 받으면 검색을 시작해야 하는 LDAP 계층 구조에서 위치를 지정하는 최대 128자의 대/소문자 구분 문자열(예: OU=Cisco). 문자열에서 공백은 허용되지 않지만, 다른 특수 문자는 사용 가능합니다.

기본값

목록의 위부터 검색을 시작합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 LDAP 서버에 대해서만 유효합니다.

예

다음 예는 호스트 1.2.3.4에서 srvgrp1이라는 LDAP AAA 서버를 구성하고, 시간 제한 간격을 9초로 설정하고, 재시도 간격을 7초로 설정하며, LDAP Base DN을 starthere로 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# exit
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
ldap-scope	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 수행할 범위를 지정합니다.
ldap-naming-attribute	LDAP 서버의 엔트리를 고유하게 식별하는 Relative Distinguished Name 특성을 지정합니다.
ldap-login-dn	시스템이 바인딩해야 하는 디렉토리 객체의 이름을 지정합니다.
ldap-login-password	로그인 DN에 대한 비밀번호를 지정합니다.

ldap-defaults

LDAP 기본값을 정의하려면 crl configure 컨피그레이션 모드에서 **ldap-defaults** 명령을 사용합니다. Crl configure 컨피그레이션 모드는 crypto ca trustpoint 컨피그레이션 모드에서 액세스할 수 있습니다. LDAP 서버에서 필요로 하는 경우에만 이러한 기본값이 사용됩니다. LDAP 기본값을 지정하지 않으려면 이 명령의 **no** 형식을 사용합니다.

ldap-defaults *server* [*port*]

no ldap-defaults

구문 설명

port	(선택 사항) LDAP 서버 포트를 지정합니다. 이 매개변수를 지정하지 않으면 ASA는 표준 LDAP 포트(389)를 사용합니다.
server	LDAP 서버의 IP 주소 또는 도메인 이름을 지정합니다. CRL 배포 지점 내에 값이 있는 경우에는 기존 값이 새 값을 재지정합니다.

기본값

기본값은 설정되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crl configure 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 기본 포트(389)에서 LDAP 기본값을 정의합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-defaults ldapdomain4 8389
```

관련 명령

명령	설명
crl configure	ca-crl 컨피그레이션 모드로 들어갑니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드로 들어갑니다.
protocol ldap	CRL의 검색 방법으로서 LDAP를 지정합니다.

ldap-dn

CRL 검색에 인증을 요청하는 LDAP 서버로 X.500 고유 이름과 비밀번호를 전달하려면 crl configure 컨피그레이션 모드에서 **ldap-dn** 명령을 사용합니다. Crl configure 컨피그레이션 모드는 crypto ca trustpoint 컨피그레이션 모드에서 액세스할 수 있습니다. LDAP 서버에서 필요로 하는 경우에만 이러한 매개변수가 사용됩니다. LDAP DN을 지정하지 않으려면 이 명령의 **no** 형식을 사용합니다.

ldap-dn *x.500-name password*

no ldap-dn

구문 설명

password	이 고유 이름에 대한 비밀번호를 정의합니다. 최대 필드 길이는 128자입니다.
x.500-name	이 CRL 데이터베이스에 액세스하기 위한 디렉토리 경로를 정의합니다(예: cn=crl,ou=certs,o=CAName,c=US). 최대 필드 길이는 128자입니다.

기본값

기본값은 설정되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crl configure 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 trustpoint central에 대해 X.500 이름 CN=admin,OU=devtest,O=engineering 및 비밀번호 xxzzyy를 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

관련 명령

명령	설명
crl configure	crl configure 컨피그레이션 모드로 들어갑니다.
crypto ca trustpoint	ca trustpoint 컨피그레이션 모드로 들어갑니다.
protocol ldap	CRL의 검색 방법으로서 LDAP를 지정합니다.

ldap-group-base-dn

그룹 검색을 위해 동적 액세스 정책에서 사용하는 Active Directory 계층 구조에서 기본 그룹을 지정하려면 aaa-server host 컨피그레이션 모드에서 **ldap-group-base-dn** 명령을 사용합니다. 실행 중인 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ldap-group-base-dn [*string*]

no ldap-group-base-dn [*string*]

구문 설명

string	서버가 검색을 시작해야 하는 Active Directory 계층 구조에서 위치를 지정하는 최대 128자의 대/소문자 구분 문자열(예: ou=Employees). 문자열에서 공백은 허용되지 않지만, 다른 특수 문자는 사용 가능합니다.

기본값

기본 동작 또는 값이 없습니다. 그룹 검색 DN을 지정하지 않으면 검색은 Base DN에서 시작됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
aaa-server host 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(4)	이 명령이 추가되었습니다.

사용 지침

ldap-group-base-dn 명령은 LDAP를 사용하는 Active Directory 서버에만 적용되며, **show ad-groups** 명령이 그룹 검색을 시작하기 위해 사용하는 Active Directory 계층 구조 수준을 지정합니다. 검색에서 반환되는 그룹은 동적 그룹 정책에서 특정 정책에 대한 선택 기준으로 사용됩니다.

예

다음 예는 그룹 Base DN이 ou(organization unit) 수준 Employees에서 검색을 시작하도록 설정합니다.

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

관련 명령

명령	설명
group-search-timeout	ASA가 그룹 목록에 대한 Active Directory 서버의 응답을 기다리는 시간을 조정합니다.
show ad-groups	Active Directory 서버에 나열되는 그룹을 표시합니다.

ldap-login-dn

시스템이 바인딩해야 하는 디렉토리 객체의 이름을 지정하려면 aaa-server host 컨피그레이션 모드에서 **ldap-login-dn** 명령을 사용합니다. aaa-server host 컨피그레이션 모드는 aaa-server protocol 컨피그레이션 모드에서 액세스할 수 있습니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ldap-login-dn *string*

no ldap-login-dn

구문 설명

string	대/소문자를 구분하는 최대 128자의 문자열로서 LDAP 계층 구조에서 디렉토리 객체의 이름을 지정합니다. 문자열에서 공백은 허용되지 않지만, 다른 특수 문자는 사용 가능합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 LDAP 서버에 대해서만 유효합니다. 지원되는 최대 문자열 길이는 128자입니다.

Microsoft Active Directory 서버를 비롯한 일부 LDAP 서버에서 ASA는 다른 LDAP 운영에 대한 요청을 허용하기 전에 인증된 바인딩을 통해 핸드셰이크를 설정합니다. ASA는 사용자 인증 요청에 Login DN 필드를 추가하는 방법으로 인증 바인딩에서 스스로를 식별합니다. Login DN 필드는 ASA의 인증 특성을 설명합니다. 이러한 특성은 관리자 권한이 있는 사용자의 특성과 일치해야 합니다.

string 변수의 경우 VPN Concentrator 인증 바인딩에 디렉토리 객체의 이름을 입력합니다(예: cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com). 익명 액세스의 경우 이 필드를 비워둡니다.

예

다음 예는 호스트 1.2.3.4에서 srvgrp1이라는 LDAP AAA 서버를 구성하고, 시간 제한 간격을 9초로 설정하고, 재시도 간격을 7초로 설정하며, LDAP login DN을 myobjectname으로 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-login-dn myobjectname
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
ldap-base-dn	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 시작할 위치를 지정합니다.
ldap-login-password	로그인 DN에 대한 비밀번호를 지정합니다. 이 명령은 LDAP 서버에 대해서만 유효합니다.
ldap-naming-attribute	LDAP 서버의 엔트리를 고유하게 식별하는 Relative Distinguished Name 특성을 지정합니다.
ldap-scope	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 수행할 범위를 지정합니다.

ldap-login-password

LDAP 서버에 대한 로그인 비밀번호를 지정하려면 aaa-server host 컨피그레이션 모드에서 **ldap-login-password** 명령을 사용합니다. aaa-server host 컨피그레이션 모드는 aaa-server protocol 컨피그레이션 모드에서 액세스할 수 있습니다. 이 비밀번호 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ldap-login-password *string*

no ldap-login-password

구문 설명

string	대/소문자를 구분하는 최대 64자의 영숫자 비밀번호. 비밀번호에는 공백 문자를 포함할 수 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 LDAP 서버에 대해서만 유효합니다. 최대 비밀번호 문자열 길이는 64자입니다.

예

다음 예는 호스트 1.2.3.4에서 srvgrp1이라는 LDAP AAA 서버를 구성하고, 시간 제한 간격을 9초로 설정하고, 재시도 간격을 7초로 설정하며, LDAP 로그인 비밀번호를 obscurepassword로 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server)# timeout 9
ciscoasa(config-aaa-server)# retry 7
ciscoasa(config-aaa-server)# ldap-login-password obscurepassword
ciscoasa(config-aaa-server)#
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
ldap-base-dn	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 시작할 위치를 지정합니다.
ldap-login-dn	시스템이 바인딩해야 하는 디렉토리 객체의 이름을 지정합니다.
ldap-naming-attribute	LDAP 서버의 엔트리를 고유하게 식별하는 Relative Distinguished Name 특성을 지정합니다.
ldap-scope	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 수행할 범위를 지정합니다.

ldap-naming-attribute

Relative Distinguished Name 특성을 지정하려면 aaa-server host 컨피그레이션 모드에서 **ldap-naming-attribute** 명령을 사용합니다. aaa-server host 컨피그레이션 모드는 aaa-server protocol 컨피그레이션 모드에서 액세스할 수 있습니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ldap-naming-attribute *string*

no ldap-naming-attribute

구문 설명

string	대/소문자를 구분하는 최대 127자의 영숫자 Relative Distinguished Name 특성으로, LDAP 서버에서 엔트리를 고유하게 식별합니다. 문자열에서 공백은 허용되지 않지만, 다른 특수 문자는 사용 가능합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

LDAP 서버의 엔트리를 고유하게 식별하는 Relative Distinguished Name 특성을 입력합니다. 일반적인 사용되는 명명 특성은 Common Name(cn) 및 User ID(uid)입니다.

이 명령은 LDAP 서버에 대해서만 유효합니다. 지원되는 최대 문자열 길이는 128자입니다.

예

다음 예는 호스트 1.2.3.4에서 srvgrp1이라는 LDAP AAA 서버를 구성하고, 시간 제한 간격을 9초로 설정하고, 재시도 간격을 7초로 설정하며, LDAP 명명 특성을 cn으로 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-naming-attribute cn
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
ldap-base-dn	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 시작할 위치를 지정합니다.
ldap-login-dn	시스템이 바인딩해야 하는 디렉토리 객체의 이름을 지정합니다.
ldap-login-password	로그인 DN에 대한 비밀번호를 지정합니다. 이 명령은 LDAP 서버에 대해서만 유효합니다.
ldap-scope	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 수행할 범위를 지정합니다.

ldap-over-ssl

ASA와 LDAP 서버 간에 안전한 SSL 연결을 설정하려면 aaa-server host 컨피그레이션 모드에서 **ldap-over-ssl** 명령을 사용합니다. 연결에 대해 SSL을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ldap-over-ssl enable

no ldap-over-ssl enable

구문 설명

enable	SSL이 LDAP 서버에 대한 연결을 보호하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

SSL이 ASA와 LDAP 서버 간 연결을 보호하도록 지정하려면 이 명령을 사용합니다.

참고 일반 텍스트 인증을 사용하는 경우 이 기능을 활성화하는 것이 좋습니다. **sasl-mechanism** 명령을 참조하십시오.

예

aaa-server host 컨피그레이션 모드에서 입력하는 다음 명령은 ASA와 LDAP 서버(이름: ldapsvr1, IP 주소: 10.10.0.1) 간 연결을 위해 SSL을 활성화합니다. 또한 일반 SASL 인증 메커니즘도 구성합니다.

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
sasl-mechanism	LDAP 클라이언트와 서버 간 SASL 인증을 지정합니다.
server-type	LDAP 서버 공급업체를 Microsoft 또는 Sun으로 지정합니다.
ldap attribute-map(글로벌 컨피그레이션 모드))	사용자 정의 특성 이름을 Cisco LDAP 특성 이름에 매핑하기 위한 LDAP 특성 맵을 생성하고 이름을 지정합니다.

ldap-scope

서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 수행해야 할 범위를 지정하려면 aaa-server host 컨피그레이션 모드에서 **ldap-scope** 명령을 사용합니다. aaa-server host 컨피그레이션 모드는 aaa-server protocol 컨피그레이션 모드에서 액세스할 수 있습니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ldap-scope *scope*

no ldap-scope

구문 설명

scope	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 시작할 LDAP 계층 구조의 수준 범위를 지정합니다. 유효한 값: • **onelevel** - Base DN의 바로 아래 수준 하나만 검색합니다. • **subtree** - Base DN 아래의 모든 수준을 검색합니다.

기본값

기본값은 **onelevel**입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

범위를 **onelevel**로 지정하면 Base DN 바로 아래 수준 하나만 검색하므로 더 빠른 검색이 가능합니다. **subtree**를 지정하면 Base DN 아래의 모든 수준을 검색하므로 속도가 더 느려집니다.

이 명령은 LDAP 서버에 대해서만 유효합니다.

예

다음 예는 호스트 1.2.3.4에서 srvgrp1이라는 LDAP AAA 서버를 구성하고, 시간 제한 간격을 9초로 설정하고, 재시도 간격을 7초로 설정하며, LDAP 범위에 하위 트리 수준을 포함하도록 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
ldap-base-dn	서버가 권한 부여 요청을 받으면 LDAP 계층 구조에서 검색을 시작할 위치를 지정합니다.
ldap-login-dn	시스템이 바인딩해야 하는 디렉토리 객체의 이름을 지정합니다.
ldap-login-password	로그인 DN에 대한 비밀번호를 지정합니다. 이 명령은 LDAP 서버에 대해서만 유효합니다.
ldap-naming-attribute	LDAP 서버의 엔트리를 고유하게 식별하는 Relative Distinguished Name 특성을 지정합니다.

leap-bypass

LEAP Bypass를 활성화하려면 그룹 정책 컨피그레이션 모드에서 **leap-bypass enable** 명령을 사용합니다. LEAP Bypass를 비활성화하려면 **leap-bypass disable** 명령을 사용합니다. 실행 중인 컨피그레이션에서 LEAP Bypass 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션은 다른 그룹 정책으로부터 LEAP Bypass의 값을 상속하도록 허용합니다.

leap-bypass {**enable** | **disable**}

no leap-bypass

구문 설명

disable	LEAP Bypass를 비활성화합니다.
enable	LEAP Bypass를 활성화합니다.

기본값

LEAP Bypass가 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

LEAP Bypass를 활성화하면, VPN 하드웨어 클라이언트 뒤에 있는 무선 디바이스에서 오는 LEAP 패킷이 사용자 인증에 앞서 VPN 터널을 통과할 수 있습니다. 따라서 Cisco 무선 액세스 포인트 디바이스를 사용하는 워크스테이션에서 LEAP 인증을 설정할 수 있습니다. 그런 다음 디바이스에서 사용자 인증 단위로 다시 인증할 수 있습니다.

상호 작용 하드웨어 클라이언트 인증을 활성화하면 이 기능이 예상대로 작동하지 않습니다.

자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

참고 무단 트래픽의 터널 통과를 허용할 보안 위험 가능성이 있습니다.

예

다음 예는 그룹 정책 "FirstGroup"에 대해 LEAP Bypass를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# leap-bypass enable
```

관련 명령

명령	설명
secure-unit-authentication	클라이언트가 터널을 시작할 때마다 VPN 하드웨어 클라이언트에서 사용자 이름 및 비밀번호로 인증하도록 요청합니다.
user-authentication	VPN 하드웨어 클라이언트 뒤의 사용자가 연결 전에 ASA에 대해 스스로를 인증해야 합니다.

license

요청이 어느 조직에서 오는지 나타내기 위해 ASA가 Cloud Web Security 프록시 서버로 전송하는 인증 키를 구성하려면 scansafe general-options 컨피그레이션 모드에서 **license** 명령을 사용합니다. 라이센스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

license *hex_key*

no license [*hex_key*]

구문 설명

hex_key	인증 키를 16바이트 16진수로 지정합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

명령 모드	방화벽 모드		보안 컨텍스트		
				다중	
	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

각 ASA는 Cloud Web Security에서 가져온 인증 키를 사용해야 합니다. 인증 키를 통해 Cloud Web Security는 웹 요청과 연결된 회사를 식별할 수 있으며, 인증 키를 사용하면 ASA가 유효한 고객과 연결되었음을 확인할 수 있습니다.

ASA에 대해 다음의 두 가지 인증 키 유형(회사 키 및 그룹 키) 중 하나를 사용할 수 있습니다.

회사 인증 키

회사 인증 키는 동일한 회사 내 여러 ASA에서 사용할 수 있습니다. 이 키는 단순히 ASA에 대한 Cloud Web Security 서비스를 활성화합니다. 관리자는 ScanCenter(https://scancenter.scansafe.com/portal/admin/login.jsp)에서 이 키를 생성하며, 나중에 사용하도록 이메일로 이 키를 보낼 수 있습니다. 나중에 ScanCenter에서 이 키를 찾을 수 없습니다. ScanCenter에서는 마지막 4자만 표시됩니다. 자세한 내용은 다음의 Cloud Web Security 설명서를 참조하십시오. http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html.

그룹 인증 키

그룹 인증 키는 각 ASA에 대해 고유한 특수 키로서 두 가지 기능을 수행합니다.

- 하나의 ASA에 대해 Cloud Web Security 서비스를 활성화합니다.
- ASA에 대한 ScanCenter 정책을 만들 수 있도록 ASA에서 오는 모든 트래픽을 식별합니다.

관리자는 ScanCenter(https://scancenter.scansafe.com/portal/admin/login.jsp)에서 이 키를 생성하며, 나중에 사용하도록 이메일로 이 키를 보낼 수 있습니다. 나중에 ScanCenter에서 이 키를 찾을 수 없습니다. ScanCenter에서는 마지막 4자만 표시됩니다. 자세한 내용은 다음의 Cloud Web Security 설명서를 참조하십시오. http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html.

예

다음 예는 기본 서버만 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	화이트리스트에 있는 사용자 및 그룹에 대한 검사 클래스 맵을 만듭니다.
default user group	ASA에서 ASA로 들어오는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**] (parameters)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스에서 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
match user group	화이트리스트를 기준으로 사용자 또는 그룹을 확인합니다.
policy-map type inspect scansafe	규칙에 대한 필수 매개변수를 구성하고 선택적으로 화이트리스트를 식별할 수 있도록 검사 정책 맵을 만듭니다.
retry-count	ASA 프록시 서버를 폴링하여 가용성 여부를 확인하기까지 Cloud Web Security에서 대기하는 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 컨텍스트 모드에서는 컨텍스트 단위로 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 정규화된 도메인 이름 또는 IP 주소를 구성합니다.
show conn scansafe	모든 Cloud Web Security 연결을 보여줍니다(대문자 Z 플래그로 표시됨).
show scansafe server	서버의 상태, 즉 현재 활성 서버인지, 백업 서버인지 또는 도달할 수 없는 서버인지를 보여줍니다.
show scansafe statistics	전체 및 현재 http 연결을 보여줍니다.
user-identity monitor	지정된 사용자 또는 그룹 정보를 AD 에이전트에서 다운로드합니다.
whitelist	트래픽의 클래스에 대해 화이트리스트 작업을 수행합니다.

license-server address

참가자가 사용할 공유 라이센스 서버 IP 주소 및 공유 암호를 식별하려면 글로벌 컨피그레이션 모드에서 **license-server address** 명령을 사용합니다. 공유 라이센스에 대한 참가를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 공유 라이센스를 사용하면 SSL VPN 세션을 대량으로 구매할 수 있으며, ASA 중 하나를 공유 라이센스 서버로 구성하고 나머지는 공유 라이센스 참가자로 구성하여 필요에 따라 ASA의 그룹 간에 세션을 공유할 수 있습니다.

license-server address *address* **secret** *secret* [**port** *port*]

no license-server address [*address* **secret** *secret* [**port** *port*]]

구문 설명

address	공유 라이센스 서버 IP 주소를 식별합니다.
port *port*	(선택 사항) **license-server port** 명령을 사용하여 서버 컨피그레이션에서 기본 포트를 변경한 경우, 일치를 확인할 백업 서버용 포트를 1~65535 범위로 설정합니다. 기본 포트는 50554입니다.
secret *secret*	공유 암호를 식별합니다. 암호는 **license-server secret** 명령을 사용하여 서버에 설정한 암호와 일치해야 합니다.

명령 기본값

기본 포트는 50554입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

공유 라이센스 참가자에는 공유 라이센스 참가자 키가 있어야 합니다. 설치된 라이센스를 확인하려면 **show activation-key** 명령을 사용합니다.

참가자당 공유 라이센스 서버를 하나만 지정할 수 있습니다.

다음 단계에서는 공유 라이센스가 어떤 방식으로 운영되는지 설명합니다.

1. 어떤 ASA가 공유 라이센스 서버가 되어야 하는지 결정하고, 디바이스 일련 번호를 사용하여 공유 라이센스 서버의 라이센스를 구매합니다.
2. 어떤 ASA가 공유 라이센스 참가자(공유 백업 서버 포함)가 되어야 하는지 결정하고, 각 디바이스 일련 번호를 사용하여 각 디바이스의 공유 라이센스 참가자 라이센스를 얻습니다.
3. (선택 사항) 두 번째 ASA를 공유 라이센스 백업 서버로 지정합니다. 하나의 백업 서버만 지정할 수 있습니다.

참고 공유 라이센스 백업 서버에는 참가자 라이센스만 필요합니다.

4. 공유 라이센스 서버에서 공유 암호를 구성합니다. 공유 암호를 보유한 모든 참가자는 공유 라이센스를 사용할 수 있습니다.
5. ASA를 참가자로 지정하면 ASA에서는 로컬 라이센스 및 모델 정보를 비롯한 자체 정보를 전송하여 공유 라이센스 서버에 등록됩니다.

참고 참가자는 IP 네트워크를 통해 서버와 통신을 수행할 수 있어야 하며, 같은 서브넷에 있을 필요는 없습니다.

6. 공유 라이센스 서버에서는 참가자가 서버에 폴링하는 빈도와 관련된 정보에 응답합니다.
7. 참가자가 로컬 라이센스의 세션을 모두 사용할 경우, 추가 세션을 50-세션 늘려달라는 요청이 공유 서버에 전송됩니다.
8. 공유 라이센스 서버에서는 공유 라이센스에 응답합니다. 참가자가 사용한 총 세션 수는 플랫폼 모델의 최대 세션 수를 초과할 수 없습니다.

참고 로컬 세션이 부족해지면 공유 라이센스 서버는 공유 라이센스 풀에도 참가할 수 있습니다. 참가를 위해 참가자 라이센스 및 서버 라이센스를 구매하지 않아도 됩니다.

   a. 공유 라이센스 풀에 참가자가 사용할 세션이 충분히 남아 있지 않은 경우, 서버에서는 최대한 사용 가능한 세션 수에 응답합니다.
   b. 참가자는 서버에서 요청을 충분히 충족할 때까지 추가 세션을 요청하는 새로 고침 메시지를 계속 전송하게 됩니다.

9. 참가자에 대한 로드가 줄어들면 공유 세션을 릴리스하라는 메시지가 서버에 전송됩니다.

참고 ASA에서는 서버와 참가자 간에 SSL을 사용하여 모든 통신을 암호화합니다.

참가자와 서버 간의 통신 문제

참가자와 서버 간의 통신 문제에 대한 내용은 다음 지침을 참조하십시오.

- 참가자가 새로 고침 간격이 3번 지난 후 새로 고침 메시지를 전송하지 못하면 서버에서는 공유 라이센스 풀에 세션을 다시 릴리스합니다.
- 참가자가 새로 고침을 전송할 라이센스 서버에 도달하지 못할 경우, 참가자는 서버에서 받은 공유 라이센스를 최대 24시간 동안 계속 사용할 수 있습니다.
- 24시간 후에도 참가자가 라이센스 서버와 계속 통신을 수행하지 못하면, 세션이 여전히 필요한 경우에도 참가자는 공유 라이센스를 릴리스합니다. 참가자는 설정된 기존 연결을 남겨두지만 라이센스 제한을 넘는 새 연결은 수락할 수 없습니다.
- 참가자가 24시간이 만료되기 전에 서버에 다시 연결하였으나 서버에서 참가자 세션이 만료된 경우, 참가자는 해당 세션에 대해 새 요청을 전송해야 합니다. 서버에서는 참가자에게 다시 할당할 수 있는 최대한 많은 수의 세션에 응답합니다.

예

다음 예에서는 라이센스 서버 IP 주소와 공유 비밀 및 백업 라이센스 서버 IP 주소를 설정합니다.

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server backup address	참가자용 공유 라이센스 백업 서버를 식별합니다.
license-server backup backup-id	주 공유 라이센스 서버용 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server backup enable	유닛을 활성화하여 공유 라이센스 백업 서버가 되도록 합니다.
license-server enable	유닛을 활성화하여 공유 라이센스 서버가 되도록 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server refresh-interval	참가자에게 제공되어 참가자가 서버와 통신해야 하는 새로 고침 빈도를 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

license-server backup address

참가자가 사용할 공유 라이센스 백업 서버 IP 주소를 식별하려면 글로벌 컨피그레이션 모드에서 **license-server backup address** 명령을 사용합니다. 백업 서버의 사용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

license-server backup address *address*

no license-server address [*address*]

구문 설명

address	공유 라이센스 백업 서버 IP 주소를 식별합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

공유 라이센스 백업 서버를 사용하려면 **license-server backup enable** 명령을 미리 구성해야 합니다.

예

다음 예에서는 라이센스 서버 IP 주소와 공유 비밀 및 백업 라이센스 서버 IP 주소를 설정합니다.

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자용 공유 라이센스 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup backup-id	주 공유 라이센스 서버용 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server backup enable	유닛을 활성화하여 공유 라이센스 백업 서버가 되도록 합니다.
license-server enable	유닛을 활성화하여 공유 라이센스 서버가 되도록 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server refresh-interval	참가자에게 제공되어 참가자가 서버와 통신해야 하는 새로 고침 빈도를 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

license-server backup backup-id

주 공유 라이센스 서버 컨피그레이션에서 공유 라이센스 백업 서버를 식별하려면 글로벌 컨피그레이션 모드에서 **license-server backup backup-id** 명령을 사용합니다. 백업 서버 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

no license-server backup *address* [**backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]]

구문 설명

address	공유 라이센스 백업 서버 IP 주소를 식별합니다.
backup-id *serial_number*	공유 라이센스 백업 서버 일련 번호를 식별합니다.
ha-backup-id *ha_serial_number*	백업 서버를 위한 장애 조치를 사용하는 경우 보조 공유 라이센스 백업 서버 일련 번호를 식별합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

1개의 백업 서버 및 선택적 스탠바이 유닛만 식별할 수 있습니다.

백업 서버 일련 번호를 보려면 **show activation-key** 명령을 입력합니다.

참가자를 활성화하여 백업 서버가 되도록 하려면 **license-server backup enable** 명령을 사용합니다.

백업 역할을 수행할 수 있도록 하려면 공유 라이센스 백업 서버를 기본 공유 라이센스 서버로 올바르게 등록해야 합니다. 등록이 완료되면 기본 공유 라이센스 서버 설정 및 공유 라이센스 정보(예: 등록된 참가자 목록 및 현재 라이센스 사용량 포함)가 백업과 동기화됩니다. 기본 서버 및 백업 서버에서는 10초 간격으로 데이터를 동기화합니다. 최초 동기화를 완료하면 백업 서버에서는 다시 로드된 경우에도 백업 업무를 성공적으로 수행할 수 있습니다.

기본 서버가 중단되면 백업 서버에서 서버 작업을 이어받습니다. 백업 서버의 참가자에 대한 발급 세션이 중단되고, 기존 세션이 만료된 후 백업 서버에서는 최대 30일간 연속으로 작업을 수행할 수 있습니다. 30일 내에 기본 서버를 복구해야 합니다. 15일에 중요도가 높은 syslog 메시지가 전송되며 30일에 다시 한 번 전송됩니다.

기본 서버가 다시 가동되면 기본 서버에서는 백업 서버와 동기화를 수행한 후 서버 작업을 이어받습니다.

백업 서버가 활성화되어 있지 않을 때에는 기본 공유 라이센스 서버의 일반 참가자 역할을 수행합니다.

참고 기본 공유 라이센스 서버를 처음 시작할 경우, 백업 서버는 개별적으로 5일 동안만 작동될 수 있습니다. 작동 한도는 30일에 도달할 때까지 일별로 증가합니다. 또한 기본 서버가 해당 기간에 중단될 경우, 백업 서버의 작동 한도는 일별로 감소합니다. 기본 서버가 다시 작동되면 백업 서버의 한도는 다시 일별로 증가합니다. 예를 들어, 기본 서버가 20일간 중단되었고 백업 서버가 해당 기간 동안 활성화되어 있었다면, 백업 서버의 남은 기간 한도는 10일밖에 되지 않습니다. 백업 서버에서는 20일 이상 백업을 비활성 상태로 유지한 후 최대 30일을 "재충전"할 수 있습니다. 이러한 재충전 기능은 공유 라이센스의 남용을 줄이기 위해 구현되었습니다.

예

다음 예에서는 공유 암호를 설정하고, 새로 고침 간격 및 포트를 변경하고, 백업 서버를 구성하고, 내부 인터페이스 및 dmz 인터페이스에서 이러한 유닛을 공유 라이센스 서버로서 활성화합니다.

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자용 공유 라이센스 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup address	참가자용 공유 라이센스 백업 서버를 식별합니다.
license-server backup enable	유닛을 활성화하여 공유 라이센스 백업 서버가 되도록 합니다.
license-server enable	유닛을 활성화하여 공유 라이센스 서버가 되도록 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server refresh-interval	참가자에게 제공되어 참가자가 서버와 통신해야 하는 새로 고침 빈도를 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

license-server backup enable

이 유닛을 공유 라이센스 백업 서버로서 활성화하려면 글로벌 컨피그레이션 모드에서 **license-server backup enable** 명령을 사용합니다. 백업 서버를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

license-server backup enable *interface_name*

no license-server enable *interface_name*

구문 설명

interface_name	참가자가 백업 서버에 접속하는 인터페이스를 지정합니다. 이 명령을 원하는 인터페이스 수에 반복할 수 있습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

백업 서버에는 공유 라이센스 참가자 키가 있어야 합니다.

백업 역할을 수행할 수 있도록 하려면 공유 라이센스 백업 서버를 기본 공유 라이센스 서버로 올바르게 등록해야 합니다. 등록이 완료되면 기본 공유 라이센스 서버 설정 및 공유 라이센스 정보(예: 등록된 참가자 목록 및 현재 라이센스 사용량 포함)가 백업과 동기화됩니다. 기본 서버 및 백업 서버에서는 10초 간격으로 데이터를 동기화합니다. 최초 동기화를 완료하면 백업 서버에서는 다시 로드된 경우에도 백업 업무를 성공적으로 수행할 수 있습니다.

기본 서버가 중단되면 백업 서버에서 서버 작업을 이어받습니다. 백업 서버의 참가자에 대한 발급 세션이 중단되고, 기존 세션이 만료된 후 백업 서버에서는 최대 30일간 연속으로 작업을 수행할 수 있습니다. 30일 내에 기본 서버를 복구해야 합니다. 15일에 중요도가 높은 syslog 메시지가 전송되며 30일에 다시 한 번 전송됩니다.

기본 서버가 다시 가동되면 기본 서버에서는 백업 서버와 동기화를 수행한 후 서버 작업을 이어받습니다.

백업 서버가 활성화되어 있지 않을 때에는 기본 공유 라이센스 서버의 일반 참가자 역할을 수행합니다.

참고 기본 공유 라이센스 서버를 처음 시작할 경우, 백업 서버는 개별적으로 5일 동안만 작동될 수 있습니다. 작동 한도는 30일에 도달할 때까지 일별로 증가합니다. 또한 기본 서버가 해당 기간에 중단될 경우, 백업 서버의 작동 한도는 일별로 감소합니다. 기본 서버가 다시 작동되면 백업 서버의 한도는 다시 일별로 증가합니다. 예를 들어, 기본 서버가 20일간 중단되었고 백업 서버가 해당 기간 동안 활성화되어 있었다면, 백업 서버의 남은 기간 한도는 10일밖에 되지 않습니다. 백업 서버에서는 20일 이상 백업을 비활성 상태로 유지한 후 최대 30일을 "재충전"할 수 있습니다. 이러한 재충전 기능은 공유 라이센스의 남용을 줄이기 위해 구현되었습니다.

예

다음 예에서는 라이센스 서버 및 공유 암호를 식별하고, 내부 인터페이스 및 dmz 인터페이스에서 이 유닛을 백업 공유 라이센스 서버로서 활성화합니다.

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자용 공유 라이센스 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup address	참가자용 공유 라이센스 백업 서버를 식별합니다.
license-server backup backup-id	주 공유 라이센스 서버용 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server enable	유닛을 활성화하여 공유 라이센스 서버가 되도록 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server refresh-interval	참가자에게 제공되어 참가자가 서버와 통신해야 하는 새로 고침 빈도를 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

license-server enable

이 유닛을 공유 라이센스 서버로서 식별하려면 글로벌 컨피그레이션 모드에서 **license-server enable** 명령을 사용합니다. 공유 라이센스 서버를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 공유 라이센스를 사용하면 SSL VPN 세션을 대량으로 구매할 수 있으며, ASA 중 하나를 공유 라이센스 서버로 구성하고 나머지는 공유 라이센스 참가자로 구성하여 필요에 따라 ASA의 그룹 간에 세션을 공유할 수 있습니다.

license-server enable *interface_name*

no license-server enable *interface_name*

구문 설명

interface_name	참가자가 서버에 접속하는 인터페이스를 지정합니다. 이 명령을 원하는 인터페이스 수에 반복할 수 있습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

공유 라이센스 서버에는 공유 라이센스 서버 키가 있어야 합니다. 설치된 라이센스를 확인하려면 **show activation-key** 명령을 사용합니다.

다음 단계에서는 공유 라이센스가 어떤 방식으로 운영되는지 설명합니다.

1. 어떤 ASA가 공유 라이센스 서버가 되어야 하는지 결정하고, 디바이스 일련 번호를 사용하여 공유 라이센스 서버의 라이센스를 구매합니다.
2. 어떤 ASA가 공유 라이센스 참가자(공유 백업 서버 포함)가 되어야 하는지 결정하고, 각 디바이스 일련 번호를 사용하여 각 디바이스의 공유 라이센스 참가자 라이센스를 얻습니다.
3. (선택 사항) 두 번째 ASA를 공유 라이센스 백업 서버로 지정합니다. 하나의 백업 서버만 지정할 수 있습니다.

   참고 공유 라이센스 백업 서버에는 참가자 라이센스만 필요합니다.

4. 공유 라이센스 서버에서 공유 암호를 구성합니다. 공유 암호를 보유한 모든 참가자는 공유 라이센스를 사용할 수 있습니다.

5. ASA를 참가자로 지정하면 ASA에서는 로컬 라이센스 및 모델 정보를 비롯한 자체 정보를 전송하여 공유 라이센스 서버에 등록됩니다.

참고 참가자는 IP 네트워크를 통해 서버와 통신을 수행할 수 있어야 하며, 같은 서브넷에 있을 필요는 없습니다.

6. 공유 라이센스 서버에서는 참가자가 서버에 폴링하는 빈도와 관련된 정보에 응답합니다.
7. 참가자가 로컬 라이센스의 세션을 모두 사용할 경우, 추가 세션을 50-세션 늘려달라는 요청이 공유 서버에 전송됩니다.
8. 공유 라이센스 서버에서는 공유 라이센스에 응답합니다. 참가자가 사용한 총 세션 수는 플랫폼 모델의 최대 세션 수를 초과할 수 없습니다.

참고 로컬 세션이 부족해지면 공유 라이센스 서버는 공유 라이센스 풀에도 참가할 수 있습니다. 참가를 위해 참가자 라이센스 및 서버 라이센스를 구매하지 않아도 됩니다.

   a. 공유 라이센스 풀에 참가자가 사용할 세션이 충분히 남아 있지 않은 경우, 서버에서는 최대한 사용 가능한 세션 수에 응답합니다.
   b. 참가자는 서버에서 요청을 충분히 충족할 때까지 추가 세션을 요청하는 새로 고침 메시지를 계속 전송하게 됩니다.
9. 참가자에 대한 로드가 줄어들면 공유 세션을 릴리스하라는 메시지가 서버에 전송됩니다.

참고 ASA에서는 서버와 참가자 간에 SSL을 사용하여 모든 통신을 암호화합니다.

참가자와 서버 간의 통신 문제

참가자와 서버 간의 통신 문제에 대한 내용은 다음 지침을 참조하십시오.

- 참가자가 새로 고침 간격이 3번 지난 후 새로 고침 메시지를 전송하지 못하면 서버에서는 공유 라이센스 풀에 세션을 다시 릴리스합니다.
- 참가자가 새로 고침을 전송할 라이센스 서버에 도달하지 못할 경우, 참가자는 서버에서 받은 공유 라이센스를 최대 24시간 동안 계속 사용할 수 있습니다.
- 24시간 후에도 참가자가 라이센스 서버와 계속 통신을 수행하지 못하면, 세션이 여전히 필요한 경우에도 참가자는 공유 라이센스를 릴리스합니다. 참가자는 설정된 기존 연결을 남겨두지만 라이센스 제한을 넘는 새 연결은 수락할 수 없습니다.
- 참가자가 24시간이 만료되기 전에 서버에 다시 연결하였으나 서버에서 참가자 세션이 만료된 경우, 참가자는 해당 세션에 대해 새 요청을 전송해야 합니다. 서버에서는 참가자에게 다시 할당할 수 있는 최대한 많은 수의 세션에 응답합니다.

예

다음 예에서는 공유 암호를 설정하고, 새로 고침 간격 및 포트를 변경하고, 백업 서버를 구성하고, 내부 인터페이스 및 dmz 인터페이스에서 이러한 유닛을 공유 라이센스 서버로서 활성화합니다.

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자용 공유 라이센스 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup address	참가자용 공유 라이센스 백업 서버를 식별합니다.
license-server backup backup-id	주 공유 라이센스 서버용 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server backup enable	유닛을 활성화하여 공유 라이센스 백업 서버가 되도록 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server refresh-interval	참가자에게 제공되어 참가자가 서버와 통신해야 하는 새로 고침 빈도를 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

license-server port

공유 라이센스 서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정하려면 글로벌 컨피그레이션 모드에서 **license-server port** 명령을 사용합니다. 기본 포트를 복원하려면 이 명령의 **no** 형식을 사용합니다.

license-server port *port*

no license-server port [*port*]

구문 설명

seconds	참가자로부터 SSL 연결을 수신하는 서버에 대한 포트 값을 1~65535 사이로 설정합니다. 기본값은 TCP 포트 50554입니다.

명령 기본값

기본 포트는 50554입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

포트를 기본값에서 변경하는 경우 **license-server address** 명령을 사용하여 각 참가자에 대해 동일한 포트를 설정해야 합니다.

예

다음 예에서는 공유 암호를 설정하고, 새로 고침 간격 및 포트를 변경하고, 백업 서버를 구성하고, 내부 인터페이스 및 DMZ 인터페이스에서 이러한 유닛을 공유 라이센스 서버로서 활성화합니다.

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자용 공유 라이센스 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup address	참가자용 공유 라이센스 백업 서버를 식별합니다.
license-server backup backup-id	주 공유 라이센스 서버용 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server backup enable	유닛을 활성화하여 공유 라이센스 백업 서버가 되도록 합니다.
license-server enable	유닛을 활성화하여 공유 라이센스 서버가 되도록 합니다.
license-server refresh-interval	참가자에게 제공되어 참가자가 서버와 통신해야 하는 새로 고침 빈도를 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

license-server refresh-interval

공유 라이센스 서버와의 통신 간격을 지정하기 위해 참가자에게 제공하는 새로 고침 간격을 설정하려면 글로벌 컨피그레이션 모드에서 **license-server refresh-interval** 명령을 사용합니다. 기본 새로 고침 간격을 복원하려면 이 명령의 **no** 형식을 사용합니다.

license-server refresh-interval *seconds*

no license-server refresh-interval [*seconds*]

구문 설명

seconds	새로 고침 간격을 10~300초 범위로 설정합니다. 기본값은 30초입니다.

명령 기본값

기본값은 30초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

각 참자가는 SSL을 사용하여 공유 라이센스 서버와 정기적으로 통신합니다. 따라서 공유 라이센스 서버는 현재 라이센스 사용을 추적할 수 있으며, 라이센스 요청을 받고 이에 응답할 수 있습니다.

예

다음 예에서는 공유 암호를 설정하고, 새로 고침 간격 및 포트를 변경하고, 백업 서버를 구성하고, 내부 인터페이스 및 dmz 인터페이스에서 이러한 유닛을 공유 라이센스 서버로서 활성화합니다.

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자용 공유 라이센스 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup address	참가자용 공유 라이센스 백업 서버를 식별합니다.
license-server backup backup-id	주 공유 라이센스 서버용 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server backup enable	유닛을 활성화하여 공유 라이센스 백업 서버가 되도록 합니다.
license-server enable	유닛을 활성화하여 공유 라이센스 서버가 되도록 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

license-server secret

공유 라이센스 서버에서 공유 암호를 설정하려면 글로벌 컨피그레이션 모드에서 **license-server secret** 명령을 사용합니다. 암호를 제거하려면 이 명령의 **no** 형식을 사용합니다.

license-server secret *secret*

no license-server secret *secret*

구문 설명

secret	4~128자의 ASCII 문자열로 된 공유 암호를 설정합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

license-server address 명령에서 식별되는 이 암호가 있는 모든 참가자는 라이센스 서버를 사용할 수 있습니다.

예

다음 예에서는 공유 암호를 설정하고, 새로 고침 간격 및 포트를 변경하고, 백업 서버를 구성하고, 내부 인터페이스 및 dmz 인터페이스에서 이러한 유닛을 공유 라이센스 서버로서 활성화합니다.

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
clear shared license	공유 라이센스 통계를 지웁니다.
license-server address	참가자용 공유 라이센스 서버 IP 주소 및 공유 암호를 식별합니다.
license-server backup address	참가자용 공유 라이센스 백업 서버를 식별합니다.
license-server backup backup-id	주 공유 라이센스 서버용 백업 서버 IP 주소 및 일련 번호를 식별합니다.
license-server backup enable	유닛을 활성화하여 공유 라이센스 백업 서버가 되도록 합니다.
license-server enable	유닛을 활성화하여 공유 라이센스 서버가 되도록 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신 대기하는 포트를 설정합니다.
license-server refresh-interval	참가자에게 제공되어 참가자가 서버와 통신해야 하는 새로 고침 빈도를 설정합니다.
show activation-key	설치된 현재 라이센스를 보여줍니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 보여줍니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

lifetime(ca server mode)

각 사용자 인증서를 발급하는 로컬 CA(Certificate Authority) 인증서 또는 CRL(Certificate Revocation List)이 유효한 상태를 유지하는 기간을 지정하려면 ca 서버 컨피그레이션 모드에서 **lifetime** 명령을 사용합니다. 수명을 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

lifetime {**ca-certificate** | **certificate** | **crl**} *time*

no lifetime {**ca-certificate** | **certificate** | **crl**}

구문 설명

ca-certificate	로컬 CA 서버 인증서의 수명을 지정합니다.
certificate	CA 서버에서 발급하는 모든 사용자 인증서의 수명을 지정합니다.
crl	CRL의 수명을 지정합니다.
time	CA 인증서 및 모든 발급된 인증서에 대해 *time*은 인증서가 유효한 상태를 유지하는 일수를 지정합니다. 유효한 범위는 1~3650일입니다. CRL의 경우 *time*은 CRL이 유효한 상태를 유지하는 일수를 지정합니다. CRL의 유효한 범위는 1~720시간입니다.

기본값

기본 수명은 다음과 같습니다.

- CA 인증서 - 3년
- 발급된 인증서 - 1년
- CRL - 6시간

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 인증서 또는 CRL이 유효한 상태를 유지하는 일수나 시간을 지정함으로써 인증서나 CRL에 포함된 만료 날짜를 결정합니다.

lifetime ca-certificate 명령은 로컬 CA 서버 인증서가 처음 생성될 때(즉, 처음에 로컬 CA 서버를 구성하고 **no shutdown** 명령을 실행할 때) 효력을 발휘합니다. CA 인증서가 만료되면, 구성된 수명 값을 사용하여 새 CA 인증서를 생성합니다. 기존 CA 인증서의 수명 값은 변경할 수 없습니다.

예

다음 예는 CA에서 3개월 동안 유효한 인증서를 발급하도록 구성합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# lifetime certificate 90
ciscoasa(config-ca-server))#
```

다음 예는 CA에서 이틀 동안 유효한 CRL을 발급하도록 구성합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# lifetime crl 48
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
cdp-url	CA에서 발급한 인증서에 포함할 인증서 폐기 목록 배포 지점(CDP)을 지정합니다.
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 ca 서버 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다.
crypto ca server crl issue	CRL을 강제로 발급합니다.
show crypto ca server	로컬 CA 컨피그레이션 세부 정보를 ASCII 텍스트로 표시합니다.
show crypto ca server cert-db	로컬 CA 서버 인증서를 표시합니다.
show crypto ca server crl	로컬 CA의 현재 CRL을 표시합니다.

lifetime(ikev2 policy mode)

AnyConnect IPsec 연결을 위한 IKEv2 SA(Security Association)에서 암호화 알고리즘을 지정하려면 IKEv2 정책 컨피그레이션 모드에서 **encryption** 명령을 사용합니다. 이 명령을 제거하고 기본 설정을 사용하려면 이 명령의 **no** 형식을 사용합니다.

lifetime {{ **seconds** *seconds*} | **none** }

구문 설명

seconds	120~2,147,483,647초 범위의 수명. 기본값은 86,400초(24시간)입니다.

기본값

기본값은 86,400초(24시간)입니다.

사용 지침

IKEv2 SA는 IKEv2 피어가 phase 2에서 안전하게 통신할 수 있도록 phase 1에서 사용되는 키입니다. SA 수명을 설정하려면 **crypto ikev2 policy** 명령을 입력한 후 **lifetime** 명령을 사용합니다.

수명은 IKEv2 SA rekey의 간격을 설정합니다. 키워드 none을 사용하면 SA의 rekey가 비활성화됩니다. 그러나 AnyConnect 클라이언트는 여전히 SA를 rekey할 수 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

예

다음 예는 IKEv2 정책 컨피그레이션 모드로 들어가서 수명을 43,200초(12시간)로 설정합니다.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

관련 명령

명령	설명
encryption	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 암호화 알고리즘을 지정합니다.
group	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 Diffie-Hellman 그룹을 지정합니다.
integrity	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 ESP 무결성 알고리즘을 지정합니다.
prf	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 PRF(의사 난수 함수)를 지정합니다.

limit-resource

다중 컨텍스트 모드에서 클래스에 대한 리소스 제한을 지정하려면 클래스 컨피그레이션 모드에서 **limit-resource** 명령을 사용합니다. 제한을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다. ASA에서는 컨텍스트를 리소스 클래스에 지정하는 방법으로 리소스를 관리합니다. 각 컨텍스트는 해당 클래스에서 설정한 리소스 제한을 적용합니다.

limit-resource [**rate**] {**all** | *resource_name*} *number*[**%**]}

no limit-resource {**all** | [**rate**] *resource_name*}

구문 설명

all	모든 리소스에 대한 제한을 설정합니다.
number[**%**]	1보다 크거나 같은 고정 숫자로 또는 1~100 범위에서 시스템 제한의 비율로서(백분율 기호 % 사용) 리소스 제한을 지정합니다. 제한을 **0**으로 설정하는 것은 리소스 무제한을 나타냅니다. VPN 리소스 유형의 경우 제한을 none으로 설정하면 됩니다. 시스템 제한이 없는 리소스는 백분율(%)을 설정할 수 없습니다. 절대값만 설정 가능합니다.
rate	리소스에 대해 초당 비율을 설정하도록 지정합니다. 초당 비율을 설정할 수 있는 리소스는 표 7-1을 참조하십시오.
resource_name	제한을 설정할 리소스 이름을 지정합니다. 이 제한은 **all**에 대해 설정된 제한을 재지정합니다.

기본값

모든 컨텍스트는 별도의 클래스에 지정되지 않는 한 기본 클래스에 속해 있습니다. 직접 기본 클래스에 컨텍스트를 지정할 필요는 없습니다.

대부분의 리소스에서 기본 클래스는 다음 제한을 제외하고 모든 컨텍스트에 무제한적인 리소스 액세스를 제공합니다.

- 텔넷 세션 - 5개 세션(컨텍스트당 최대 제한)
- SSH 세션 - 5개 세션(컨텍스트당 최대 제한)
- IPsec 세션 - 5개 세션(컨텍스트당 최대 제한)
- MAC 주소 - 65,535개 엔트리(컨텍스트당 최대 제한)
- VPN 사이트 대 사이트 터널 - 0개 세션(VPN 세션을 허용하려면 직접 클래스를 구성해야 함)

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
9.0(1)	각 컨텍스트에서 라우팅 테이블 엔트리의 최대값을 설정하기 위해 새로운 리소스 유형인 routes를 개발했습니다. 각 컨텍스트에서 사이트 대 사이트 VPN 터널의 최대값을 설정할 수 있도록 새로운 리소스 유형인 vpn other와 vpn burst other가 추가되었습니다.

사용 지침

기본적으로 모든 보안 컨텍스트는 컨텍스트별 최대 제한이 적용되는 경우는 제외하고 ASA의 리소스에 무제한으로 액세스할 수 있습니다. 유일한 예외가 VPN 리소스인데, 이는 기본적으로 비활성화되어 있습니다. 하나 이상의 컨텍스트에서 너무 많은 리소스를 사용하고 있으며 그로 인해 다른 컨텍스트의 연결이 거부되는 것과 같은 상황이 벌어진다면, 컨텍스트별 리소스 사용을 제한하는 리소스 관리를 구성할 수 있습니다. VPN 리소스의 경우 임의의 VPN 터널을 허용하도록 리소스 관리를 구성해야 합니다.

표 7-1에서는 리소스 유형과 그 제한을 보여줍니다. **show resource types** 명령도 참조하십시오.

표 7-1 리소스 이름 및 제한

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한[1]	설명
asdm	동시	최소 1 최대 5	32	ASDM 관리 세션 **참고** ASDM 세션은 2개의 HTTPS 연결을 사용합니다. 하나는 모니터링용으로 항상 실행되며, 다른 하나는 컨피그레이션 변경용으로 변경할 때만 실행됩니다. 예를 들어, 시스템 제한이 32개 ASDM 세션이라면 64개 HTTPS 세션을 의미합니다.
conns	동시 또는 비율	N/A	동시 연결: 플랫폼의 연결 제한은 CLI 컨피그레이션 가이드를 참조하십시오. 비율: N/A	임의의 두 호스트 간의 TCP 또는 UDP 연결. 단일 호스트와 여러 다른 호스트 간의 연결 포함
hosts	동시	N/A	N/A	ASA를 통해 연결될 수 있는 호스트
inspects	비율	N/A	N/A	애플리케이션 검사
mac-addresses	동시	N/A	65,535	투명 방화벽 모드의 경우 MAC 주소 테이블에서 허용되는 MAC 주소의 수
routes	동시	N/A	N/A	동적 경로
SSH	동시	최소 1 최대 5	100	SSH 세션
syslogs	비율	N/A	N/A	시스템 로그 메시지
telnet	동시	최소 1 최대 5	100	텔넷 세션

표 7-1 리소스 이름 및 제한(계속)

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한[1]	설명
vpn burst other	동시	N/A	해당 모델의 Other VPN 세션의 양에서 **vpn other**의 모든 컨텍스트에 할당된 세션의 합계를 뺀 것.	**vpn other**로 컨텍스트에 할당된 양을 초과하도록 허용된 사이트 대 사이트 VPN 세션 수. 예를 들어, 모델에서 세션 5000개를 지원하는데 **vpn other**로 컨텍스트 전체에 세션 4000개를 할당한 경우, 나머지 1000개 세션은 **vpn burst other**에서 사용 가능합니다. 컨텍스트에 대한 세션을 보장하는 **vpn other**와 달리, **vpn burst other**는 오버서브스크립션이 가능합니다. 버스트 풀은 모든 컨텍스트에서 선착순으로 사용할 수 있습니다.
vpn other	동시	N/A	모델에서 사용할 수 있는 Other VPN 세션은 CLI 컨피그레이션 가이드의 "모델당 지원되는 기능 라이센스" 섹션을 참조하십시오.	사이트 대 사이트 VPN 세션. 이 리소스는 오버서브스크립션할 수 없습니다. 모든 컨텍스트의 할당량 합계가 모델의 제한을 초과할 수 없습니다. 이 리소스에 대해 할당하는 세션은 해당 컨텍스트에 보장됩니다.
xlates	동시	N/A	N/A	주소 변환

1. 이 열의 값이 N/A 이면 해당 리소스에 대한 명시적 시스템 제한이 없으므로 리소스의 비율을 설정할 수 없습니다 .

예

다음 예는 conns에 대한 기본 클래스 제한을 무제한 대신 10퍼센트로 설정합니다.

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

다른 모든 리소스는 무제한으로 유지됩니다.

gold라는 클래스를 추가하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
```

관련 명령

명령	설명
class	리소스 클래스를 만듭니다.
context	보안 컨텍스트를 구성합니다.
member	리소스 클래스에 컨텍스트를 할당합니다.
show resource allocation	클래스 간에 리소스를 할당한 방법을 보여줍니다.
show resource types	제한을 설정할 수 있는 리소스 유형을 보여줍니다.

lmfactor

last-modified 타임스탬프만 있고 서버에 설정된 다른 만료 값은 없는 객체를 캐싱하기 위한 재검증 정책을 설정하려면 캐시 컨피그레이션 모드에서 **lmfactor** 명령을 사용합니다. 그러한 객체를 재검증하기 위한 새 정책을 설정하려면 명령을 다시 사용합니다. 특성을 기본값 20으로 재설정하려면 이 명령의 **no** 버전을 입력합니다.

lmfactor *value*

no lmfactor

구문 설명

value	0~100 범위의 정수

기본값

기본값은 20입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
캐시 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

ASA는 캐시된 객체가 변경되지 않은 상태를 유지해야 하는 시간을 예측하는 데 lmfactor의 값을 사용합니다. 이 시간을 만료 시간이라고 합니다. ASA는 마지막 수정 이후 경과된 시간과 lmfactor를 곱하여 만료 시간을 예측합니다.

lmfactor를 0으로 설정하는 것은 즉각적인 재지정을 적용하는 것과 동일합니다. 반면 100으로 설정하면 재검증 이후 허용 시간이 가장 길어집니다.

예

다음 예는 lmfactor를 30으로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(config-webvpn-cache)#
```

관련 명령

명령	설명
cache	WebVPN 캐시 모드로 들어갑니다.
cache-compressed	WebVPN 캐시 압축을 구성합니다.
disable	캐싱을 비활성화합니다.
expiry-time	캐싱 객체의 만료 시간을 구성합니다(재검증 없음).
max-object-size	캐시할 객체의 최대 크기를 정의합니다.
min-object-size	캐시할 객체의 최소 크기를 정의합니다.

local-unit

이 클러스터 멤버에 이름을 제공하려면 클러스터 그룹 컨피그레이션 모드에서 **local-unit** 명령을 사용합니다. 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다.

local-unit *unit_name*

no local-unit [*unit_name*]

구문 설명

unit_name	이 클러스터 멤버의 이름을 1~38자의 고유한 ASCII 문자열로 지정합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

각 유닛에는 고유한 이름이 있어야 합니다. 이름이 중복된 유닛은 클러스터에서 사용할 수 없습니다.

예

다음 예는 이 유닛의 이름을 unit1로 지정합니다.

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용할 경우 ASA에서는 cLACP를 사용하여 EtherChannel과 인접 스위치의 협상을 수행합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드로 들어갑니다.
cluster-interface	클러스터 제어 링크 인터페이스를 지정합니다.
cluster interface-mode	클러스터 인터페이스 모드를 설정합니다.
conn-rebalance	연결 리밸런싱을 활성화합니다.
console-replicate	슬레이브 유닛에서 마스터 유닛으로의 콘솔 복제를 활성화합니다.
enable (cluster group)	클러스터링을 활성화합니다.
health-check	유닛 검사 모니터링 및 인터페이스 상태 모니터링이 포함된 클러스터 상태 검사 기능을 활성화합니다.
key	클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 설정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스의 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택을 위해 이 유닛의 우선순위를 설정합니다.

log

Modular Policy Framework를 사용하는 경우, 일치 또는 클래스 컨피그레이션 모드에서 **log** 명령을 사용하여 **match** 명령 또는 클래스 맵과 일치하는 패킷을 기록합니다. 이 로그 작업은 검사 정책 맵에서 애플리케이션 트래픽에 대해 사용 가능합니다(**policy-map type inspect** 명령). 이 작업을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

log

no log

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
일치 및 클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

검사 정책 맵은 **match** 및 **class** 명령으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 명령은 애플리케이션에 따라 다릅니다. **match** 또는 **class** 명령을 입력하여 애플리케이션 트래픽을 식별한 후(**class** 명령은 기존의 **class-map type inspect** 명령을 참조하며, 여기에 **match** 명령이 포함됨), **log** 명령을 입력하여 **match** 명령 또는 **class** 명령과 일치하는 모든 패킷을 기록할 수 있습니다.

Layer 3/4 정책 맵에서(**policy-map** 명령) **inspect** 명령을 사용하여 애플리케이션 검사를 활성화할 경우 이 작업을 포함하는 검사 정책 맵을 활성화할 수 있습니다. 예를 들어 **inspect http http_policy_map** 명령(http_policy_map은 검사 정책 맵의 이름)을 입력할 수 있습니다.

예

다음 예는 패킷이 http-traffic 클래스 맵과 일치할 경우 로그를 전송합니다.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# log
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
policy-map type inspect	애플리케이션 검사를 위한 특수 작업을 정의합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

log-adj-changes(OSPFv2)

OSPF 인접 디바이스가 가동되거나 다운될 때 syslog 메시지를 전송하도록 라우터를 구성하려면 라우터 컨피그레이션 모드에서 **log-adj-changes** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

구문 설명

detail	(선택 사항) 상태 변화가 발생할 때마다 또는 인접 디바이스가 가동되거나 다운될 때에만 syslog 메시지를 전송합니다.

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.01)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

log-adj-changes 명령은 기본적으로 활성화되며, 명령의 **no** 형식으로 제거되지 않는 한 실행 중인 컨피그레이션에 나타납니다.

예

다음 예는 OSPF 인접 디바이스가 가동되거나 다운될 때 syslog 메시지의 전송을 비활성화합니다.

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)# no log-adj-changes
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드로 들어갑니다.
show ospf	OSPF 라우팅 프로세스에 대한 일반 정보가 표시됩니다.

log-adjacency-changes(OSPFv3)

OSPFv3 인접 디바이스가 가동 또는 다운될 때 syslog 메시지를 전송하도록 라우터를 구성하려면 IPv6 라우터 컨피그레이션 모드에서 **log-adjacency-changes** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

log-adjacency-changes [**detail**]

no log-adjacency-changes [**detail**]

구문 설명

detail	(선택 사항) 상태 변화가 발생할 때마다 또는 인접 디바이스가 가동되거나 다운될 때에만 syslog 메시지를 전송합니다.

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
IPv6 라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.01)	이 명령이 추가되었습니다.

사용 지침

log-adjacency-changes 명령은 기본적으로 사용되며, 명령의 **no** 형식으로 제거되지 않는 한 실행 중인 컨피그레이션에 나타납니다.

예

다음 예는 OSPFv3 인접 디바이스가 가동되거나 다운될 때 syslog 메시지의 전송을 비활성화합니다.

```
ciscoasa(config)# ipv6 router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

관련 명령

명령	설명
ipv6 router ospf	라우터 컨피그레이션 모드로 들어갑니다.
show ipv6 ospf	OSPFv3 라우팅 프로세스에 대한 일반 정보가 표시됩니다.

8 장

logging asdm through logout message 명령

logging asdm

Syslog 메시지를 ASDM 로그 버퍼로 전송하려면 글로벌 컨피그레이션 모드에서 **logging asdm** 명령을 사용합니다. ASDM 로그 버퍼에 대한 로깅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

구문 설명

level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
logging_list	ASDM 로그 버퍼로 전송할 메시지를 식별하는 목록을 지정합니다. 목록 생성에 대한 정보는 **logging list** 명령을 참조하십시오.

기본값

ASDM 로깅은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

메시지를 ASDM 로그 버퍼로 전송하기 전에 **logging enable** 명령을 사용하여 로깅을 활성화해야 합니다.

ASDM 로그 버퍼가 가득 차면 ASA는 새로운 메시지를 위한 버퍼 공간을 확보하기 위해 가장 오래된 메시지부터 삭제합니다. ASDM 로그 버퍼에 보존할 syslog 메시지 수를 제어하려면 **logging asdm-buffer-size** 명령을 사용합니다.

ASDM 로그 버퍼는 **logging buffered** 명령으로 활성화한 로그 버퍼와 다릅니다.

예

다음 예는 로깅을 활성화하고, 심각도 수준 0, 1 및 2의 로그 버퍼 메시지를 ASDM에 전송하고, ASDM 로그 버퍼 크기를 메시지 200개로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

관련 명령

명령	설명
clear logging asdm	포함하고 있는 모든 메시지의 ASDM 로그 버퍼를 지웁니다.
logging asdm-buffer-size	ASDM 로그 버퍼에 보존할 ASDM 메시지의 수를 지정합니다.
logging enable	로깅을 활성화합니다.
logging list	메시지 선택 기준의 재사용 가능한 목록을 생성합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	로깅 컨피그레이션을 표시합니다.

logging asdm-buffer-size

ASDM 로그 버퍼에 보존할 syslog 메시지 수를 지정하려면 글로벌 컨피그레이션 모드에서 **logging asdm-buffer-size** 명령을 사용합니다. ASDM 로그 버퍼를 기본 크기인 메시지 100개로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

구문 설명

num_of_msgs	ASA가 ASDM 로그 버퍼에 보존할 syslog 메시지 수를 지정합니다.

기본값

기본 ASDM syslog 버퍼 크기는 메시지 100개입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ASDM 로그 버퍼가 가득 차면 ASA는 새로운 메시지를 위한 버퍼 공간을 확보하기 위해 가장 오래된 메시지부터 삭제합니다. ASDM 로그 버퍼에 대한 로깅의 활성화 여부를 제어하거나 ASDM 로그 버퍼에 보존할 syslog 메시지의 종류를 제어하려면 **logging asdm** 명령을 사용합니다.

ASDM 로그 버퍼는 **logging buffered** 명령으로 활성화한 로그 버퍼와 다릅니다.

예

다음 예는 ASDM 로그 버퍼에 심각도 수준 0, 1, 2의 메시지를 로깅하는 방법 및 ASDM 로그 버퍼 크기를 메시지 200개로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

관련 명령

명령	설명
clear logging asdm	포함하고 있는 모든 메시지의 ASDM 로그 버퍼를 지웁니다.
logging asdm	ASDM 로그 버퍼에 대한 로깅을 활성화합니다.
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	현재 실행 중인 로깅 컨피그레이션을 표시합니다.

logging buffered

ASA가 로그 버퍼로 syslog 메시지를 전송하도록 하려면 글로벌 컨피그레이션 모드에서 **logging buffered** 명령을 사용합니다. 로그 버퍼에 대한 로깅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

구문 설명

level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
logging_list	로그 버퍼로 전송할 메시지를 식별하는 목록을 지정합니다. 목록 생성에 대한 정보는 **logging list** 명령을 참조하십시오.

기본값

기본값은 다음과 같습니다.

- 버퍼에 대한 로깅은 비활성화되어 있습니다.
- 버퍼 크기는 4KB입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

메시지를 로그 버퍼로 전송하기 전에 **logging enable** 명령을 사용하여 로깅을 활성화해야 합니다.

새 메시지는 버퍼의 끝에 추가됩니다. 버퍼가 가득 차면 ASA는 버퍼를 지우고 메시지를 계속 추가합니다. 로그 버퍼가 가득 차면 ASA는 새로운 메시지를 위한 버퍼 공간을 확보하기 위해 가장 오래된 메시지를 삭제합니다. 버퍼 내용이 "래핑"될 때마다, 즉 마지막 저장 이후 모든 메시지가 새 메시지로 교체될 때마다 버퍼 내용을 자동으로 저장할 수 있습니다. 자세한 내용은 **logging flash-bufferwrap** 및 **logging ftp-bufferwrap** 명령을 참조하십시오.

언제든지 버퍼의 내용을 플래시 메모리에 저장할 수 있습니다. 자세한 내용은 **logging savelog** 명령을 참조하십시오.

show logging 명령으로 버퍼에 전송된 syslog 메시지를 볼 수 있습니다.

예

다음 예는 심각도 수준 0 및 수준 1 이벤트를 버퍼에 로깅하도록 구성합니다.

```
ciscoasa(config)# logging buffered alerts
ciscoasa(config)#
```

다음 예는 최대 심각도 수준 7의 "notif-list"라는 목록을 만들고, "notif-list" 목록으로 식별된 syslog 메시지를 버퍼에 로깅하도록 구성합니다.

```
ciscoasa(config)# logging list notif-list level 7
ciscoasa(config)# logging buffered notif-list
ciscoasa(config)#
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
logging buffer-size	로그 버퍼 크기를 지정합니다.
logging enable	로깅을 활성화합니다.
logging list	메시지 선택 기준의 재사용 가능한 목록을 생성합니다.
logging savelog	내부 로그 버퍼의 내용을 플래시 메모리에 저장합니다.

logging buffer-size

로그 버퍼의 크기를 지정하려면 글로벌 컨피그레이션 모드에서 **logging buffer-size** 명령을 사용합니다. 로그 버퍼를 기본 크기인 메모리 4KB로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logging buffer-size *bytes*

no logging buffer-size *bytes*

구문 설명

bytes	로그 버퍼에 사용할 메모리의 양을 바이트 단위로 설정합니다. 예를 들어 8192를 지정하면 ASA는 로그 버퍼에 메모리 8KB를 사용합니다.

기본값

기본 버퍼 크기는 메모리 4KB입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA에서 기본 버퍼 크기 이외의 로그 버퍼 크기를 사용 중인지 알아보려면 **show running-config logging** 명령을 사용합니다. **logging buffer-size** 명령이 표시되지 않으면 ASA에서 4KB의 로그 버퍼를 사용하는 것입니다.

ASA의 버퍼 사용법에 대해 자세히 알아보려면 **logging buffered** 명령을 참조하십시오.

예

다음 예는 로깅을 활성화하고, 로깅 버퍼를 활성화하고, ASA에서 로그 버퍼에 16KB 메모리를 사용하도록 지정합니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging buffer-size 16384
ciscoasa(config)#
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
logging buffered	로그 버퍼에 대한 로깅을 활성화합니다.
logging enable	로깅을 활성화합니다.
logging flash-bufferwrap	로그 버퍼가 꽉 차면 로그 버퍼를 플래시 메모리에 기록합니다.
logging savelog	내부 로그 버퍼의 내용을 플래시 메모리에 저장합니다.

logging class

메시지 클래스의 로깅 대상에 대한 최대 심각도 수준을 구성하려면 글로벌 컨피그레이션 모드에서 **logging class** 명령을 사용합니다. 메시지 클래스 심각도 수준 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging class *class destination level* [*destination level . . .*]

no logging class *class*

구문 설명

class	최대 심각도 수준이 대상별로 구성되는 메시지 클래스를 지정합니다. *class*의 유효한 값은 "사용 지침" 섹션을 참조하십시오.
destination	*class*의 로깅 대상을 지정합니다. 대상의 경우, *destination*으로 전송되는 최대 심각도 수준을 *level*이 결정합니다. *destination*의 유효한 값은 다음의 "사용 지침" 섹션을 참조하십시오.
level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지

기본값

기본적으로 ASA는 로깅 대상 및 메시지 클래스 기반에 심각도 수준을 적용하지 않습니다. 실제로, 활성화된 각 로깅 대상은 로깅 목록에 의해 확인된 심각도 수준 또는 로깅 대상을 활성화할 때 지정한 심각도 수준에서 모든 클래스의 메시지를 수신합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.0(2)	유효한 클래스 값에 **eigrp**가 추가되었습니다.
8.2(1)	유효한 클래스 값에 **dap**가 추가되었습니다.

사용 지침

*class*의 유효한 값은 다음과 같습니다.

- **auth** - 사용자 인증.
- **bridge** - 투명 방화벽.
- **ca** - PKI 인증 기관.
- **config** - 명령 인터페이스.
- **dap -** 동적 액세스 정책.
- **eap** - EAP(Extensible Authentication Protocol). EAP 세션 상태 변경, EAP 세션 쿼리 이벤트, EAP 헤더 및 패킷 내용의 16진수 덤프 등, Network Admission Control을 지원하는 이벤트 유형을 기록합니다.
- **eapoudp** - EAP(Extensible Authentication Protocol) over UDP. Network Admission Control을 지원하는 EAPoUDP 이벤트를 기록하고, EAPoUDP 헤더 및 패킷 내용의 완전한 레코드를 생성합니다.
- **eigrp** - EIGRP 라우팅.
- **email** - 이메일 프록시.
- **ha** - 장애 조치.
- **ids** - 침입 감지 시스템.
- **ip** - IP 스택.
- **ipaa -** IP 주소 할당.
- **nac** - Network Admission Control. 초기화, 예외 목록 일치, ACS 트랜잭션, 클라이언트리스 인증, 기본 ACL 애플리케이션, 재검증 등의 이벤트 유형을 기록합니다.
- **np** - 네트워크 프로세서.
- **ospf** - OSPF 라우팅.
- **rip** - RIP 라우팅.
- **rm** - Resource Manager.
- **session** - 사용자 세션.
- **snmp** - SNMP.
- **sys** - System.
- **vpn** - IKE 및 IPsec.
- **vpnc** - VPN 클라이언트.
- **vpnfo** - VPN 장애 조치.
- **vpnlb** - VPN 로드 밸런싱.

유효한 로깅 대상은 다음과 같습니다.

- **asdm** - 자세한 내용은 **logging asdm** 명령을 참조하십시오.
- **buffered** - 자세한 내용은 **logging buffered** 명령을 참조하십시오.
- **console** - 자세한 내용은 **logging console** 명령을 참조하십시오.
- **history** - 자세한 내용은 **logging history** 명령을 참조하십시오.
- **mail** - 자세한 내용은 **logging mail** 명령을 참조하십시오.
- **monitor** - 자세한 내용은 **logging monitor** 명령을 참조하십시오.
- **trap** - 자세한 내용은 **logging trap** 명령을 참조하십시오.

예

다음 예는, 장애 조치 관련 메시지에서 ASDM 로그 버퍼의 최대 심각도 수준은 2, syslog 버퍼의 최대 심각도 수준은 7로 지정합니다.

```
ciscoasa(config)# logging class ha asdm 2 buffered 7
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging console

ASA가 콘솔 세션에 syslog 메시지가 표시되도록 하려면 글로벌 컨피그레이션 모드에서 **logging console** 명령을 사용합니다. 콘솔 세션에 syslog 메시지가 표시되지 않도록 하려면 이 명령의 **no** 형식을 사용합니다.

logging console [*logging_list* | *level*]

no logging console

참고 버퍼 오버플로 때문에 많은 syslog 메시지가 삭제될 수 있으므로 이 명령을 사용하지 않는 것이 좋습니다. 자세한 내용은 "사용 지침" 섹션을 참조하십시오.

구문 설명

level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
logging_list	콘솔 세션으로 전송할 메시지를 식별하는 목록을 지정합니다. 목록 생성에 대한 정보는 **logging list** 명령을 참조하십시오.

기본값

기본적으로 ASA는 콘솔 세션에 syslog 메시지를 표시하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

메시지를 콘솔로 전송하기 전에 **logging enable** 명령을 사용하여 로깅을 활성화해야 합니다.

주의 **logging console** 명령을 사용하면 시스템 성능이 심각하게 저하될 수 있습니다. 대신, 로깅을 시작하려면 **logging buffered** 명령을 사용하고 메시지를 보려면 **show logging** 명령을 사용합니다. 최신 메시지를 좀 더 쉽게 보려면 **clear logging buffer** 명령을 사용하여 버퍼를 지웁니다.

예

다음 예는 심각도 수준 0, 1, 2, 3의 syslog 메시지를 콘솔 세션에 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging console errors
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging list	메시지 선택 기준의 재사용 가능한 목록을 생성합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging debug-trace

디버깅 메시지를 심각도 수준 7의 syslog 메시지 711001로서 로그로 리디렉션하려면 글로벌 컨피그레이션 모드에서 **logging debug-trace** 명령을 사용합니다. 디버깅 메시지의 전송을 중지하려면 이 명령의 **no** 형식을 사용합니다.

logging debug-trace

no logging debug-trace

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 ASA는 syslog 메시지에 디버깅 출력을 포함하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

디버깅 메시지는 심각도 수준 7 메시지로서 생성됩니다. 디버깅 메시지는 로그에서 syslog 메시지 번호 711001로 나타나지만, 모니터링 세션에는 나타나지 않습니다.

예

다음 예는 로깅을 활성화하고, 로그 메시지를 시스템 로그 버퍼로 전송하고, 디버깅 출력을 로그로 리디렉션하고, 디스크 활동의 디버깅을 켜는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace
ciscoasa(config)# debug disk filesystem
```

다음은 로그에 나타날 수 있는 디버깅 메시지의 샘플 출력입니다.

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging device-id

비 EMBLEM 형식 syslog 메시지에 디바이스 ID를 포함하도록 ASA를 구성하려면 글로벌 컨피그레이션 모드에서 **logging device-id** 명령을 사용합니다. 디바이스 ID의 사용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

no logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

구문 설명

cluster-id	클러스터에 있는 개별 ASA 유닛의 고유한 이름을 디바이스 ID로 지정합니다.
hostname	ASA의 호스트 이름을 디바이스 ID로 지정합니다.
ipaddress *interface_name*	디바이스 ID 또는 인터페이스의 IP 주소를 *interface_name* 형식으로 지정합니다. **ipaddress** 키워드를 사용하면, 로그 데이터를 외부 서버로 전송하기 위해 ASA에서 어떤 인터페이스를 사용하는지와 상관없이 외부 서버로 전송된 syslog 메시지는 지정된 인터페이스의 IP 주소를 포함하게 됩니다.
string *text*	*text*의 문자를 디바이스 ID로서 지정합니다. 문자의 최대 길이는 16자이며, 공백 또는 다음 문자를 사용할 수 없습니다. • & - 앰퍼샌드 • ' - 작은따옴표 • " - 큰따옴표 • < - 보다 작음 • > - 보다 큼 • ? - 물음표
system	(선택 사항) 클러스터 환경에서, 디바이스 ID가 인터페이스의 시스템 IP 주소가 되도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	**cluster-id** 및 **system** 키워드가 추가되었습니다.

사용 지침

ipaddress 키워드를 사용하는 경우 메시지가 전송되는 인터페이스에 관계없이, 디바이스 ID가 지정된 ASA 인터페이스 IP 주소가 됩니다. 이 키워드는 디바이스에서 전송되는 모든 메시지에 대해 하나의 일관된 디바이스 ID를 제공합니다. **system** 키워드를 사용하는 경우, 지정된 ASA는 클러스터에 있는 유닛의 로컬 IP 주소 대신 시스템 IP 주소를 사용합니다. **cluster-id** 및 **system** 키워드는 ASA 5580 및 5585-X에만 적용됩니다.

예

다음 예는 "secappl-1"이라는 호스트를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

다음 메시지와 같이, 호스트 이름은 syslog 메시지의 시작 부분에 나타납니다.

```
secappl-1 %ASA-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging emblem

Syslog 서버 이외의 대상으로 syslog 메시지를 전송하는 데 EMBLEM 형식을 사용하려면 글로벌 컨피그레이션 모드에서 **logging emblem** 명령을 사용합니다. EMBLEM 형식의 사용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging emblem

no logging emblem

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 ASA는 syslog 메시지에 EMBLEM 형식을 사용하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령은 **logging host** 명령에 의존하지 않도록 변경되었습니다.

사용 지침

logging emblem 명령을 사용하면 syslog 서버 이외의 모든 로깅 대상에 대해 EMBLEM 형식의 로깅을 사용할 수 있습니다. **logging timestamp** 키워드도 함께 활성화하면 타임스탬프가 있는 메시지가 전송됩니다.

Syslog 서버에 대해 EMBLEM 형식의 로깅을 활성화하려면 **format emblem** 옵션과 함께 **logging host** 명령을 사용합니다.

예

다음 예는 로깅을 활성화하는 방법 및 syslog 서버를 제외한 모든 로깅 대상에 EMBLEM 형식을 사용하여 로깅하도록 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging emblem
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging enable

구성된 모든 출력 위치에 대해 로깅을 활성화하려면 글로벌 컨피그레이션 모드에서 **logging enable** 명령을 사용합니다. 로깅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging enable

no logging enable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

로깅은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령은 **logging on** 명령에서 변경되었습니다.

사용 지침

logging enable 명령을 사용하면 지원되는 로깅 대상으로 syslog 메시지를 전송하는 기능을 활성화 또는 비활성화할 수 있습니다. 모든 로깅을 중지하려면 **no logging enable** 명령을 사용할 수 있습니다.

다음 명령을 사용하면 개별 로깅 대상에 대한 로깅을 활성화할 수 있습니다.

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

예

다음 예는 로깅을 활성화하는 방법을 보여줍니다. **show logging** 명령의 출력은 각각의 가능한 로깅 대상을 개별적으로 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

관련 명령

명령	설명
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging facility

Syslog 서버로 전송되는 메시지에 사용할 로깅 facility를 지정하려면 글로벌 컨피그레이션 모드에서 **logging facility** 명령을 사용합니다. 로깅 facility를 기본값 20으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logging facility *facility*

no logging facility

구문 설명

facility	로깅 facility를 지정합니다. 유효한 값은 16~23입니다.

기본값

기본 facility는 20(LOCAL4)입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다(예외는 구문 설명 섹션에서 설명).

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Syslog 서버는 메시지에 있는 *facility* 번호를 기반으로 메시지를 보관합니다. 16(LOCAL0)에서 23(LOCAL7)까지 8개의 가능한 facility가 있습니다.

예

다음 예는 ASA가 syslog 메시지에서 로깅 facility를 16으로 표시하도록 지정하는 방법을 보여줍니다. **show logging** 명령의 출력에는 ASA에서 사용하는 facility가 포함됩니다.

```
ciscoasa(config)# logging facility 16
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging host	Syslog 서버를 정의합니다.
logging trap	Syslog 서버에 대한 로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging flash-bufferwrap

저장되지 않은 메시지로 버퍼가 가득 찰 때마다 ASA에서 로그 버퍼를 플래시 메모리에 기록하도록 하려면 글로벌 컨피그레이션 모드에서 **logging flash-bufferwrap** 명령을 사용합니다. 로그 버퍼를 플래시 메모리에 기록하는 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging flash-bufferwrap

no logging flash-bufferwrap

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본값은 다음과 같습니다.

- 버퍼에 대한 로깅은 비활성화되어 있습니다.
- 로그 버퍼를 플래시 메모리에 기록하는 기능은 비활성화되어 있습니다.
- 버퍼 크기는 4KB입니다.
- 최소 여유 플래시 메모리는 3MB입니다.
- 버퍼 로깅을 위한 최대 플래시 메모리 할당은 1MB입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA가 로그 버퍼를 플래시 메모리에 기록하도록 하려면 먼저 버퍼에 대한 로깅을 활성화해야 합니다. 그렇게 하지 않으면 로그 버퍼가 데이터를 플래시 메모리에 기록할 수 없습니다. 버퍼에 대한 로깅을 활성화하려면 **logging buffered** 명령을 사용합니다.

ASA는 로그 버퍼 내용을 플래시 메모리에 기록하는 한편, 새 이벤트 메시지를 계속해서 로그 버퍼에 저장합니다.

ASA는 다음과 같이 기본 타임스탬프 형식을 사용하는 이름으로 로그 파일을 생성합니다.

LOG-*YYYY-MM-DD-HHMMSS*.TXT

*YYYY*는 연도이고 *MM*는 달이며 *DD*는 날짜입니다. *HHMMSS*는 시간, 분, 초를 나타냅니다.

플래시 메모리의 가용성은 ASA가 **logging flash-bufferwrap** 명령을 사용하여 syslog 메시지를 저장하는 방법에 영향을 미칩니다. 자세한 내용은 **logging flash-maximum-allocation** 및 **logging flash-minimum-free** 명령을 참조하십시오.

예

다음 예는 로깅을 활성화하고, 로그 버퍼를 활성화하고, ASA가 로그 버퍼를 플래시 메모리에 기록하도록 하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)#
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
copy	파일을 한 위치에서 TFTP 또는 FTP 서버를 비롯한 다른 위치로 복사합니다.
delete	저장된 로그 파일 등의 디스크 파티션에서 파일을 삭제합니다.
logging buffered	로그 버퍼에 대한 로깅을 활성화합니다.
logging buffer-size	로그 버퍼 크기를 지정합니다.

logging flash-maximum-allocation

ASA가 로그 데이터 저장에 사용하는 최대 플래시 메모리의 양을 지정하려면 글로벌 컨피그레이션 모드에서 **logging flash-maximum-allocation** 명령을 사용합니다. 이 목적에 사용되는 최대 플래시 메모리의 양을 기본값인 1MB로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

구문 설명

kbytes	ASA가 로그 버퍼 데이터 저장에 사용할 수 있는 최대 플래시 메모리의 양(킬로바이트 단위)

기본값

로그 데이터를 위한 기본 최대 플래시 메모리 할당은 1MB입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 **logging savelog** 및 **logging flash-bufferwrap** 명령에 사용 가능한 플래시 메모리의 양을 결정합니다.

logging savelog 또는 **logging flash-bufferwrap**에 의해 저장되는 로그 파일 때문에 로그 파일에 대한 플래시 메모리 사용이 **logging flash-maximum-allocation** 명령으로 지정한 최대값을 초과하면 ASA에서는 새 로그 파일을 위한 충분한 여유 메모리를 확보하기 위해 가장 오래된 로그 파일부터 삭제합니다. 삭제할 파일이 없거나, 오래된 파일을 모두 삭제한 후에도 새 로그 파일에 사용할 여유 메모리가 너무 부족하면 ASA는 새 로그 파일을 저장하지 못합니다.

ASA의 최대 플래시 메모리 할당 크기가 기본 크기와 다른지 알아보려면 **show running-config logging** 명령을 사용합니다. **logging flash-maximum-allocation** 명령이 표시되지 않으면 ASA는 저장된 로그 버퍼 데이터에 최대 1MB를 사용합니다. 할당된 메모리는 **logging savelog** 및 **logging flash-bufferwrap** 명령에 모두 사용됩니다.

ASA의 로그 버퍼 사용법에 대해 자세히 알아보려면 **logging buffered** 명령을 참조하십시오.

예

다음 예는 로깅을 활성화하고, 로그 버퍼를 활성화하고, ASA가 로그 버퍼를 플래시 메모리에 기록하도록 지정하며, 로그 파일 기록에 사용할 최대 플래시 메모리의 양을 약 1.2MB로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-maximum-allocation 1200
ciscoasa(config)#
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
logging buffered	로그 버퍼에 대한 로깅을 활성화합니다.
logging enable	로깅을 활성화합니다.
logging flash-bufferwrap	로그 버퍼가 꽉 차면 로그 버퍼를 플래시 메모리에 기록합니다.
logging flash-minimum-free	ASA가 로그 버퍼를 플래시 메모리에 기록하도록 허용하기 위해 필요한 최소 플래시 메모리의 양을 지정합니다.

logging flash-minimum-free

ASA에서 새 로그 파일을 저장하기 전에 반드시 필요한 최소 여유 플래시 메모리의 양을 지정하려면 글로벌 컨피그레이션 모드에서 **logging flash-minimum-free** 명령을 사용합니다. 필요한 최소 여유 플래시 메모리의 양을 기본값인 3MB로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

구문 설명

kbytes	ASA에서 새 로그 파일을 저장하기 전에 반드시 필요한 최소 여유 플래시 메모리의 양(킬로바이트 단위)

기본값

최소 기본 여유 플래시 메모리는 3MB입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logging flash-minimum-free 명령은 **logging savelog** 및 **logging flash-bufferwrap** 명령이 항상 유지해야 하는 플래시 메모리의 양을 지정합니다.

logging savelog 또는 **logging flash-bufferwrap**에 의해 저장되는 로그 파일 때문에 여유 플래시 메모리의 양이 **logging flash-minimum-free** 명령으로 지정한 하한값보다 낮으면 ASA에서는 새 로그 파일을 저장한 이후에도 최소 메모리의 양이 유지되도록 가장 오래된 로그 파일부터 삭제합니다. 삭제할 파일이 없거나 모든 오래된 파일을 삭제한 후에도 여유 메모리가 여전히 하한값보다 낮으면 ASA는 새 로그 파일을 저장하지 못합니다.

예

다음 예는 로깅을 활성화하고, 로그 버퍼를 활성화하고, ASA가 로그 버퍼를 플래시 메모리에 기록하도록 지정하며, 최소 여유 플래시 메모리의 양을 약 4000KB로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-minimum-free 4000
ciscoasa(config)#
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
logging buffered	로그 버퍼에 대한 로깅을 활성화합니다.
logging enable	로깅을 활성화합니다.
logging flash-bufferwrap	로그 버퍼가 꽉 차면 로그 버퍼를 플래시 메모리에 기록합니다.
logging flash-maximum-allocation	로그 버퍼 내용을 기록하는 데 사용할 수 있는 최대 플래시 메모리의 양을 지정합니다.

logging flow-export-syslogs enable | disable

NetFlow가 캡처하는 모든 syslog 메시지를 활성화하려면 글로벌 컨피그레이션 모드에서 **logging flow-export-syslogs enable** 명령을 사용합니다. NetFlow가 캡처하는 모든 syslog 메시지를 비활성화하려면 글로벌 컨피그레이션 모드에서 **logging flow-export-syslogs disable** 명령을 사용합니다.

logging flow-export-syslogs {enable | disable}

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 NetFlow에서 캡처되는 모든 syslog가 활성화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.1(1)	이 명령이 추가되었습니다.

사용 지침

성능 향상을 위해 NetFlow 데이터를 내보내도록 보안 어플라이언스를 구성한 경우 **logging flow-export-syslogs disable** 명령을 입력하여 중복 syslog 메시지를 비활성화할 것을 권장합니다. 비활성화할 syslog 메시지는 다음과 같습니다.

Syslog 메시지	설명
106015	첫 번째 패킷이 SYN 패킷이 아니기 때문에 TCP 흐름이 거부되었습니다.
106023	**access-group** 명령을 통해 인터페이스에 추가되는 인그레스 ACL 또는 이그레스 ACL에서 거부하는 흐름.
106100	ACL에서 허용 또는 거부하는 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	보안 어플라이언스에 대한 ICMP 패킷이 거부되었습니다.
313008	보안 어플라이언스에 대한 ICMPv6 패킷이 거부되었습니다.
710003	보안 어플라이언스에 대한 연결 시도가 거부되었습니다.

참고 이 명령은 컨피그레이션 모드 명령이기는 하지만 컨피그레이션에 저장되지는 않습니다. 컨피그레이션에는 **no logging message xxxxxx** 명령만 저장됩니다.

예

다음 예는 NetFlow에서 캡처하는 중복 syslog 메시지 및 나타나는 샘플 출력을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# logging flow-export-syslogs disable

ciscoasa(config)# show running-config logging

no logging message xxxxx1
no logging message xxxxx2
```

NetFlow를 통해 동일한 정보가 캡처되었으므로, 여기서 *xxxxx1* 및 *xxxxx2*는 중복되는 syslog 메시지입니다. 이 명령은 명령 별칭과도 같으며 일련의 **no logging message xxxxxx** 명령으로 전환됩니다. Syslog 메시지를 비활성화한 이후 **logging message xxxxxx** 명령을 사용해 개별적으로 활성화할 수 있습니다. 여기서 *xxxxxx*는 특정 syslog 메시지 번호입니다.

관련 명령

명령	설명
flow-export destination *interface-name ipv4-address* | *hostname udp-port*	NetFlow 컬렉터의 IP 주소 또는 호스트 이름, 그리고 NetFlow 컬렉터가 수신 대기하는 UDP 포트를 지정합니다.
flow-export template timeout-rate *minutes*	템플릿 정보가 NetFlow 컬렉터로 전송되는 간격을 제어합니다.
show flow-export counters	NetFlow에 대한 런타임 카운터를 표시합니다.

logging from-address

ASA에서 전송하는 syslog 메시지의 발신자 이메일 주소를 지정하려면 글로벌 컨피그레이션 모드에서 **logging from-address** 명령을 사용합니다. 전송된 모든 syslog 메시지는 사용자가 지정한 주소에서 오는 것으로 표시됩니다. 발신자 이메일 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging from-address *from-email-address*

no logging from-address *from-email-address*

구문 설명

from-email-address	Syslog 메시지가 오는 것으로 표시되는 이메일 주소인 소스 이메일 주소(예: cdb@example.com)

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이메일에 의한 syslog 메시지 전송은 **logging mail** 명령으로 활성화됩니다.

이 명령으로 지정한 주소는 기존 이메일 계정과 일치할 필요가 없습니다.

예

로깅을 활성화하고 ASA가 이메일 주소로 syslog 메시지를 전송하도록 지정하려면 다음 기준을 사용합니다.

- Critical, alerts 또는 emergencies의 메시지를 전송합니다.
- 발신자 주소로 ciscosecurityappliance@example.com을 사용하여 메시지를 전송합니다.
- admin@example.com으로 메시지를 전송합니다.
- SMTP, 기본 서버 pri-smtp-host 및 보조 서버 sec-smtp-host를 사용하여 메시지를 전송합니다.

다음 명령을 입력합니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging mail critical
ciscoasa(config)# logging from-address ciscosecurityappliance@example.com
ciscoasa(config)# logging recipient-address admin@example.com
ciscoasa(config)# smtp-server pri-smtp-host sec-smtp-host
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging mail	ASA에서 이메일로 syslog 메시지를 전송하도록 지정하고, 어떤 메시지를 이메일로 전송할지를 결정합니다.
logging recipient-address	Syslog 메시지의 수신 이메일 주소를 지정합니다.
smtp-server	SMTP 서버를 구성합니다.
show logging	활성화된 로깅 옵션을 표시합니다.

logging ftp-bufferwrap

저장되지 않은 메시지로 버퍼가 가득 찰 때마다 ASA에서 로그 버퍼를 FTP 서버로 전송하도록 하려면 글로벌 컨피그레이션 모드에서 **logging ftp-bufferwrap** 명령을 사용합니다. 로그 버퍼를 FTP 서버로 전송하는 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging ftp-bufferwrap

no logging ftp-bufferwrap

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본값은 다음과 같습니다.

- 버퍼에 대한 로깅은 비활성화되어 있습니다.
- 로그 버퍼를 FTP 서버로 전송하는 기능이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logging ftp-bufferwrap을 활성화하면 ASA는 사용자가 **logging ftp-server** 명령으로 지정한 FTP 서버로 로그 버퍼 데이터를 전송합니다. ASA는 로그 데이터를 FTP 서버로 전송하는 한편, 새 이벤트 메시지를 계속해서 로그 버퍼에 저장합니다.

ASA가 로그 버퍼 내용을 FTP 서버로 전송하도록 하려면 먼저 버퍼에 대한 로깅을 활성화해야 합니다. 그렇게 하지 않으면 로그 버퍼가 데이터를 플래시 메모리에 기록할 수 없습니다. 버퍼에 대한 로깅을 활성화하려면 **logging buffered** 명령을 사용합니다.

ASA는 다음과 같이 기본 타임스탬프 형식을 사용하는 이름으로 로그 파일을 생성합니다.

LOG-*YYYY-MM-DD-HHMMSS*.TXT

*YYYY*는 연도이고 *MM*는 달이며 *DD*는 날짜입니다. *HHMMSS*는 시간, 분, 초를 나타냅니다.

예

다음 예는 로깅을 활성화하고, 로그 버퍼를 활성화하고, FTP 서버를 지정하고, ASA가 로그 버퍼를 FTP 서버에 기록하도록 하는 방법을 보여줍니다. 여기에서는 호스트 이름이 logserver-352인 FTP 서버를 지정합니다. 이 서버에는 사용자 이름 logsupervisor 및 비밀번호 1luvMy10gs로 액세스할 수 있습니다. 로그 파일은 /syslogs 디렉터리에 저장됩니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
ciscoasa(config)# logging ftp-bufferwrap
ciscoasa(config)#
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
logging buffered	로그 버퍼에 대한 로깅을 활성화합니다.
logging buffer-size	로그 버퍼 크기를 지정합니다.
logging enable	로깅을 활성화합니다.
logging ftp-server	**logging ftp-bufferwrap** 명령과 함께 사용할 FTP 서버 매개변수를 지정합니다.

logging ftp-server

logging ftp-bufferwrap이 활성화된 경우 ASA에서 로그 버퍼 데이터를 전송할 FTP 서버의 세부 정보를 지정하려면 글로벌 컨피그레이션 모드에서 **logging ftp-server** 명령을 사용합니다. FTP 서버에 대한 모든 세부 정보를 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging ftp-server *ftp_server path username* [*0* | *8*] *password*

no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

구문 설명

0	(선택 사항) 암호화되지 않은(일반 텍스트) 사용자 비밀번호가 이어짐을 지정합니다.
8	(선택 사항) 암호화된 사용자 비밀번호가 이어짐을 지정합니다.
ftp-server	외부 FTP 서버 IP 주소 또는 호스트 이름. **참고** 호스트 이름을 지정하는 경우 네트워크에서 DNS가 올바르게 작동하는지 확인하십시오.
password	지정된 사용자 이름의 비밀번호(최대 64자).
path	로그 버퍼 데이터를 저장할 FTP 서버의 디렉토리 경로. 이 경로는 FTP 루트 디렉토리에 대한 상대적인 경로입니다. 예: `/security_appliances/syslogs/appliance107`
username	FTP 서버에 로그인할 수 있는 사용자 이름.

기본값

FTP 서버는 기본적으로 지정되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.3(1)	비밀번호 암호화에 대한 지원이 추가되었습니다.

사용 지침

하나의 FTP 서버만 지정할 수 있습니다. 로깅 FTP 서버가 이미 지정되어 있는 경우 **logging ftp-server** 명령을 사용하면 FTP 서버 컨피그레이션이 사용자가 입력한 새로운 것으로 교체됩니다.

ASA는 사용자가 지정한 FTP 서버 정보를 확인하지 않습니다. 세부 정보 중 일부를 잘못 구성하면 ASA는 로그 버퍼 데이터를 FTP 서버로 전송하지 못합니다.

ASA의 부팅 또는 업그레이드 중에는 한 자리 비밀번호 및 숫자로 시작하고 뒤에 공백이 오는 비밀번호는 지원되지 않습니다. 예를 들어 0 pass 및 1은 잘못된 비밀번호입니다.

예

다음 예는 로깅을 활성화하고, 로그 버퍼를 활성화하고, FTP 서버를 지정하고, ASA가 로그 버퍼를 FTP 서버에 기록하도록 하는 방법을 보여줍니다. 여기서는 호스트 이름이 logserver인 FTP 서버를 지정합니다. 이 서버에는 사용자 이름 user1 및 비밀번호 pass1로 액세스할 수 있습니다. 로그 파일은 /path1 디렉터리에 저장됩니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver /path1 user1 pass1
ciscoasa(config)# logging ftp-bufferwrap
```

다음 예는 암호화된 비밀번호를 입력하는 방법을 보여줍니다.

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

다음 예는 암호화되지 않은(일반 텍스트) 비밀번호를 입력하는 방법을 보여줍니다.

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 0 pass1
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
logging buffered	로그 버퍼에 대한 로깅을 활성화합니다.
logging buffer-size	로그 버퍼 크기를 지정합니다.
logging enable	로깅을 활성화합니다.
logging ftp-bufferwrap	로그 버퍼가 꽉 차면 로그 버퍼를 FTP 서버로 전송합니다.

logging history

SNMP 로깅을 활성화하고 어떤 메시지를 SNMP 서버로 전송할지를 지정하려면 글로벌 컨피그레이션 모드에서 **logging history** 명령을 사용합니다. SNMP 로깅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging history [*logging_list* | *level*]

no logging history

구문 설명

level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
logging_list	SNMP 서버로 전송할 메시지를 식별하는 목록을 지정합니다. 목록 생성에 대한 정보는 **logging list** 명령을 참조하십시오.

기본값

ASA는 기본적으로 SNMP 서버에 기록하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logging history 명령을 사용하면 SNMP 서버에 대한 로깅을 활성화하고 SNMP 메시지 수준 또는 이벤트 목록을 설정할 수 있습니다.

예

다음 예는 SNMP 로깅을 활성화하고 심각도 수준 0, 1, 2, 3의 메시지를 구성된 SNMP 서버로 전송하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
ciscoasa(config)# snmp-server enable traps syslog
ciscoasa(config)# logging history errors
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging list	메시지 선택 기준의 재사용 가능한 목록을 생성합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.
snmp-server	SNMP 서버 세부 정보를 지정합니다.

logging host

Syslog 서버를 정의하려면 글로벌 컨피그레이션 모드에서 **logging host** 명령을 사용합니다. Syslog 서버 정의를 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

no logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

구문 설명

format emblem	(선택 사항) Syslog 서버에 대해 EMBLEM 형식 로깅을 활성화합니다.
interface_name	Syslog 서버가 상주하는 인터페이스를 지정합니다.
port	Syslog 서버가 메시지를 수신 대기하는 포트를 지정합니다. 각 프로토콜에 대한 유효한 포트 값은 1025~65535입니다. 포트 번호로 영(0)을 입력하거나 잘못된 문자나 기호를 사용하면 오류가 발생합니다.
secure	(선택 사항) 원격 로깅 호스트로의 연결에 SSL/TLS를 사용하도록 지정합니다. 이 옵션은 선택된 프로토콜이 TCP인 경우에만 유효합니다. **참고** SSL/TLS 지원 syslog 서버에서만 안전한 로깅 연결을 설정할 수 있습니다. SSL/TLS 연결이 설정되지 않으면 새로운 모든 연결이 거부됩니다. 이러한 기본 동작은 **logging permit-hostdown** 명령으로 변경할 수 있습니다.
syslog_ip	Syslog 서버의 IP 주소를 지정합니다.
tcp	ASA가 syslog 서버로 메시지를 전송하는 데 TCP를 사용하도록 지정합니다.
udp	ASA가 syslog 서버로 메시지를 전송하는 데 UDP를 사용하도록 지정합니다.

기본값

기본 프로토콜은 UDP입니다.

format emblem 옵션에 대한 기본 설정은 false입니다.

secure 옵션에 대한 기본 설정은 false입니다.

기본 포트 번호는 다음과 같습니다.

- UDP - 514
- TCP - 1470

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0	이 명령이 추가되었습니다.
8.0(2)	**secure** 키워드가 추가되었습니다.
8.4(1)	연결 차단을 활성화 및 비활성화할 수 있습니다.

사용 지침

logging host *syslog_ip* **format emblem** 명령을 사용하면 각 syslog 서버에 대해 EMBLEM 형식의 로깅을 활성화할 수 있습니다. EMBLEM 형식의 로깅은 UDP syslog 메시지에만 사용할 수 있습니다. 특정 syslog 서버에 대해 EMBLEM 형식의 로깅을 활성화하면 해당 서버로 메시지가 전송됩니다. **logging timestamp** 명령을 사용하면 타임스탬프가 있는 메시지도 전송됩니다.

여러 **logging host** 명령을 사용하여 syslog 메시지를 모두 수신하는 추가 서버를 지정할 수 있습니다. 그러나 UDP 또는 TCP syslog 메시지만(둘 모두가 아니라) 수신하도록 서버를 구성할 수 있습니다.

TCP를 사용하여 syslog 서버로 메시지를 전송하도록 **logging host** 명령을 구성한 경우 연결 차단에 대한 기본 설정이 사용됩니다. TCP 기반 syslog 서버가 구성된 경우 **logging permit-hostdown** 명령으로 연결 차단을 비활성화할 수 있습니다.

참고 **logging host** 명령에서 **tcp** 옵션이 사용되는 경우, syslog 서버에 도달할 수 없으면 ASA는 방화벽을 통과하는 연결을 삭제합니다.

전에 **show running-config logging** 명령을 사용한 후 목록에서 명령을 찾아서 입력한 *port* 및 *protocol* 값만 표시할 수 있습니다. TCP는 6, UDP는 17로 표시됩니다. TCP 포트만 syslog 서버에서 작동합니다. *port*는 syslog 서버에서 수신 대기하는 포트와 동일해야 합니다.

참고 **logging host** 명령과 **secure** 키워드를 UDP와 함께 사용하려는 경우 오류 메시지가 표시됩니다.

대기 ASA에서는 TCP를 통한 syslog 전송이 지원되지 않습니다.

예

다음 예는 심각도 수준 0, 1, 2, 3의 syslog 메시지를 기본 프로토콜 및 포트 번호를 사용하는 내부 인터페이스의 syslog 서버로 전송하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging trap	Syslog 서버에 대한 로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging list

다양한 기준(로깅 수준, 이벤트 클래스 및 메시지 ID)으로 메시지를 지정하기 위해 다른 명령에서 사용할 로깅 목록을 생성하려면 글로벌 컨피그레이션 모드에서 **logging list** 명령을 사용합니다. 목록을 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[**-***end_id*]}

no logging list *name*

구문 설명

class *event_class*	(선택 사항) Syslog 메시지에 대한 이벤트 클래스를 설정합니다. 지정된 수준의 경우, 지정된 클래스의 syslog 메시지만 이 명령으로 식별됩니다. 클래스 목록은 "사용 지침" 섹션을 참조하십시오.
level *level*	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
message *start_id*[**-***end_id*]	메시지 ID 또는 ID의 범위를 지정합니다. 메시지의 기본 수준을 조회하려면 **show logging** 명령을 사용하거나 syslog 메시지 가이드를 참조하십시오.
name	로깅 목록 이름을 설정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

사용할 수 있는 logging 명령은 다음과 같습니다.

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

*event_class*에 사용할 수 있는 값은 다음과 같습니다.

- **auth** - 사용자 인증.
- **bridge** - 투명 방화벽.
- **ca** - PKI 인증 기관.
- **config** - 명령 인터페이스.
- **eap** - EAP(Extensible Authentication Protocol). EAP 세션 상태 변경, EAP 세션 쿼리 이벤트, EAP 헤더 및 패킷 내용의 16진수 덤프 등, Network Admission Control을 지원하는 이벤트 유형을 기록합니다.
- **eapoudp** - EAP(Extensible Authentication Protocol) over UDP. Network Admission Control을 지원하는 EAPoUDP 이벤트를 기록하고, EAPoUDP 헤더 및 패킷 내용의 완전한 레코드를 생성합니다.
- **email** - 이메일 프록시.
- **ha** - 장애 조치.
- **ids** - 침입 감지 시스템.
- **ip** - IP 스택.
- **nac** - Network Admission Control. 초기화, 예외 목록 일치, ACS 트랜잭션, 클라이언트리스 인증, 기본 ACL 애플리케이션, 재검증 등의 이벤트 유형을 기록합니다.
- **np** - 네트워크 프로세서.
- **ospf** - OSPF 라우팅.
- **rip** - RIP 라우팅.
- **session** - 사용자 세션.
- **snmp** - SNMP.
- **sys** - System.
- **vpn** - IKE 및 IPsec.
- **vpnc** - VPN 클라이언트.
- **vpnfo** - VPN 장애 조치.
- **vpnlb** - VPN 로드 밸런싱.

예

다음 예는 logging list 명령의 사용 방법을 보여줍니다.

```
ciscoasa(config)# logging list my-list 100100-100110
ciscoasa(config)# logging list my-list level critical
ciscoasa(config)# logging list my-list level warning class vpn
ciscoasa(config)# logging buffered my-list
```

위의 예는 지정된 기준과 일치하는 syslog 메시지가 로깅 버퍼로 전송될 것임을 나타냅니다. 이 예에서 지정한 기준은 다음과 같습니다.

- 100100~100110 범위에 해당하는 syslog 메시지 ID
- Critical 수준 이상의 모든 syslog 메시지(emergency, alert 또는 critical)
- Warning 수준 이상의 모든 VPN 클래스 syslog 메시지(emergency, alert, critical, error 또는 warning)

Syslog 메시지가 이러한 조건 중 하나를 충족하면 버퍼에 기록됩니다.

참고 목록 기준을 설계할 때 중복되는 메시지의 집합을 지정할 수 있습니다. 둘 이상의 기준 집합과 일치하는 syslog 메시지가 일반적으로 기록됩니다.

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging mail

ASA에서 이메일로 syslog 메시지를 전송하며 어떤 메시지를 이메일로 전송할지를 결정하도록 하려면 글로벌 컨피그레이션 모드에서 **logging mail** 명령을 사용합니다. 이메일로 syslog 메시지를 전송하는 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

구문 설명

level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
logging_list	이메일 수신자에게 전송할 메시지를 식별하는 목록을 지정합니다. 목록 생성에 대한 정보는 **logging list** 명령을 참조하십시오.

기본값

이메일에 대한 로깅은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이메일 syslog 메시지는 전송하는 이메일의 제목 줄에 나타납니다.

예

ASA가 이메일 주소로 syslog 메시지를 전송하도록 지정하려면 다음 기준을 사용합니다.

- Critical, alerts 또는 emergencies의 메시지를 전송합니다.
- 발신자 주소로 ciscosecurityappliance@example.com을 사용하여 메시지를 전송합니다.
- admin@example.com으로 메시지를 전송합니다.
- SMTP, 기본 서버 pri-smtp-host 및 보조 서버 sec-smtp-host를 사용하여 메시지를 전송합니다.

다음 명령을 입력합니다.

```
ciscoasa(config)# logging mail critical
ciscoasa(config)# logging from-address ciscosecurityappliance@example.com
ciscoasa(config)# logging recipient-address admin@example.com
ciscoasa(config)# smtp-server pri-smtp-host sec-smtp-host
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging from-address	Syslog 메시지의 발신 이메일 주소를 지정합니다.
logging list	메시지 선택 기준의 재사용 가능한 목록을 생성합니다.
logging recipient-address	Syslog 메시지의 수신 이메일 주소를 지정합니다.
smtp-server	SMTP 서버를 구성합니다.

logging message

Syslog 메시지의 로깅 수준을 지정하려면 글로벌 컨피그레이션 모드에서 **logging message** 명령과 **level** 키워드를 사용합니다. 메시지의 로깅 수준을 기본 수준으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

구문 설명

level *level*	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
syslog_id	활성화/비활성화하거나 심각도 수준을 수정할 syslog 메시지의 ID. 메시지의 기본 수준을 조회하려면 **show logging** 명령을 사용하거나 syslog 메시지 가이드를 참조하십시오.

기본값

기본적으로 모든 syslog 메시지가 활성화되며, 모든 메시지의 심각도 수준은 기본 수준으로 설정됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logging message 명령은 다음을 위해 사용할 수 있습니다.

- 메시지의 활성화 여부를 지정하기 위해
- 메시지의 심각도 수준을 표시하기 위해

메시지에 현재 할당된 수준 및 메시지의 활성화 여부를 확인하려면 **show logging** 명령을 사용할 수 있습니다.

ASA에서 특정 syslog 메시지를 생성하지 못하도록 하려면 글로벌 컨피그레이션 모드에서 **logging message** 명령(**level** 키워드 없이)의 **no** 형식을 사용합니다. ASA에서 특정 syslog 메시지를 생성하도록 하려면 **logging message** 명령(**level** 키워드 없이)을 사용합니다. **logging message** 명령의 이 두 가지 버전을 함께 사용할 수 있습니다.

예

다음 예에 나오는 일련의 명령은 **logging message** 명령을 사용하여 메시지의 활성화 여부 및 심각도 수준을 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

관련 명령

명령	설명
clear configure logging	모든 로깅 컨피그레이션을 지우거나 메시지 컨피그레이션만 지웁니다.
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging monitor

ASA가 SSH 및 Telnet 세션에서 syslog 메시지를 표시하도록 하려면 글로벌 컨피그레이션 모드에서 **logging monitor** 명령을 사용합니다. SSH 및 Telnet 세션에 syslog 메시지를 표시하지 못하게 하려면 이 명령의 **no** 형식을 사용합니다.

logging monitor [*logging_list* | *level*]

no logging monitor

구문 설명

level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
logging_list	SSH 또는 Telnet 세션으로 전송할 메시지를 식별하는 목록을 지정합니다. 목록 생성에 대한 정보는 **logging list** 명령을 참조하십시오.

기본값

기본적으로 ASA는 SSH 또는 Telnet 세션에 syslog 메시지를 표시하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logging monitor 명령은 현재 컨텍스트의 모든 세션에 대해 syslog 메시지를 활성화합니다. 그러나 각 세션에서 **terminal** 명령은 syslog 메시지를 해당 세션에서 표시할지 여부를 제어합니다.

예

다음 예는 콘솔 세션에서 syslog 메시지의 표시를 활성화하는 방법을 보여줍니다. **errors** 키워드를 사용하면 SSH 및 Telnet 세션에서 심각도 수준 0, 1, 2, 3의 메시지가 표시됩니다. **terminal** 명령을 사용하면 현재 세션에서 메시지가 표시됩니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging monitor errors
ciscoasa(config)# terminal monitor
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging list	메시지 선택 기준의 재사용 가능한 목록을 생성합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.
terminal	terminal 라인 매개변수를 설정합니다.

logging permit-hostdown

TCP 기반 syslog 서버의 상태가 새 사용자 세션과 관련되지 않도록 지정하려면 글로벌 컨피그레이션 모드에서 **logging permit-hostdown** 명령을 사용합니다. TCP 기반 syslog 서버를 사용할 수 없는 경우 ASA에서 새 사용자 세션을 거부하도록 하려면 이 명령의 **no** 형식을 사용합니다.

logging permit-hostdown

no logging permit-hostdown

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로, TCP 연결을 사용하는 syslog 서버에 대한 로깅을 활성화한 상태에서 어떤 이유로든 syslog 서버를 사용할 수 없는 경우 ASA는 새 네트워크 액세스 세션을 허용하지 않습니다. **logging permit-hostdown** 명령의 기본 설정은 false입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Syslog 서버로 메시지를 전송하기 위한 투명한 로깅 프로토콜로서 TCP를 사용하는 경우, ASA가 syslog 서버에 도달할 수 없으면 보안 조치로서 ASA에서 새 네트워크 액세스 세션이 거부됩니다. 이 제한을 제거하려면 **logging permit-hostdown** 명령을 사용할 수 있습니다.

예

다음 예는 TCP 기반 syslog 서버의 상태가 ASA에서 새 세션을 허용하는지 여부와 관련이 없도록 지정합니다. **show running-config logging** 명령의 출력에 **logging permit-hostdown** 명령이 포함되어 있으면, TCP 기반 syslog 서버의 상태는 새 네트워크 액세스 세션과 관련이 없는 것입니다.

```
ciscoasa(config)# logging permit-hostdown
ciscoasa(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging host	Syslog 서버를 정의합니다.
logging trap	Syslog 서버에 대한 로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging queue

로깅 컨피그레이션에 따라 처리를 시작하기까지 ASA가 큐에 보유할 수 있는 syslog 메시지의 수를 지정하려면 글로벌 컨피그레이션 모드에서 **logging queue** 명령을 사용합니다. 로깅 큐 크기를 기본값인 메시지 512개로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logging queue *queue_size*

no logging queue *queue_size*

구문 설명

queue_size	처리를 시작하기까지 syslog 메시지 저장용 큐에 추가할 수 있는 syslog 메시지의 수. 유효한 값은 플랫폼 유형에 따라 메시지 0~8192개입니다. 로깅 큐가 0으로 설정된 경우 큐는 플랫폼에 따라 최대 구성 가능한 크기(메시지 8192개)가 됩니다. ASA-5505에서 최대 큐 크기는 1024입니다. ASA-5510에서는 2048이고, 다른 모든 플랫폼에서는 8192입니다.

기본값

기본 큐 크기는 메시지 512개입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

트래픽이 과중하여 큐가 가득 찬 경우 ASA는 메시지를 폐기할 수 있습니다. ASA 5505에서 최대 큐 크기는 1024입니다. ASA-5510에서는 2048입니다. 다른 모든 플랫폼에서는 8192입니다.

예

다음 예는 **logging queue** 및 **show logging queue** 명령의 출력을 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# logging queue 0
ciscoasa(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

이 예에서는 **logging queue** 명령이 0으로 설정되었는데, 이는 큐가 최대 크기 8192로 설정됨을 의미합니다. 큐의 syslog 메시지는 로깅 컨피그레이션에 지정된 방식(예: syslog 메시지를 메일 수신자에게 전송, 플래시 메모리에 전송 등)으로 ASA에 의해 처리됩니다.

이 **show logging queue** 명령 예를 출력하면 큐에 현재 5개의 메시지가 있고, ASA가 마지막으로 부팅된 이후 특정 시점에 큐에 포함된 최대 메시지 수는 3513개였으며, 메시지 1개가 폐기되었음이 표시됩니다. 큐의 메시지 수가 무제한으로 설정되었더라도, 메시지를 큐에 추가하는 데 사용할 수 있는 블록 메모리가 없기 때문에 메시지가 폐기되었습니다.

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging rate-limit

Syslog 메시지가 생성되는 속도를 제한하려면 특별 권한 EXEC 모드에서 **logging rate-limit** 명령을 사용합니다. 속도 제한을 비활성화하려면 특별 권한 EXEC 모드에서 이 명령의 **no** 형식을 사용합니다.

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

[no] logging rate-limit [**unlimited** | {*num* [*interval*]}} **message** *syslog_id*] **level** *severity_level*

구문 설명

interval	(선택 사항) 메시지가 생성되는 속도를 측정하는 데 사용할 시간 간격(초 단위). 유효한 *interval* 값의 범위는 0~2147483647입니다.
level *severity_level*	특정 심각도 수준에 속하는 모든 syslog 메시지에 설정된 속도 제한을 적용합니다. 지정된 심각도 수준의 모든 syslog 메시지는 개별적으로 속도가 제한됩니다. 유효한 *severity_level* 범위는 1~7입니다.
message	이 syslog 메시지의 보고를 억제합니다.
num	지정된 시간 간격 동안 생성 가능한 syslog 메시지 수. 유효한 *num* 값의 범위는 0~2147483647입니다.
syslog_id	억제할 syslog 메시지의 ID. 유효한 값의 범위는 100000-999999입니다.
unlimited	속도 제한을 비활성화합니다. 즉, 로깅 속도에 제한이 없습니다.

기본값

기본 *interval* 설정은 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

명령 모드	방화벽 모드		보안 컨텍스트		
				다중	
	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(4)	이 명령이 추가되었습니다.

사용 지침

Syslog 메시지 심각도 수준은 다음과 같습니다.

- 0 - 시스템을 사용할 수 없음
- 1 - 즉각적인 조치 필요
- 2 - 심각한 상태
- 3 - 오류 상태
- 4 - 경고 상태

- 5 - 정상이지만 중요한 상태
- 6 - 정보 메시지
- 7 - 디버깅 메시지

예

Syslog 메시지 생성 속도를 제한하려면 특정 메시지 ID를 입력할 수 있습니다. 다음 예는 특정 메시지 ID 및 시간 간격을 사용하여 syslog 메시지 생성의 속도를 제한하는 방법을 보여줍니다.

```
ciscoasa(config)# logging rate-limit 100 600 message 302020
```

이 예는 지정된 간격 600초에서 속도 제한 100에 도달한 이후 syslog 메시지 302020이 호스트로 전송되는 것을 억제합니다.

Syslog 메시지 생성 속도를 제한하려면 특정 심각도 수준을 입력할 수 있습니다. 다음 예는 특정 심각도 수준 및 시간 간격을 사용하여 syslog 메시지 생성의 속도를 제한하는 방법을 보여줍니다.

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

이 예는 지정된 시간 간격 600초에서 지정된 속도 제한 1000으로 심각도 수준 6 미만의 모든 syslog 메시지를 억제합니다. 심각도 수준 6의 각 syslog 메시지는 속도 제한이 1000입니다.

관련 명령

명령	설명
clear running-config logging rate-limit	로깅 속도 제한 설정을 기본값으로 재설정합니다.
show logging	현재 내부 버퍼 또는 로깅 컨피그레이션 설정에 있는 메시지를 표시합니다.
show running-config logging rate-limit	현재 로깅 속도 제한 설정을 보여줍니다.

logging recipient-address

ASA에서 전송하는 syslog 메시지의 수신자 이메일 주소를 지정하려면 글로벌 컨피그레이션 모드에서 **logging recipient-address** 명령을 사용합니다. 이메일 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

구문 설명

address	이메일로 syslog 메시지를 전송할 때 수신자 이메일 주소를 지정합니다.
level	심각도 수준이 이어짐을 나타냅니다.
level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지 **참고** **logging recipient-address** 명령에서는 3보다 큰 심각도 수준을 사용하지 않는 것이 좋습니다. 심각도 수준이 높으면 버퍼 오버플로 때문에 syslog 메시지가 삭제될 수 있습니다. **logging recipient-address** 명령으로 지정하는 메시지 심각도 수준은 **logging mail** 명령으로 지정하는 메시지 심각도 수준을 재지정합니다. 예를 들어 **logging recipient-address** 명령은 심각도 수준 7을 지정하지만 **logging mail** 명령은 심각도 수준 3을 지정하는 경우, ASA는 심각도 수준 4, 5, 6, 7의 메시지를 포함한 모든 메시지를 수신자에게 전송합니다.

기본값

기본값은 errors 로깅 수준입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

최대 2개의 수신자 주소를 구성할 수 있습니다. 원하는 경우 각 수신자 주소에 대해 **logging mail** 명령으로 지정한 것과 다른 메시지 수준을 지정할 수 있습니다. 이메일에 의한 syslog 메시지 전송은 **logging mail** 명령으로 활성화됩니다.

더 많은 수신자에게 좀 더 긴급한 메시지를 보내려는 경우 이 명령을 사용합니다.

예

ASA가 이메일 주소로 syslog 메시지를 전송하도록 지정하려면 다음 기준을 사용합니다.

- Critical, alerts 또는 emergencies의 메시지를 전송합니다.
- 발신자 주소로 ciscosecurityappliance@example.com을 사용하여 메시지를 전송합니다.
- admin@example.com으로 메시지를 전송합니다.
- SMTP, 기본 서버 pri-smtp-host 및 보조 서버 sec-smtp-host를 사용하여 메시지를 전송합니다.

다음 명령을 입력합니다.

```
ciscoasa(config)# logging mail critical
ciscoasa(config)# logging from-address ciscosecurityappliance@example.com
ciscoasa(config)# logging recipient-address admin@example.com
ciscoasa(config)# smtp-server pri-smtp-host sec-smtp-host
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging from-address	Syslog 메시지의 발신 이메일 주소를 지정합니다.
logging mail	ASA에서 이메일로 syslog 메시지를 전송하도록 지정하고, 어떤 메시지를 이메일로 전송할지를 결정합니다.
smtp-server	SMTP 서버를 구성합니다.
show logging	활성화된 로깅 옵션을 표시합니다.

logging savelog

로그 버퍼를 플래시 메모리에 저장하려면 특별 권한 EXEC 모드에서 **logging savelog** 명령을 사용합니다.

logging savelog [*savefile*]

구문 설명

savefile	(선택 사항) 저장된 플래시 메모리 파일 이름. 파일 이름을 지정하지 않으면 ASA는 다음과 같은 타임스탬프 형식을 사용하여 로그 파일을 저장합니다. LOG-*YYYY-MM-DD-HHMMSS*.TXT *YYYY*는 연도이고 *MM*는 달이며 *DD*는 날짜입니다. *HHMMSS*는 시간, 분, 초를 나타냅니다.

기본값

기본값은 다음과 같습니다.

- 버퍼 크기는 4KB입니다.
- 최소 여유 플래시 메모리는 3MB입니다.
- 버퍼 로깅을 위한 최대 플래시 메모리 할당은 1MB입니다.
- 기본 로그 파일 이름은 "구문 설명" 섹션에서 설명합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

로그 버퍼를 플래시 메모리에 저장하려면 먼저 버퍼에 대한 로깅을 활성화해야 합니다. 그렇게 하지 않으면 로그 버퍼가 데이터를 플래시 메모리에 저장할 수 없습니다. 버퍼에 대한 로깅을 활성화하려면 **logging buffered** 명령을 사용합니다.

참고 **logging savelog** 명령은 버퍼를 지우지 않습니다. 버퍼를 지우려면 **clear logging buffer** 명령을 사용합니다.

예

다음 예는 로깅과 로그 버퍼를 활성화하고, 글로벌 컨피그레이션을 종료하고, latest-logfile.txt 파일 이름을 사용하여 로그 버퍼를 플래시 메모리에 저장합니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# exit
ciscoasa# logging savelog latest-logfile.txt
ciscoasa#
```

관련 명령

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
copy	파일을 한 위치에서 TFTP 또는 FTP 서버를 비롯한 다른 위치로 복사합니다.
delete	저장된 로그 파일 등의 디스크 파티션에서 파일을 삭제합니다.
logging buffered	로그 버퍼에 대한 로깅을 활성화합니다.
logging enable	로깅을 활성화합니다.

logging standby

장애 조치 스탠바이 ASA가 syslog 메시지를 로깅 대상으로 전송하도록 하려면 글로벌 컨피그레이션 모드에서 **logging standby** 명령을 사용합니다. Syslog 메시징 및 SNMP 로깅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

logging standby

no logging standby

구문 설명

이 명령에는 인수나 키워드가 없습니다.

명령 기본값

logging standby 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logging standby 명령을 사용하여 장애 조치가 발생할 경우 장애 조치 스탠바이 ASA의 syslog 메시지가 동기화를 유지하도록 합니다.

참고 **logging standby** 명령을 사용하면 syslog 서버, SNMP 서버 및 FTP 서버와 같은 공유 로깅 대상에서 트래픽이 두 배 증가합니다.

예

다음 예는 ASA가 syslog 메시지를 장애 조치 스탠바이 ASA로 전송하도록 설정합니다. **show logging** 명령의 출력을 보면 이 기능이 활성화되었음을 알 수 있습니다.

```
ciscoasa(config)# logging standby
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

관련 명령

명령	설명
failover	장애 조치 기능을 활성화합니다.
logging enable	로깅을 활성화합니다.
logging host	Syslog 서버를 정의합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging timestamp

Syslog 메시지에 메시지가 생성된 날짜와 시간을 포함하도록 지정하려면 글로벌 컨피그레이션 모드에서 **logging timestamp** 명령을 사용합니다. Syslog 메시지에서 날짜 및 시간을 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging timestamp

no logging timestamp

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 ASA는 syslog 메시지에 날짜와 시간을 포함하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logging timestamp 명령을 실행하면 ASA는 모든 syslog 메시지에 타임스탬프를 포함합니다.

예

다음 예에서는 모든 syslog 메시지에 타임스탬프 정보를 포함합니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

logging trap

ASA가 syslog 서버로 전송하는 syslog 메시지를 지정하려면 글로벌 컨피그레이션 모드에서 **logging trap** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

logging trap [*logging_list* | *level*]

no logging trap

구문 설명

level	Syslog 메시지의 최대 심각도 수준을 설정합니다. 예를 들어 심각도를 3으로 설정한 경우 ASA는 심각도 수준 3, 2, 1 또는 0에 대해 syslog 메시지를 생성합니다. 다음과 같은 숫자 또는 이름을 지정할 수 있습니다. • **0** 또는 **emergencies** - 시스템을 사용할 수 없음 • **1** 또는 **alerts** - 즉각적인 조치 필요 • **2** 또는 **critical** - 심각한 상태 • **3** 또는 **errors** - 오류 상태 • **4** 또는 **warnings** - 경고 상태 • **5** 또는 **notifications** - 정상이지만 중요한 상태 • **6** 또는 **informational** - 정보 메시지 • **7** 또는 **debugging** - 디버깅 메시지
logging_list	Syslog 서버로 전송할 메시지를 식별하는 목록을 지정합니다. 목록 생성에 대한 정보는 **logging list** 명령을 참조하십시오.

기본값

기본 syslog 메시지 트랩이 정의되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

투명한 로깅 프로토콜로서 TCP를 사용할 때 ASA가 syslog 서버에 도달할 수 없거나, syslog 서버가 잘못 구성되어 있거나, 디스크가 가득 찬 경우 보안 조치로서 ASA에서 새 네트워크 액세스 세션이 거부됩니다.

Syslog 서버에 장애가 발생하는 경우 UDP 기반 로깅은 ASA의 트래픽 통과를 차단하지 않습니다.

예

다음 예는 심각도 수준 0, 1, 2, 3의 syslog 메시지를 기본 프로토콜 및 포트 번호를 사용하는 내부 인터페이스에 상주하는 syslog 서버로 전송하는 방법을 보여줍니다.

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

관련 명령

명령	설명
logging enable	로깅을 활성화합니다.
logging host	Syslog 서버를 정의합니다.
logging list	메시지 선택 기준의 재사용 가능한 목록을 생성합니다.
show logging	활성화된 로깅 옵션을 표시합니다.
show running-config logging	실행 중인 컨피그레이션의 로깅 관련 부분을 표시합니다.

login

로컬 사용자 데이터베이스를 사용하여 특별 권한 EXEC 모드에 로그인하거나(username 명령 참조) 사용자 이름을 변경하려면 사용자 EXEC 모드에서 **login** 명령을 사용합니다.

login

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

사용자 EXEC 모드에서 **login** 명령을 사용하면 로컬 데이터베이스에 있는 어떤 사용자 이름으로도 특별 권한 EXEC 모드에 로그인할 수 있습니다. 인증 활성화(enable authentication)를 켜 둔 경우 **login** 명령은 **enable** 명령과 유사합니다(**aaa authentication console** 명령 참조). 인증 활성화와는 달리 **login** 명령은 로컬 사용자 이름 데이터베이스만 사용할 수 있으며, 이 명령에는 항상 인증이 필요합니다. 또한 어떤 CLI 모드에서든 **login** 명령을 사용하여 사용자를 변경할 수 있습니다.

사용자가 로그인할 때 특별 권한 EXEC 모드(및 모든 명령)에 액세스할 수 있게 하려면 사용자 권한 레벨을 2(기본값)~15로 설정합니다. 로컬 명령 권한 부여를 구성한 경우, 사용자는 해당 권한 레벨 이하에 지정된 명령만 입력할 수 있습니다. 자세한 내용은 **aaa authorization command**를 참조하십시오.

주의 CLI에 대한 액세스는 허용되지만 특별 권한 EXEC 모드 액세스는 허용되지 않는 사용자를 로컬 데이터베이스에 추가하려는 경우 명령 권한 부여를 구성해야 합니다. 명령 권한 부여가 없으면, 권한 레벨이 2 이상(2가 기본값)인 사용자는 CLI에서 각자의 비밀번호를 사용하여 특별 권한 EXEC 모드(및 모든 명령)에 액세스할 수 있습니다. RADIUS나 TACACS+ 인증을 사용할 수도 있습니다. 또는 모든 로컬 사용자를 레벨 1로 설정해 놓고 누가 시스템 enable 비밀번호를 사용하여 특별 권한 EXEC 모드에 액세스할 수 있는가를 제어하는 방법도 있습니다.

예

다음 예는 **login** 명령을 입력한 후의 프롬프트를 보여줍니다.

```
ciscoasa> login
Username:
```

관련 명령

명령	설명
aaa authorization command	CLI 액세스를 위한 명령 인증을 활성화합니다.
aaa authentication console	콘솔, 텔넷, HTTP, SSH 또는 **enable** 명령 액세스를 위한 인증을 요청합니다.
logout	CLI에서 로그아웃합니다.
username	로컬 데이터베이스에 사용자를 추가합니다.

login-button

WebVPN 사용자가 보안 어플라이언스에 연결할 때 표시되는 WebVPN 페이지 로그인 상자의 로그인 버튼을 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **login-button** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하고 값이 상속되도록 하려면 이 명령의 **no** 형식을 사용합니다.

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

구문 설명

style	스타일 변경을 지정합니다.
text	텍스트 변경을 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자).

기본값

기본 로그인 버튼 텍스트는 "Login"입니다.

다음은 기본 로그인 버튼 스타일입니다.

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 CSS(Cascading Style Sheet) 매개변수로서 표현됩니다. 이러한 매개변수에 대해 설명하는 것은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트 www.w3.org에서 제공하는 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수의 편리한 목록이 포함되어 있습니다.

WebVPN 페이지에 대한 가장 일반적인 변경 사항, 즉 페이지 색상과 관련된 몇 가지 팁은 다음과 같습니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값, 색상의 이름(HTML에서 인식되는 경우) 등을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며 각 색상은 0~255 범위의 십진수입니다. 쉼표로 구분된 엔트리는 다른 색상과 결합되는 각 색상의 강도 수준을 나타냅니다.
- HTML 형식은 #000000으로서, 여섯 자리 16진수 형식으로 되어 있습니다. 첫 번째와 두 번째는 빨강, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파랑을 나타냅니다.

참고 WebVPN 페이지를 손쉽게 사용자 지정하려면 색상 조각, 미리 보기 기능 등의 스타일 요소를 구성하기 위한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예는 로그인 버튼을 텍스트 "OK"로 사용자 지정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-button text OK
```

관련 명령

명령	설명
login-title	WebVPN 페이지 로그인 상자의 제목을 사용자 지정합니다.
group-prompt	WebVPN 페이지 로그인 상자의 그룹 프롬프트를 사용자 지정합니다.
password-prompt	WebVPN 페이지 로그인 상자의 비밀번호 프롬프트를 사용자 지정합니다.
username-prompt	WebVPN 페이지 로그인 상자의 사용자 이름 프롬프트를 사용자 지정합니다.

login-message

WebVPN 사용자가 보안 어플라이언스에 연결할 때 표시되는 WebVPN 페이지의 로그인 메시지를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **login-message** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하고 값이 상속되도록 하려면 이 명령의 **no** 형식을 사용합니다.

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

구문 설명

text	텍스트 변경을 지정합니다.
style	스타일 변경을 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자).

기본값

기본 로그인 메시지는 "Please enter your username and password."입니다.

기본 로그인 메시지 스타일은 background-color:#CCCCCC;color:black입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
WebVPN 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 CSS(Cascading Style Sheet) 매개변수로서 표현됩니다. 이러한 매개변수에 대해 설명하는 것은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트 www.w3.org에서 제공하는 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수의 편리한 목록이 포함되어 있습니다.

WebVPN 페이지에 대한 가장 일반적인 변경 사항, 즉 페이지 색상과 관련된 몇 가지 팁은 다음과 같습니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값, 색상의 이름(HTML에서 인식되는 경우) 등을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며 각 색상은 0~255 범위의 십진수입니다. 쉼표로 구분된 엔트리는 다른 색상과 결합되는 각 색상의 강도 수준을 나타냅니다.
- HTML 형식은 #000000으로서, 여섯 자리 16진수 형식으로 되어 있습니다. 첫 번째와 두 번째는 빨강, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파랑을 나타냅니다.

참고 WebVPN 페이지를 손쉽게 사용자 지정하려면 색상 조각, 미리 보기 기능 등의 스타일 요소를 구성하기 위한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예에서 로그인 메시지 텍스트는 "username and password"로 설정됩니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-message text username and password
```

관련 명령

명령	설명
login-title	WebVPN 페이지에서 로그인 상자의 제목을 사용자 지정합니다.
username-prompt	WebVPN 페이지 로그인의 사용자 이름 프롬프트를 사용자 지정합니다.
password-prompt	WebVPN 페이지 로그인의 비밀번호 프롬프트를 사용자 지정합니다.
group-prompt	WebVPN 페이지 로그인의 그룹 프롬프트를 사용자 지정합니다.

login-title

WebVPN 사용자에게 표시되는 WebVPN 페이지에서 로그인 상자의 제목을 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **login-title** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하고 값이 상속되도록 하려면 이 명령의 **no** 형식을 사용합니다.

login-title {**text** | **style**} *value*

[**no**] **login-title** {**text** | **style**} *value*

구문 설명

text	텍스트 변경을 지정합니다.
style	HTML 스타일 변경을 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자).

기본값

기본 로그인 텍스트는 "Login"입니다.

로그인 제목의 기본 HTML 스타일은 background-color: #666666; color: white입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 CSS(Cascading Style Sheet) 매개변수로서 표현됩니다. 이러한 매개변수에 대해 설명하는 것은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트 www.w3.org에서 제공하는 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수의 편리한 목록이 포함되어 있습니다.

WebVPN 페이지에 대한 가장 일반적인 변경 사항, 즉 페이지 색상과 관련된 몇 가지 팁은 다음과 같습니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값, 색상의 이름(HTML에서 인식되는 경우) 등을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며 각 색상은 0~255 범위의 십진수입니다. 쉼표로 구분된 엔트리는 다른 색상과 결합되는 각 색상의 강도 수준을 나타냅니다.
- HTML 형식은 #000000으로서, 여섯 자리 16진수 형식으로 되어 있습니다. 첫 번째와 두 번째는 빨강, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파랑을 나타냅니다.

참고 WebVPN 페이지를 손쉽게 사용자 지정하려면 색상 조각, 미리 보기 기능 등의 스타일 요소를 구성하기 위한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예는 로그인 제목 스타일을 구성합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

관련 명령

명령	설명
login-message	WebVPN 로그인 페이지의 로그인 메시지를 사용자 지정합니다.
username-prompt	WebVPN 로그인 페이지의 사용자 이름 프롬프트를 사용자 지정합니다.
password-prompt	WebVPN 로그인 페이지의 비밀번호 프롬프트를 사용자 지정합니다.
group-prompt	WebVPN 로그인 페이지의 그룹 프롬프트를 사용자 지정합니다.

logo

WebVPN 사용자가 보안 어플라이언스에 연결할 때 표시되는 WebVPN 페이지의 로고를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **logo** 명령을 사용합니다. 컨피그레이션에서 로고를 제거하고 기본값(Cisco 로고)을 재설정하려면 이 명령의 **no** 형식을 사용합니다.

logo {**none** | **file** {*path value*}}

[**no**] **logo** {**none** | **file** {*path value*}}

구문 설명

file	로고가 포함된 파일을 제공함을 나타냅니다.
none	로고가 없음을 나타냅니다. Null 값을 설정하여 로고를 허용하지 않습니다. 로고의 상속을 차단합니다.
path	파일 이름의 경로. 가능한 경로는 disk0:, disk1: 또는 flash:입니다.
value	로고의 파일 이름을 지정합니다. 최대 길이는 공백 없이 255자입니다. 파일 형식은 JPG, PNG 또는 GIF여야 하며 100KB보다 작아야 합니다.

기본값

기본 로고는 Cisco 로고입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

지정한 파일 이름이 존재하지 않으면 오류 메시지가 표시됩니다. 로고 파일을 제거했지만 컨피그레이션에서 여전히 이를 가리키면 로고가 표시되지 않습니다.

파일 이름에는 공백을 포함할 수 없습니다.

예

다음 예에서 cisco_logo.gif 파일은 사용자 지정 로고를 포함합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

관련 명령

명령	설명
title	WebVPN 페이지의 제목을 사용자 지정합니다.
page style	CSS(Cascading Style Sheet) 매개변수를 사용하여 WebVPN 페이지를 사용자 지정합니다.

logout

CLI를 종료하려면 사용자 EXEC 모드에서 **logout** 명령을 사용합니다.

logout

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

logout 명령을 사용하면 ASA에서 로그아웃할 수 있습니다. 일반 모드로 돌아가려면 **exit** 또는 **quit** 명령을 사용할 수 있습니다.

예

다음 예는 ASA에서 로그아웃하는 방법을 보여줍니다.

```
ciscoasa> logout
```

관련 명령

명령	설명
login	로그인 프롬프트를 시작합니다.
exit	액세스 모드를 종료합니다.
quit	컨피그레이션 또는 특별 권한 모드를 종료합니다.

logout-message

WebVPN 사용자가 WebVPN 서비스에서 로그아웃할 때 표시되는 WebVPN 로그아웃 화면의 로그아웃 메시지를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **logout-message** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하고 값이 상속되도록 하려면 이 명령의 **no** 형식을 사용합니다.

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

구문 설명

style	스타일 변경을 지정합니다.
text	텍스트 변경을 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자).

기본값

기본 로그아웃 메시지 텍스트는 "Goodbye"입니다.

기본 로그아웃 메시지 스타일은 background-color:#999999;color:black입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
WebVPN 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 CSS(Cascading Style Sheet) 매개변수로서 표현됩니다. 이러한 매개변수에 대해 설명하는 것은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트 www.w3.org에서 제공하는 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수의 편리한 목록이 포함되어 있습니다.

WebVPN 페이지에 대한 가장 일반적인 변경 사항, 즉 페이지 색상과 관련된 몇 가지 팁은 다음과 같습니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값, 색상의 이름(HTML에서 인식되는 경우) 등을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며 각 색상은 0~255 범위의 십진수입니다. 쉼표로 구분된 엔트리는 다른 색상과 결합되는 각 색상의 강도 수준을 나타냅니다.
- HTML 형식은 #000000으로서, 여섯 자리 16진수 형식으로 되어 있습니다. 첫 번째와 두 번째는 빨강, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파랑을 나타냅니다.

참고 WebVPN 페이지를 손쉽게 사용자 지정하려면 색상 조각, 미리 보기 기능 등의 스타일 요소를 구성하기 위한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예는 로그인 메시지 스타일을 구성합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style:
italic; font-weight: bold
```

관련 명령

명령	설명
logout-title	WebVPN 페이지의 로그아웃 제목을 사용자 지정합니다.
group-prompt	WebVPN 페이지 로그인 상자의 그룹 프롬프트를 사용자 지정합니다.
password-prompt	WebVPN 페이지 로그인 상자의 비밀번호 프롬프트를 사용자 지정합니다.
username-prompt	WebVPN 페이지 로그인 상자의 사용자 이름 프롬프트를 사용자 지정합니다.

9 장

mac address through match dscp 명령

mac address

액티브 및 스탠바이 유닛용 가상 MAC 주소를 지정하려면 장애 조치 그룹 컨피그레이션 모드에서 **mac address** 명령을 사용합니다. 기본 가상 MAC 주소를 복원하려면 이 명령의 **no** 형식을 사용합니다.

mac address *phy_if* [*active_mac*] [*standby_mac*]

no mac address *phy_if* [*active_mac*] [*standby_mac*]

구문 설명

phy_if	MAC 주소를 설정하기 위한 인터페이스의 실제 이름.
active_mac	액티브 유닛에 대한 가상 MAC 주소. MAC 주소는 h.h.h 형식으로 입력해야 하며, 여기서 h는 16비트 16진수입니다.
standby_mac	스탠바이 유닛에 대한 가상 MAC 주소. MAC 주소는 h.h.h 형식으로 입력해야 하며, 여기서 h는 16비트 16진수입니다.

기본값

기본값은 다음과 같습니다.

- 액티브 유닛 기본 MAC 주소: 00a0.c9*physical_port_number.failover_group_id*01.
- 스탠바이 유닛 기본 MAC 주소: 00a0.c9*physical_port_number.failover_group_id*02.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
장애 조치 그룹 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

장애 조치 그룹에 대해 가상 MAC 주소가 정의되어 있지 않으면 기본값이 사용됩니다.

동일한 네트워크에 액티브/액티브 장애 조치 쌍이 둘 이상 있는 경우 기본 가상 MAC 주소를 지정하는 방식 때문에, 한 쌍의 인터페이스에 할당된 것과 동일한 기본 가상 MAC 주소가 다른 쌍의 인터페이스에도 할당될 가능성이 있습니다. 네트워크에서 중복되는 MAC 주소를 사용하지 않으려면 각 물리적 인터페이스에 가상 액티브 및 스탠바이 MAC 주소를 할당해야 합니다.

다른 명령이나 방법을 사용하여 MAC 주소를 설정할 수도 있으나, 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

예

다음의 부분적인 예는 장애 조치 그룹에 대해 가능한 컨피그레이션을 보여줍니다.

```
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	액티브/액티브 장애 조치에 대한 장애 조치 그룹을 정의합니다.
failover mac address	물리적 인터페이스의 가상 MAC 주소를 지정합니다.

mac-address

인터페이스 또는 하위 인터페이스에 사설 MAC 주소를 수동으로 할당하려면 인터페이스 컨피그레이션 모드에서 **mac-address** 명령을 사용합니다. 다중 컨텍스트 모드에서는 이 명령으로 각 컨텍스트의 인터페이스에 고유한 MAC 주소를 할당할 수 있습니다. 클러스터의 개별 인터페이스에는 MAC 주소의 클러스터 풀을 할당할 수 있습니다. MAC 주소를 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

mac-address {*mac_address* [**standby** *mac_address*] | **cluster-pool** *pool_name*}

no mac-address [*mac_address* [**standby** *mac_address*] | **cluster-pool** *pool_name*]

구문 설명

cluster-pool *pool_name*	개별 인터페이스 모드의 클러스터(**cluster interface-mode** 명령 참조) 또는 클러스터 인터페이스 모드의 관리 인터페이스의 경우, 각 클러스터 멤버의 지정된 인터페이스에 사용할 MAC 주소의 풀을 설정합니다. **mac-address pool** 명령을 사용하여 풀을 정의합니다.
mac_address	이 인터페이스의 MAC 주소를 H.H.H 형식으로 설정하며, 여기서 H는 16비트 16진수입니다. 예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. 장애 조치를 사용하는 경우 이 MAC 주소는 액티브 MAC 주소입니다. **참고** 자동 생성 주소(**mac-address auto** 명령)는 A2로 시작하므로, 자동 생성도 사용하려는 경우 수동 MAC 주소가 A2로 시작해서는 안 됩니다.
standby *mac_address*	(선택 사항) 장애 조치용 스탠바이 MAC 주소를 설정합니다. 활성 유닛이 장애 조치되고 대기 유닛이 활성 상태가 되면, 네트워크 중단을 최소화하기 위해 새 활성 유닛에서 활성 MAC 주소를 사용하기 시작하고 기존 활성 유닛은 대기 주소를 사용합니다.

기본값

기본 MAC 주소는 물리적 인터페이스의 번인된(burned-in) MAC 주소입니다. 하위 인터페이스는 물리적 인터페이스 MAC 주소를 상속합니다. 몇몇 명령이 물리적 인터페이스 MAC 주소(단일 모드의 이 명령 포함)를 설정하므로 상속되는 주소는 해당 컨피그레이션에 따라 달라집니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.0(5)/8.2(2)	**mac-address auto** 명령도 함께 사용할 경우 MAC 주소를 시작하기 위해 A2를 사용하는 것이 제한되었습니다.
9.0(1)	클러스터링 지원을 위해 **cluster-pool** 키워드가 추가되었습니다.

사용 지침

다중 컨텍스트 모드에서는 여러 컨텍스트가 하나의 인터페이스를 공유할 경우 각 컨텍스트에서 인터페이스에 고유한 MAC 주소를 지정할 수 있습니다. 이 기능 덕분에 ASA에서 손쉽게 적절한 컨텍스트로 패킷을 분류할 수 있습니다. 고유한 MAC 주소 없이 공유 인터페이스를 사용할 수 있으나, 몇 가지 제한이 있습니다. 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

이 명령으로 각 MAC 주소를 직접 할당할 수도 있고, **mac-address auto** 명령을 사용하여 컨텍스트에서 공유 인터페이스의 MAC 주소를 자동으로 생성할 수도 있습니다. MAC 주소를 자동으로 생성하는 경우 생성된 주소를 재지정하려면 **mac-address** 명령을 사용할 수 있습니다.

단일 컨텍스트 모드에서는 또는 다중 컨텍스트 모드에서 공유되지 않는 인터페이스에 대해서는 하위 인터페이스에 고유 MAC 주소를 지정해야 하는 경우가 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다.

다른 명령이나 방법을 사용하여 MAC 주소를 설정할 수도 있으나, 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

예

다음 예는 GigabitEthernet 0/1.1의 MAC 주소를 구성합니다.

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
ciscoasa/contextA(config-if)# no shutdown
```

관련 명령

명령	설명
failover mac address	액티브/스탠바이 장애 조치에 대해 물리적 인터페이스의 액티브 및 스탠바이 MAC 주소를 설정합니다.
mac address	액티브/액티브 장애 조치에 대해 물리적 인터페이스의 액티브 및 스탠바이 MAC 주소를 설정합니다.
mac-address auto	다중 컨텍스트 모드에서 공유 인터페이스에 대해 MAC 주소(액티브 및 스탠바이)를 자동 생성합니다.
mode	보안 컨텍스트 모드를 multiple 또는 single로 설정합니다.
show interface	MAC 주소를 비롯한 인터페이스 특성을 보여줍니다.

mac-address auto

각 공유 컨텍스트 인터페이스에 사설 MAC 주소를 자동으로 할당하려면 글로벌 컨피그레이션 모드에서 **mac-address auto** 명령을 사용합니다. 자동 MAC 주소를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

mac-address auto [**prefix** *prefix*]

no mac-address auto

구문 설명

prefix *prefix*	(선택 사항) MAC 주소의 일부로서 사용자 정의 접두사를 설정합니다. *prefix*는 0~65535 범위의 십진수 값입니다. 접두사를 입력하지 않으면 ASA에서 기본 접두사를 생성합니다. 이 접두사는 4자리 16진수로 변환됩니다. 접두사를 사용할 경우 각 ASA에서 고유한 MAC 주소의 사용아 보장되므로(서로 다른 접두사 값 사용), 예를 들면 네트워크 세그먼트에서 여러 ASA를 보유할 수 있습니다.

기본값

자동 MAC 주소 생성이 활성화되어 있습니다. 자동 생성되는 접두사를 사용합니다. ASA는 인터페이스의 마지막 2바이트(ASA 5500) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동 생성합니다. 기존의 자동 생성 방법(접두사 없음)은 사용할 수 없습니다.

MAC 주소 생성을 비활성화한 경우 다음 기본 MAC 주소를 참조하십시오.

- ASA 5500 시리즈 어플라이언스 - 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.
- ASASM - 모든 VLAN 인터페이스가 백플레인 MAC 주소에서 파생된 동일한 MAC 주소를 사용합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.0(5)/8.2(2)	**prefix** 키워드가 추가되었습니다. 접두사를 사용하고, 고정 시작 값(A2)을 사용하고, 장애 조치 쌍에서는 기본 유닛 MAC 주소와 보조 유닛 MAC 주소에 서로 다른 체계를 사용하도록 MAC 주소 형식이 변경되었습니다. 또한 MAC 주소는 다시 로드하더라도 유지됩니다. 명령 구문 분석기에서 자동 생성 활성화 여부를 확인합니다. 직접 MAC 주소를 지정하는 것도 원할 경우 수동 MAC 주소는 A2로 시작할 수 없습니다.

릴리스	수정
8.5(1)	이제 자동 생성이 기본적으로 활성화됩니다(**mac-address auto**).
8.6(1)	이제 ASA의 자동 MAC 주소 생성 컨피그레이션은 기본 접두사를 사용하도록 변환됩니다. ASA는 인터페이스의 마지막 2바이트(ASA 5500) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동 생성합니다. 다시 로드할 때 또는 MAC 주소 생성을 다시 활성화할 경우 이 변환이 자동으로 이루어집니다. 기존의 MAC 주소 생성 방식은 더 이상 사용되지 않습니다. **참고** 장애 조치 쌍의 히트리스 업그레이드를 유지하고자 ASA에서는 장애 조치가 활성화된 경우 다시 로드할 때 기존 컨피그레이션의 MAC 주소 방식을 변환하지 *않습니다*.

사용 지침

컨텍스트에서 인터페이스를 공유하도록 하려면 각 공유 컨텍스트 인터페이스에 고유한 MAC 주소를 할당하면 됩니다. 이 MAC 주소는 컨텍스트 내에서 패킷을 분류하는 데 사용됩니다. 인터페이스를 공유하고 있지만 각 컨텍스트의 인터페이스에 고유한 MAC 주소가 없는 경우, 패킷을 분류하는 데 수신 IP 주소가 사용됩니다. 수신 주소는 컨텍스트 NAT 컨피그레이션과 비교되는데, 이 방법은 MAC 주소 방법과 비교하면 일부 제한이 있습니다. 패킷 분류에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 컨텍스트 내에서 그 인터페이스의 MAC 주소를 직접 설정할 수 있습니다. MAC 주소를 수동으로 설정하는 방법은 **mac-address** 명령을 참조하십시오.

수동 MAC 주소와의 상호 작용

직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우 직접 지정한 수동 MAC 주소가 사용됩니다. 나중에 수동 MAC 주소를 삭제할 경우 자동 생성 주소가 사용됩니다.

자동 생성 주소는 A2로 시작하므로, 자동 생성도 사용하려는 경우 수동 MAC 주소가 A2로 시작해서는 안 됩니다.

장애 조치 MAC 주소

장애 조치에 사용할 수 있도록 ASA에서는 인터페이스마다 활성 MAC 주소와 대기 MAC 주소를 모두 생성합니다. 활성 유닛이 장애 조치하고 대기 유닛이 활성화되면 새 활성 유닛은 활성 MAC 주소를 사용하기 시작하므로 네트워크 중단이 최소화됩니다. 자세한 내용은 "접두사를 사용하는 MAC 주소 형식" 섹션을 참조하십시오.

prefix 키워드가 추가되기 전 **mac-address auto** 명령의 기존 버전으로 장애 조치 유닛을 업그레이드하려면 "접두사가 없는 MAC 주소 형식(기존 방법)" 섹션을 참조하십시오.

접두사를 사용하는 MAC 주소 형식

ASA에서는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2*xx*.*yyzz*.*zzzz*

여기서 *xx*.*yy*는 사용자가 정의한 접두사이거나 인터페이스의 마지막 2바이트(ASA 5500) 또는 백플레인(ASASM) MAC 주소를 기반으로 자동 생성된 접두사이며, *zz*.*zzzz*는 ASA에 의해 생성된 내부 카운터입니다. 대기 MAC 주소는 동일하지만, 내부 카운터가 1만큼 큽니다.

접두사가 어떻게 사용되는지 예를 들어 설명하자면, 접두사를 77로 설정한 경우ASA는 77을 16진수 값인 004D(*yyxx*)로 변환합니다. 접두사가 MAC 주소에서 쓰일 때는 ASA 기본 형식에 부합하도록 역전됩니다(*xxyy*).

A2**4D.00***zz*.*zzzz*

접두사가 1009 (03F1)일 때 MAC 주소는 다음과 같습니다.

A2**F1.03***zz.zzzz*

접두사가 없는 MAC 주소 형식 (기존 방법)

장애 조치를 사용하며 버전 8.6 이상으로 업그레이드한 경우 이 방법을 사용할 수 있습니다. 이 경우 접두사 방법을 수동으로 활성화해야 합니다.

접두사가 없으면 다음 형식을 사용하여 MAC 주소가 생성됩니다.

- 액티브 유닛 MAC 주소: 12*_slot.port_subid.contextid*.
- 스탠바이 유닛 MAC 주소: 02*_slot.port_subid.contextid*.

인터페이스 슬롯이 없는 플랫폼의 경우 슬롯은 항상 0입니다. *port*는 인터페이스 포트입니다. *subid*는 보이지 않는 하위 인터페이스의 내부 ID입니다. *contextid*는 컨텍스트의 내부 ID이며 **show context detail** 명령으로 볼 수 있습니다. 예를 들어, ID가 1인 컨텍스트의 GigabitEthernet 0/1.200에는 다음과 같은 MAC 주소가 생성됩니다. 여기서 하위 인터페이스 200의 내부 ID는 31입니다.

- 액티브: 1200.0131.0001
- 스탠바이: 0200.0131.0001

이 MAC 주소 생성 방법을 사용하면 영구 MAC 주소가 다시 로드 간에 지속되지 않으며, 동일한 네트워크 세그먼트에 여러 ASA를 둘 수 없고(고유한 MAC 주소가 보장되지 않으므로), 수동으로 할당한 MAC 주소로 MAC 주소의 중복을 차단할 수 없습니다. 이러한 문제를 피하려면 MAC 주소 생성 시 접두사를 사용하는 것이 좋습니다.

MAC 주소가 생성될 경우

컨텍스트에서 인터페이스에 대해 **nameif** 명령을 구성하면 새 MAC 주소가 즉시 생성됩니다. 컨텍스트 인터페이스를 구성한 다음 이 명령을 활성화하면, 명령 입력 직후에 모든 인터페이스에 대해 MAC 주소가 생성됩니다. **no mac-address auto** 명령을 사용하면 각 인터페이스의 MAC 주소가 기본 MAC 주소로 돌아갑니다. 예를 들어, GigabitEthernet 0/1의 하위 인터페이스는 다시 GigabitEthernet 0/1의 MAC 주소를 사용하게 됩니다.

다른 방법을 사용하여 MAC 주소 설정

다른 명령이나 방법을 사용하여 MAC 주소를 설정할 수도 있으나, 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

시스템 컨피그레이션에서 MAC 주소 보기

할당된 MAC 주소를 시스템 실행 공간에서 보려면 **show running-config all context** 명령을 입력합니다.

지정된 MAC 주소를 보려면 **all** 옵션이 필요합니다. 이 명령은 글로벌 컨피그레이션 모드에서만 사용자 구성이 가능하지만, **mac-address auto** 명령은 할당된 MAC 주소와 함께 각 컨텍스트에 대한 컨피그레이션에서 읽기 전용 엔트리로 나타납니다. 컨텍스트 내에서 **nameif** 명령으로 구성된, 할당된 인터페이스만 MAC 주소를 받습니다.

참고 직접 인터페이스에 MAC 주소를 지정하지만 자동 생성도 활성화한 경우, 수동 MAC 주소가 사용되지만 자동 생성 주소도 계속 컨피그레이션에 표시됩니다. 나중에 수동 MAC 주소를 삭제하면, 여기에 표시되었던 자동 생성 주소가 사용됩니다.

컨텍스트 내 MAC 주소 보기

컨텍스트 내 각 인터페이스에 사용되는 MAC 주소를 보려면 **show interface | include (Interface)|(MAC)** 명령을 입력합니다.

참고 **show interface** 명령은 사용 중인 MAC 주소를 보여줍니다. 직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우, 시스템 컨피그레이션 내에서는 사용되지 않은 자동 생성 주소만 볼 수 있습니다.

예

다음 예는 접두사 78로 자동 MAC 주소 생성을 활성화합니다.

```
ciscoasa(config)# mac-address auto prefix 78
```

다음은 **show running-config all context admin** 명령의 출력이며, Management0/0 인터페이스에 지정된 기본 및 대기 MAC 주소를 보여줍니다.

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

다음은 **show running-config all context** 명령의 출력이며, 모든 컨텍스트 인터페이스의 모든 MAC 주소(기본 및 대기)를 보여줍니다. GigabitEthernet0/0 및 GigabitEthernet0/1 기본 인터페이스는 컨텍스트 내에서 **nameif** 명령으로 구성되지 않았으므로, 어떤 MAC 주소도 생성되지 않았습니다.

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

관련 명령

명령	설명
failover mac address	액티브/스탠바이 장애 조치에 대해 물리적 인터페이스의 액티브 및 스탠바이 MAC 주소를 설정합니다.
mac address	액티브/액티브 장애 조치에 대해 물리적 인터페이스의 액티브 및 스탠바이 MAC 주소를 설정합니다.
mac-address	물리적 인터페이스 또는 하위 인터페이스에 대해 MAC 주소(액티브 및 스탠바이)를 수동으로 설정합니다. 다중 컨텍스트 모드에서는 동일한 인터페이스의 각 컨텍스트에서 서로 다른 MAC 주소를 설정할 수 있습니다.
mode	보안 컨텍스트 모드를 multiple 또는 single로 설정합니다.
show interface	MAC 주소를 비롯한 인터페이스 특성을 보여줍니다.

mac-address pool

ASA 클러스터의 개별 인터페이스에서 사용할 MAC 주소 풀을 추가하려면 글로벌 컨피그레이션 모드에서 **mac-address pool** 명령을 사용합니다. 사용되지 않은 풀을 제거하려면 이 명령의 **no** 형식을 사용합니다.

mac-address pool *name start_mac_address* **-** *end_mac_address*

no mac-address pool *name* [*start_mac_address* **-** *end_mac_address*]

구문 설명

name	풀의 이름을 최대 63자로 지정합니다.
start_mac_address **-** *end_mac_address*	첫 번째 MAC 주소 및 마지막 MAC 주소를 지정합니다. 대시(-) 전후에 공백을 추가해야 합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스 컨피그레이션 모드의 **mac-address cluster-pool** 명령에서 풀을 사용할 수 있습니다. 인터페이스에 대해 수동으로 MAC 주소를 구성하는 것은 일반적이지 않지만, 그렇게 해야 하는 특별한 이유가 있는 경우 이 풀을 사용하여 각 인터페이스에 고유한 MAC 주소를 할당할 수 있습니다.

예

다음 예는 8개의 MAC 주소가 포함된 MAC 주소 풀을 추가하고 이를 gigabitethernet 0/0 인터페이스에 할당합니다.

```
ciscoasa(config)# mac-address pool pool1 000C.F142.4CD1 - 000C.F142.4CD7
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-ifc)# mac-address cluster-pool pool1
```

관련 명령

명령	설명
interface	인터페이스를 구성합니다.
mac-address	인터페이스에 대한 MAC 주소를 구성합니다.

mac-address-table aging-time

MAC 주소 테이블 엔트리에 대한 시간 제한을 설정하려면 글로벌 컨피그레이션 모드에서 **mac-address-table aging-time** 명령을 사용합니다. 기본값을 5분으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

mac-address-table aging-time *timeout_value*

no mac-address-table aging-time

구문 설명

timeout_value	시간이 초과되기까지 MAC 주소 엔트리가 MAC 주소 테이블에 머무는 시간으로, 범위는 5~720분(12시간)입니다. 5분이 기본값입니다.

기본값

시간 제한 기본값은 5분입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

사용 지침 없음

예

다음 예는 MAC 주소 시간 제한을 10분으로 설정합니다.

```
ciscoasa(config)# mac-address-timeout aging time 10
```

관련 명령

명령	설명
arp-inspection	ARP 패킷을 고정 ARP 엔트리와 비교하는 ARP 검사를 활성화합니다.
firewall transparent	방화벽 모드를 투명 모드로 설정합니다.
mac-address-table static	고정 MAC 주소 엔트리를 MAC 주소 테이블에 추가합니다.
mac-learn	MAC 주소 파악을 비활성화합니다.
show mac-address-table	동적 및 고정 엔트리를 포함하여 MAC 주소 테이블을 보여줍니다.

mac-address-table static

MAC 주소 테이블에 고정 엔트리를 추가하려면 글로벌 컨피그레이션 모드에서 **mac-address-table static** 명령을 사용합니다. 고정 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다. 일반적으로 MAC 주소는 특정 MAC 주소의 트래픽이 인터페이스에 들어올 때 MAC 주소 테이블에 동적으로 추가됩니다. 원하는 경우 고정 MAC 주소를 MAC 주소 테이블에 추가할 수 있습니다. 고정 항목을 추가함으로써 얻을 수 있는 한 가지 혜택은 MAC 스푸핑을 차단할 수 있다는 점입니다. 동일한 MAC 주소를 고정 항목으로 보유한 클라이언트에서 고정 항목이 일치하지 않는 인터페이스에 트래픽을 전송하려고 시도할 경우, ASA에서는 해당 트래픽을 누락하며 시스템 메시지가 생성됩니다.

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

구문 설명

interface_name	소스 인터페이스
mac_address	테이블에 추가할 MAC 주소

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 고정 MAC 주소 엔트리를 MAC 주소 테이블에 추가합니다.

```
ciscoasa(config)# mac-address-table static inside 0010.7cbe.6101
```

관련 명령

명령	설명
arp	고정 ARP 항목을 추가합니다.
firewall transparent	방화벽 모드를 투명 모드로 설정합니다.
mac-address-table aging-time	동적 MAC 주소 엔트리용 시간 제한을 설정합니다.
mac-learn	MAC 주소 파악을 비활성화합니다.
show mac-address-table	MAC 주소 테이블 엔트리를 표시합니다.

mac-learn

인터페이스에 대한 MAC 주소 학습을 비활성화하려면 글로벌 컨피그레이션 모드에서 **mac-learn** 명령을 사용합니다. MAC 주소 학습을 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다. 기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, ASA에서는 해당 항목을 MAC 주소 테이블에 추가합니다. 원하는 경우 MAC 주소 학습을 비활성화할 수 있습니다.

mac-learn *interface_name* **disable**

no mac-learn *interface_name* **disable**

구문 설명

interface_name	MAC 학습을 비활성화할 인터페이스.
disable	MAC 학습을 비활성화합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 외부 인터페이스에서 MAC 학습을 비활성화합니다.

```
ciscoasa(config)# mac-learn outside disable
```

관련 명령

명령	설명
clear configure mac-learn	**mac-learn** 컨피그레이션을 기본값으로 설정합니다.
firewall transparent	방화벽 모드를 투명 모드로 설정합니다.
mac-address-table static	고정 MAC 주소 엔트리를 MAC 주소 테이블에 추가합니다.
show mac-address-table	동적 및 고정 엔트리를 포함하여 MAC 주소 테이블을 보여줍니다.
show running-config mac-learn	**mac-learn** 컨피그레이션을 보여줍니다..

mac-list

인증 및/또는 권한 부여에서 MAC 주소를 제외하는 데 사용할 MAC 주소 목록을 지정하려면 글로벌 컨피그레이션 모드에서 **mac-list** 명령을 사용합니다. MAC 목록 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

mac-list *id* {**deny | permit**} *mac macmask*

no mac-list *id* {**deny | permit**} *mac macmask*

구문 설명

deny	이 MAC 주소와 일치하는 트래픽은 MAC 목록에서 확인되지 않으며, **aaa mac-exempt** 명령에 지정된 경우 인증 및 권한 부여 모두의 대상이 된다는 것을 나타냅니다. ffff.ffff.0000과 같은 MAC 주소 마스크를 사용하여 MAC 주소의 범위를 허용하는 경우, 그리고 그 범위의 MAC 주소에 인증과 권한 부여를 적용하려는 경우 MAC 목록에 deny 엔트리를 추가해야 할 수 있습니다.
id	16진수 MAC 액세스 목록 번호를 지정합니다. MAC 주소 집합을 그룹화하려면 동일한 ID 값으로 필요한 만큼 **mac-list** 명령을 입력합니다. 시나리오와는 반대로, 패킷은 일치하는 첫 번째 엔트리를 사용하므로 엔트리의 순서가 중요합니다. permit 엔트리를 가지고 있으며, permit 엔트리에서 허용하는 주소를 거부하고자 하는 경우에는 permit 엔트리 이전에 deny 엔트리를 입력해야 합니다.
mac	12자리 16진수 형식, 즉 nnnn.nnnn.nnnn 형식으로 소스 MAC 주소를 지정합니다.
macmask	매칭에 사용해야 할 MAC 주소의 부분을 지정합니다. 예를 들어 ffff.ffff.ffff는 MAC 주소와 정확히 일치합니다. ffff.ffff.0000은 처음 8자리만 일치합니다.
permit	이 MAC 주소와 일치하는 트래픽은 MAC 목록에서 확인되며, **aaa mac-exempt** 명령에 지정된 경우 인증 및 권한 부여 모두의 대상에서 제외된다는 것을 나타냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

MAC 주소가 인증 및 권한 부여에서 제외되도록 설정하려면 **aaa mac-exempt** 명령을 사용합니다. **aaa mac-exempt** 명령의 인스턴스를 하나만 추가할 수 있으므로 MAC 목록에 제외하고자 하는 모든 MAC 주소를 포함해야 합니다. MAC 목록을 여러 개 만들 수 있지만 한 번에 하나만 사용할 수 있습니다.

예

다음 예는 단일 MAC 주소에 대한 인증을 우회합니다.

```
ciscoasa(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# aaa mac-exempt match abc
```

다음 엔트리는 하드웨어 ID가 0003.E3인 모든 Cisco IP Phone에 대한 인증을 우회합니다.

```
ciscoasa(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
ciscoasa(config)# aaa mac-exempt match acd
```

다음 예는 MAC 주소 그룹에 대한 인증을 우회합니다(00a0.c95d.02b2 제외). 00a0.c95d.02b2는 permit 문도 확인하며 이것이 첫 번째인 경우 deny 문은 확인조차 하지 않기 때문에, permit 문 앞에 deny 문을 입력해야 합니다.

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(config)# aaa mac-exempt match 1
```

관련 명령

명령	설명
aaa authentication	사용자 인증을 활성화합니다.
aaa authorization	사용자 인증 서비스를 활성화합니다.
aaa mac-exempt	인증 및 권한 부여에서 MAC 주소 목록을 제외합니다.
clear configure mac-list	전에 **mac-list** 명령으로 지정한 MAC 주소 목록을 제거합니다.
show running-config mac-list	전에 **mac-list** 명령으로 지정한 MAC 주소 목록을 표시합니다.

mail-relay

로컬 도메인 이름을 구성하려면 매개변수 컨피그레이션 모드에서 **mail-relay** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

mail-relay *domain_name* **action** {**drop-connection** | **log**}

no mail-relay *domain_name* **action** {**drop-connection** | **log**}

구문 설명

domain_name	도메인 이름을 지정합니다.
drop-connection	연결을 닫습니다.
log	시스템 로그 메시지를 생성합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 특정 도메인에 대해 메일 릴레이를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mail-relay mail action drop-connection
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

management-access

VPN 사용 시 ASA에 들어간 인터페이스 이외의 인터페이스에 대한 관리 액세스를 허용하려면 글로벌 컨피그레이션 모드에서 **management-access** 명령을 사용합니다. 관리 액세스를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

management-access *mgmt_if*

no management-access *mgmt_if*

구문 설명

mgmt_if	다른 인터페이스에서 ASA에 들어갈 때 액세스하려는 관리 인터페이스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 풀 터널 IPsec VPN이나 SSL VPN 클라이언트(AnyConnect 2.x 클라이언트, SVC 1.x) 사용 시 또는 Site-to-Site IPsec 터널 전체에서 ASA에 들어간 인터페이스 이외의 다른 인터페이스에 연결할 수 있습니다. ASA 인터페이스에 연결하려면 텔넷, SSH, Ping 또는 ASDM을 사용할 수 있습니다.

관리 액세스 인터페이스를 하나만 정의할 수 있습니다.

참고 관리 액세스 인터페이스 네트워크와 VPN 네트워크(VPN 트래픽용 일반 NAT 컨피그레이션) 간에 아이덴티티 NAT를 사용하려면 **nat** 명령과 **route-lookup** 키워드를 지정해야 합니다. 경로 조회가 없으면 ASA는 라우팅 테이블의 내용과 상관없이 **nat** 명령으로 지정한 인터페이스 외부로 트래픽을 전송합니다. 예를 들어 외부에서 들어오는 VPN 사용자가 내부 인터페이스를 관리할 수 있도록 하려면 **management-access inside**를 구성합니다. 아이덴티티 **nat** 명령으로 **(inside,outside)**를 지정하고 ASA에서 관리 트래픽을 내부 네트워크로 전송하지 못하게 하는 경우, 해당 트래픽은 내부 IP 주소로 돌아올 수 없습니다. 경로 조회 옵션을 사용하면 ASA는 트래픽을 내부 네트워크가 아니라 내부 인터페이스 IP 주소로 직접 전송합니다. VPN 클라이언트에서 내부 네트워크의 호스트로 이동하는 트래픽의 경우 경로 조회 옵션을 사용해도 여전히 올바른 이그레스 인터페이스(내부)로 이동하므로, 정상적인 트래픽 흐름에는 영향이 미치지 않습니다.

예

다음 예는 "inside"라는 이름의 방화벽 인터페이스를 관리 액세스 인터페이스로 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# management-access inside
ciscoasa(config)# show running-config management-access
management-access inside
```

관련 명령

명령	설명
clear configure management-access	ASA의 관리 액세스에 대한 내부 인터페이스의 컨피그레이션을 제거합니다.
show management-access	관리 액세스용으로 구성된 내부 인터페이스의 이름을 표시합니다.

management-only

관리 트래픽만 허용하도록 인터페이스를 설정하려면 인터페이스 컨피그레이션 모드에서 **management-only** 명령을 사용합니다. 통과 트래픽을 허용하려면 이 명령의 **no** 형식을 사용합니다.

management-only

no management-only

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

Management *n*/*n* 인터페이스(모델에서 사용 가능한 경우)는 기본적으로 관리 전용 모드로 설정됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	실행 중인 컨피그레이션에서 ASA 클러스터링을 지원하도록 이 명령의 위치가 인터페이스 섹션의 상단으로 이동했습니다. 여기에는 관리 인터페이스에 대한 특별 예외 사항이 있습니다.

사용 지침

일부 모델에는 ASA에 대한 트래픽을 지원하도록 Management *n*/*n*이라는 전용 관리 인터페이스가 포함되어 있습니다. 그러나 **management-only** 명령을 사용하면 어떤 인터페이스든 관리 전용 인터페이스가 되도록 구성할 수 있습니다. 또한 Management *n*/*n*의 경우, 인터페이스가 다른 인터페이스처럼 통과 트래픽을 전달할 수 있도록 관리 전용 모드를 비활성화할 수 있습니다.

참고 ASA 5512-X~ASA 5555-X의 경우, Management 인터페이스에 대해 관리 전용 모드를 비활성화할 수 없습니다. 기본적으로 이 명령은 항상 활성화되어 있습니다.

투명 방화벽 모드에서는 최대 허용되는 통과 트래픽 인터페이스 외에도, 관리 인터페이스(물리적 인터페이스 또는 하위 인터페이스(모델에서 지원되는 경우) 또는 여러 개의 관리 인터페이스로 구성된 EtherChannel 인터페이스(관리 인터페이스가 여러 개인 경우))를 별도의 관리 인터페이스로 사용할 수 있습니다. 다른 기타 인터페이스 유형은 관리 인터페이스로 사용할 수 없습니다.

사용하는 모델에 관리 인터페이스가 없을 경우 데이터 인터페이스에서 투명 방화벽 모드를 관리해야 합니다.

다중 컨텍스트 모드에서는 관리 인터페이스를 비롯하여 어떤 인터페이스도 여러 컨텍스트에서 공유할 수 없습니다. 컨텍스트별 관리를 위해 관리 인터페이스의 하위 인터페이스를 만들고 각 컨텍스트에 관리 하위 인터페이스를 할당할 수 있습니다. ASA 5512-X~ASA 5555-X에서는 관리 인터페이스에서 하위 인터페이스를 지원하지 않습니다. 따라서 컨텍스트별 관리를 위해서는 데이터 인터페이스에 연결해야 합니다.

관리 인터페이스는 일반적인 브릿지 그룹에 포함되지 않습니다. 운영상의 용도로 인해 관리 인터페이스는 구성 불가능한 브릿지 그룹에 포함됩니다.

예

다음 예는 Management 인터페이스에서 관리 전용 모드를 비활성화합니다.

```
ciscoasa(config)# interface management0/0
ciscoasa(config-if)# no management-only
```

다음 예는 하위 인터페이스에서 관리 전용 모드를 활성화합니다.

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# management-only
```

관련 명령

명령	설명
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어갑니다.

map-name

사용자 정의 특성 이름을 Cisco 특성 이름에 매핑하려면 ldap-attribute-map 컨피그레이션 모드에서 **map-name** 명령을 사용합니다.

이 매핑을 제거하려면 이 명령의 **no** 형식을 사용합니다.

map-name *user-attribute-name Cisco-attribute-name*

no map-name *user-attribute-name Cisco-attribute-name*

구문 설명

user-attribute-name	Cisco 특성에 매핑하려는 사용자 정의 특성 이름을 지정합니다.
Cisco-attribute-name	사용자 정의 이름에 매핑하려는 Cisco 특성 이름을 지정합니다.

기본값

기본적으로 이름 매핑이 존재하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
ldap-attribute-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

map-name 명령을 사용하면 고유한 특성 이름을 Cisco 특성 이름에 매핑할 수 있습니다. 그런 다음 결과 특성 맵을 LDAP 서버에 바인딩할 수 있습니다. 일반적인 단계는 다음과 같습니다.

1. 글로벌 컨피그레이션 모드에서 **ldap attribute-map** 명령을 사용하여 채워지지 않은 특성 맵을 생성합니다. 이 명령을 실행하면 ldap-attribute-map 컨피그레이션 모드로 들어갑니다.
2. ldap-attribute-map 컨피그레이션 모드에서 **map-name** 및 **map-value** 명령을 사용하여 특성 맵을 채웁니다.
3. aaa-server host 모드에서 **ldap-attribute-map** 명령을 사용하여 특성 맵을 LDAP 서버에 바인딩합니다. 이 명령에서 "ldap" 뒤에 하이픈이 있음에 유의하십시오.

참고 특성 매핑 기능을 올바르게 사용하려면 Cisco LDAP 특성의 이름 및 값 그리고 사용자 정의 특성의 이름 및 값을 모두 알고 있어야 합니다.

예

다음의 명령 예에서는 LDAP 특성 맵 myldapmap에서 사용자 정의 특성 이름 Hours를 Cisco 특성 이름 cVPN3000-Access-Hours에 매핑합니다.

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
ciscoasa(config-ldap-attribute-map)#
```

ldap-attribute-map 컨피그레이션 모드 내에서 "?"를 입력하면 Cisco LDAP 특성 이름의 전체 목록을 표시할 수 있습니다.

```
ciscoasa(config-ldap-attribute-map)# map-name <name>
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
    :
    :
  cVPN3000-X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

관련 명령

명령	설명
ldap attribute-map(글로벌 컨피그레이션 모드)	사용자 정의 특성 이름을 Cisco LDAP 특성 이름에 매핑하기 위한 LDAP 특성 맵을 생성하고 이름을 지정합니다.
ldap-attribute-map(aaa-server host 모드)	LDAP 특성 맵을 LDAP 서버에 바인딩합니다.
map-value	사용자 정의 특성 값을 Cisco 특성에 매핑합니다.
show running-config ldap attribute-map	실행 중인 특정 LDAP 특성 맵 또는 실행 중인 모든 특성 맵을 표시합니다.
clear configure ldap attribute-map	모든 LDAP 특성 맵을 제거합니다.

map-value

사용자 정의 값을 Cisco LDAP 값에 매핑하려면 ldap-attribute-map 컨피그레이션 모드에서 **map-value** 명령을 사용합니다. 맵 내 엔트리를 삭제하려면 이 명령의 **no** 형식을 사용합니다.

map-value *user-attribute-name user-value-string Cisco-value-string*

no map-value *user-attribute-name user-value-string Cisco-value-string*

구문 설명

Cisco-value-string	Cisco 특성에 대한 Cisco 값 문자열을 지정합니다.
user-attribute-name	Cisco 특성 이름에 매핑하려는 사용자 정의 특성 이름을 지정합니다.
user-value-string	Cisco 특성 값에 매핑하려는 사용자 정의 값 문자열을 지정합니다.

기본값

기본적으로 Cisco 특성에 매핑되는 사용자 정의 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
ldap-attribute-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

map-value 명령을 사용하면 고유한 특성 값을 Cisco 특성 이름 및 값에 매핑할 수 있습니다. 그런 다음 결과 특성 맵을 LDAP 서버에 바인딩할 수 있습니다. 일반적인 단계는 다음과 같습니다.

1. 글로벌 컨피그레이션 모드에서 **ldap attribute-map** 명령을 사용하여 채워지지 않은 특성 맵을 생성합니다. 이 명령을 실행하면 ldap-attribute-map 컨피그레이션 모드로 들어갑니다.
2. ldap-attribute-map 컨피그레이션 모드에서 **map-name** 및 **map-value** 명령을 사용하여 특성 맵을 채웁니다.
3. aaa-server host 모드에서 **ldap-attribute-map** 명령을 사용하여 특성 맵을 LDAP 서버에 바인딩합니다. 이 명령에서 "ldap" 뒤에 하이픈이 있음에 유의하십시오.

참고 특성 매핑 기능을 올바르게 사용하려면 Cisco LDAP 특성의 이름 및 값 그리고 사용자 정의 특성의 이름 및 값을 모두 알고 있어야 합니다.

예

다음 예에서는 ldap-attribute-map 컨피그레이션 모드로 들어가고, 사용자 특성 Hours의 사용자 정의 값을 workDay라는 사용자 정의 시간 정책 및 Daytime이라는 Cisco 정의 시간 정책으로 설정합니다.

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-value Hours workDay Daytime
ciscoasa(config-ldap-attribute-map)#
```

관련 명령

명령	설명
ldap attribute-map(글로벌 컨피그레이션 모드)	사용자 정의 특성 이름을 Cisco LDAP 특성 이름에 매핑하기 위한 LDAP 특성 맵을 생성하고 이름을 지정합니다.
ldap-attribute-map(aaa-server host 모드)	LDAP 특성 맵을 LDAP 서버에 바인딩합니다.
map-name	Cisco LDAP 특성 이름을 이용해 사용자 정의 LDAP 특성 이름을 매핑합니다.
show running-config ldap attribute-map	실행 중인 특정 LDAP 특성 맵 또는 실행 중인 모든 특성 맵을 표시합니다.
clear configure ldap attribute-map	모든 LDAP 맵을 제거합니다.

mapping-service

Cisco Intercompany Media Engine 프록시에 대한 매핑 서비스를 구성하려면 UC-IME 컨피그레이션 모드에서 **mapping-service** 명령을 사용합니다. 프록시에서 매핑 서비스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

no mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

구문 설명

interface	listening 인터페이스 또는 uc-ime 인터페이스에 사용할 인터페이스의 이름을 지정합니다.
listening-interface	ASA가 매핑 요청을 수신 대기할 인터페이스를 구성합니다.
listening-port	(선택 사항) 매핑 서비스를 위한 수신 대기 포트를 구성합니다.
port	(선택 사항) ASA가 매핑 요청을 수신 대기할 TCP 포트 번호를 구성합니다. 디바이스에서 다른 서비스(예: 텔넷 또는 SSH)와의 충돌을 피하려면 포트 번호가 1024 이상이어야 합니다. 기본적으로 포트 번호는 TCP 8060입니다.
uc-ime-interface	원격 Cisco UCM에 연결되는 인터페이스를 구성합니다.

기본값

기본적으로 Cisco Intercompany Media Engine 프록시의 off-path 구축을 위한 매핑 서비스는 TCP 포트 8060에서 수신 대기합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
UC-IME 구성	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

ASA에서 Cisco Intercompany Media Engine 프록시의 off-path 구축을 수행하려면 프록시 컨피그레이션에 매핑 서비스를 추가합니다. 매핑 서비스를 구성하려면 매핑 요청을 수신 대기할 외부 인터페이스(원격 엔터프라이즈 측) 및 원격 Cisco UCM에 연결할 인터페이스를 지정해야 합니다.

참고 Cisco Intercompany Media Engine 프록시에 대해서는 매핑 서버를 하나만 구성할 수 있습니다.

Off-path 구축을 위해 Cisco Intercompany Media Engine 프록시를 구성할 때 매핑 서비스를 구성합니다.

Off-path 구축 시 인바운드 및 아웃바운드 Cisco Intercompany Media Engine 호출은 Cisco Intercompany Media Engine 프록시로 활성화된 Adaptive Security Appliance를 통과합니다. Adaptive Security Appliance는 DMZ에 배치되며 주로 Cisco Intercompany Media Engine을 지원하도록 구성됩니다. 일반적인 인터넷 대면 트래픽은 이 ASA를 통과하지 못합니다.

모든 인바운드 호출에 대해 ASA로 신호가 전송되는데, 이는 지정된 Cisco UCM이 ASA에서 전역 IP 주소로 구성되기 때문입니다. 아웃바운드 호출의 경우 수신자는 인터넷의 특정 IP 주소일 수 있습니다. 따라서 ASA는 매핑 서비스로 구성됩니다. 매핑 서비스는 인터넷에서 수신자의 각 전역 IP 주소에 대해 ASA의 내부 IP 주소를 동적으로 제공합니다.

Cisco UCM은 모든 아웃바운드 호출을 인터넷에서 수신자의 전역 IP 주소 대신 Adaptive Security Appliance의 매핑된 내부 IP 주소에 직접 전송합니다. 그런 다음 ASA는 수신자의 전역 IP 주소로 호출을 전달합니다.

예

다음 예를 참조하십시오.

```
ciscoasa(config)# uc-ime offpath_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
ciscoasa(config-uc-ime)# mapping-service listening-interface inside listening-port 8060
uc-ime-interface outside
```

관련 명령

명령	설명
show running-config uc-ime	Cisco Intercompany Media Engine 프록시의 실행 중인 컨피그레이션을 보여줍니다.
show uc-ime	Fallback 알림, mapping-service 세션 및 signaling 세션에 대한 통계 정보 또는 자세한 정보를 표시합니다.
uc-ime	ASA에서 Cisco Intercompany Media Engine 프록시 인스턴스를 생성합니다.

mask

Modular Policy Framework 사용 시, 일치 또는 클래스 컨피그레이션 모드에서 **mask** 명령을 사용하여 **match** 명령 또는 클래스 맵과 일치하는 패킷의 일부를 마스크 처리합니다. 이 마스크 작업은 검사 정책 맵에서 애플리케이션 트래픽에 대해 사용 가능하지만(**policy-map type inspect** 명령), 모든 애플리케이션에서 이 작업을 허용하는 것은 아닙니다. 예를 들면 DNS 애플리케이션 검사용 **mask** 명령을 사용하여, 트래픽이 ASA를 통과하도록 허용하기 전에 헤더 플래그를 마스크 처리할 수 있습니다. 이 작업을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

mask [**log**]

no mask [**log**]

구문 설명

log	일치를 기록합니다. 시스템 로그 메시지 번호는 애플리케이션에 따라 다릅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
일치 및 클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

검사 정책 맵은 **match** 및 **class** 명령으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 명령은 애플리케이션에 따라 다릅니다. **match** 또는 **class** 명령을 입력하여 애플리케이션 트래픽을 식별한 후(**class** 명령은 기존의 **class-map type inspect** 명령을 참조하며, 여기에 **match** 명령이 포함됨), **mask** 명령을 입력하여 **match** 명령 또는 **class** 명령과 일치하는 패킷의 일부를 마스크 처리할 수 있습니다.

Layer 3/4 정책 맵에서(**policy-map** 명령) **inspect** 명령을 사용하여 애플리케이션 검사를 활성화할 경우 이 작업을 포함하는 검사 정책 맵을 활성화할 수 있습니다. 예를 들어 **inspect dns dns_policy_map** 명령(dns_policy_map은 검사 정책 맵의 이름)을 입력할 수 있습니다.

예

다음 예는 트래픽이 ASA를 통과하도록 허용하기 전 DNS 헤더에서 RD 및 RA 플래그를 마스크 처리합니다.

```
ciscoasa(config-cmap)# policy-map type inspect dns dns-map1
ciscoasa(config-pmap-c)# match header-flag RD
ciscoasa(config-pmap-c)# mask log
ciscoasa(config-pmap-c)# match header-flag RA
ciscoasa(config-pmap-c)# mask log
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
policy-map type inspect	애플리케이션 검사를 위한 특수 작업을 정의합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

mask-banner

서버 배너를 애매하게 처리하려면 매개변수 컨피그레이션 모드에서 **mask-banner** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

mask-banner

no mask-banner

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 서버 배너를 마스크 처리하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

mask-syst-reply

클라이언트에서 FTP 서버 응답을 숨기려면 **ftp-map** 명령을 사용하여 액세스할 수 있는 FTP 맵 컨피그레이션 모드에서 **mask-syst-reply** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

mask-syst-reply

no mask-syst-reply

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
FTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

FTP 서버 시스템을 클라이언트로부터 보호하려면 엄격한 FTP 검사와 함께 mask-syst-reply 명령을 사용합니다. 이 명령을 활성화하면 **syst** 명령에 대한 서버 응답이 일련의 X로 교체됩니다.

예

다음 명령을 실행하면 ASA는 syst 명령에 대한 FTP 서버 응답을 X로 교체합니다.

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# mask-syst-reply
ciscoasa(config-ftp-map)#
```

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
ftp-map	FTP 맵을 정의하고 FTP 맵 컨피그레이션 모드를 활성화합니다.
inspect ftp	애플리케이션 검사에 사용할 특정 FTP 맵을 적용합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
request-command deny	허용하지 않을 FTP 명령을 지정합니다.

match access-list

Modular Policy Framework 사용 시, 액세스 목록을 사용하여 작업을 적용할 트래픽을 식별하려면 클래스 맵 컨피그레이션 모드에서 **match access-list** 명령을 사용합니다. **match access-list** 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match access-list *access_list_name*

no match access-list *access_list_name*

구문 설명

access_list_name	일치 기준으로 사용할 액세스 목록의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Modular Policy Framework의 구성은 네 작업으로 구성됩니다.

1. **class-map** 명령을 사용하여 작업을 적용할 Layer 3 및 4 트래픽을 식별합니다.

   class-map 명령을 입력한 후 **match access-list** 명령을 입력하여 트래픽을 식별할 수 있습니다. 또는 **match** 명령의 다른 유형(예: **match port** 명령)을 입력할 수도 있습니다. 클래스 맵에는 하나의 **match access-list** 명령만 포함할 수 있으며, 이를 다른 유형의 **match** 명령과 결합할 수 없습니다. 단, ASA에서 검사할 수 있는 모든 애플리케이션에 사용되는 기본 TCP 및 UDP 포트와 일치하는 **match default-inspection-traffic** 명령을 정의하는 경우는 예외입니다. 이 경우 **match access-list** 명령을 사용하여 일치하는 트래픽의 범위를 좁힐 수 있습니다. **match default-inspection-traffic** 명령은 확인할 포트를 지정하므로 액세스 목록의 포트는 모두 무시됩니다.

2. (애플리케이션 검사 전용) **policy-map type inspect** 명령을 사용하여 애플리케이션 검사 트래픽에 대한 특별 작업을 정의합니다.

3. **policy-map** 명령을 사용하여 Layer 3 및 4 트래픽에 작업을 적용합니다.

4. **service-policy** 명령을 사용하여 인터페이스에 대한 작업을 활성화합니다.

예

다음 예는 세 개의 액세스 목록과 일치하는 세 개의 Layer 3/4 클래스 맵을 생성합니다.

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp

ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp

ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match any

Modular Policy Framework 사용 시, 작업을 적용할 모든 트래픽을 확인하려면 클래스 맵 컨피그레이션 모드에서 **match any** 명령을 사용합니다. **match any** 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match any

no match any

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Modular Policy Framework의 구성은 네 작업으로 구성됩니다.

1. **class-map** 명령을 사용하여 작업을 적용할 Layer 3 및 4 트래픽을 식별합니다.

   class-map 명령을 입력한 후 **match any** 명령을 입력하면 모든 트래픽을 식별할 수 있습니다. 또는 **match** 명령의 다른 유형(예: **match port** 명령)을 입력할 수도 있습니다. **match any** 명령은 다른 유형의 **match** 명령과 결합할 수 없습니다.
2. (애플리케이션 검사 전용) **policy-map type inspect** 명령을 사용하여 애플리케이션 검사 트래픽에 대한 특별 작업을 정의합니다.
3. **policy-map** 명령을 사용하여 Layer 3 및 4 트래픽에 작업을 적용합니다.
4. **service-policy** 명령을 사용하여 인터페이스에 대한 작업을 활성화합니다.

예

다음 예는 클래스 맵 및 **match any** 명령을 사용하여 트래픽 클래스를 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match access-list	액세스 목록에 따라 트래픽을 확인합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match apn

GTP 메시지에서 액세스 포인트 이름에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match apn** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] apn regex [*regex_name* | **class** *regex_class_name*]

no match [not] apn regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 GTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. GTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 GTP 검사 클래스 맵에서 액세스 포인트 이름에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match apn class gtp_regex_apn
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match as-path

BGP 자동 시스템 경로 액세스 목록을 확인하려면 경로 맵 컨피그레이션 모드에서 **match as-path** 명령을 사용합니다. 경로 목록 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match as-path *path-list-number*

no match as-path *path-list-number*

구문 설명

path-list-number	자동 시스템 경로 액세스 목록 번호

기본값

경로 목록이 정의되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
경로 맵 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

match as-path 및 **set weight** 명령으로 설정된 값은 전역 값을 재지정합니다. 예를 들어, **match as-path** 및 **set weight** 경로 맵 컨피그레이션 명령으로 할당된 가중치는 **neighbor weight** 명령으로 할당된 가중치를 재지정합니다.

경로 맵은 여러 부분으로 구성될 수 있습니다. **route-map** 명령과 관련된 **match** 구문과 하나 이상 일치하지 않는 경로는 무시됩니다. 즉, 경로가 아웃바운드 경로 맵에 대해 광고되지 않으며 인바운드 경로 맵에 대해 허용되지 않습니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 일치를 지정해야 합니다. 둘 이상의 path-list-name이 허용됩니다.

예

다음 예는 BGP 자동 시스템 경로 액세스 목록 as-path-acl과 일치하도록 자동 시스템 경로를 설정합니다.

```
ciscoasa(config)# route-map IGP2BGP
ciscoasa(config-route-map)# match as-path 23
```

관련 명령

명령	설명
set-weight	라우팅 테이블에 대한 BGP 가중치를 지정합니다.
neighbor-weight	인접 디바이스 연결에 가중치를 할당합니다.

match body

ESMTP 본문 메시지의 길이 또는 줄 길이에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match body** 명령을 사용합니다. 구성한 섹션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] body [length | line length] gt *bytes*

no match [not] body [length | line length] gt *bytes*

구문 설명

length	ESMTP 본문 메시지의 길이를 지정합니다.
line length	ESMTP 본문 메시지 줄의 길이를 지정합니다.
bytes	일치해야 하는 숫자를 바이트 단위로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 ESMTP 검사 정책 맵에서 본문 줄 길이에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match body line length gt 1000
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match called-party

H.323 수신자에 대한 일치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match called-party** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] called-party [regex *regex***]**

no match [not] match [not] called-party [regex *regex***]**

구문 설명

regex *regex*	정규식을 확인하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 H.323 검사 클래스 맵에서 수신자에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match called-party regex caller1
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match calling-party

H.323 발신자에 대한 일치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match calling-party** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] calling-party [regex *regex***]**

no match [not] match [not] calling-party [regex *regex***]**

구문 설명

regex *regex*	정규식을 확인하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 H.323 검사 클래스 맵에서 발신자에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match calling-party regex caller1
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match certificate

인증서 일치 규칙을 구성하려면 crypto ca trustpoint 컨피그레이션 모드에서 **match certificate** 명령을 사용합니다. 컨피그레이션에서 규칙을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match certificate *map-name* **override ocsp [trustpoint** *trustpoint-name***]** *seq-num* **url** *URL*

no match certificate *map-name* **override ocsp**

구문 설명

map-name	이 규칙에 대해 일치를 확인할 인증서 맵의 이름을 지정합니다. 일치 규칙을 구성하기 전에 인증서 맵을 구성해야 합니다. 최대 길이는 65자입니다.
override ocsp	규칙의 목적이 인증서에서 OCSP URL을 재지정하는 것임을 지정합니다.
seq-num	이 일치 규칙의 우선순위를 설정합니다. 유효한 범위는 1~10000입니다. ASA는 먼저 가장 낮은 시퀀스 번호로 일치 규칙을 평가하고, 그 후에는 일치가 발견될 때까지 순서대로 번호를 평가합니다.
trustpoint	(선택 사항) OCSP responder 인증서 확인을 위해 신뢰 지점을 사용하도록 지정합니다.
trustpoint-name	(선택 사항) Responder 인증서 확인을 위해 override와 함께 사용할 신뢰 지점을 식별합니다.
url	OCSP 폐기 상태의 URL에 액세스하도록 지정합니다.
URL	OCSP 폐기 상태에 액세스하기 위한 URL을 식별합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

PKI 인증서 검증 과정에서 ASA는 보안 유지를 위해 CRL 검사 또는 OCSP(Online Certificate Status Protocol)를 사용하여 인증서 폐기 상태를 확인합니다. CRL 검사에서 ASA는 CRL에 대한 검색, 구문 분석, 캐싱을 수행하며, 그 결과 폐기된 인증서의 전체 목록이 제공됩니다. OCSP는 특정 인증서의 상태를 쿼리하는 VA(validation authority)에서 인증서 상태를 현지화하므로 좀 더 확장 가능한 방식으로 폐기 상태를 검사하게 됩니다.

인증서 일치 규칙을 사용하면 OCSP URL 재지정을 구성할 수 있습니다. 이 경우 원격 사용자 인증서의 AIA 필드에서 URL을 지정하는 것이 아니라 폐기 상태를 검사할 URL을 지정합니다. 또한 일치 규칙을 사용하면 OCSP responder 인증서의 검증에 사용할 신뢰 지점을 구성할 수 있습니다. 이 경우 ASA는 자체 서명 인증서, 클라이언트 인증서의 검증 경로 외부에 있는 인증서를 비롯하여 모든 CA의 responder 인증서를 검증할 수 있습니다.

OCSP 구성 시 다음 요구 사항에 유의하십시오.

- 신뢰 지점 컨피그레이션 내에서 여러 일치 규칙을 구성할 수 있지만, 각 crypto ca certificate map 당 일치 규칙을 하나만 가질 수 있습니다. 그러나 여러 crypto ca certificate map을 구성하여 동일한 신뢰 지점과 연결할 수 있습니다.
- 일치 규칙을 구성하기 전에 인증서 맵을 구성해야 합니다.
- 자체 서명된 OCSP responder 인증서의 검증을 위한 신뢰 지점을 구성하려면, 자체 서명된 responder 인증서를 신뢰할 수 있는 CA 인증서로 간주하면서 해당 신뢰 지점으로 가져옵니다. 그런 다음 클라이언트 인증서를 검증하는 신뢰 지점에서 **match certificate** 명령을 구성하여 responder 인증서의 검증에 자체 서명된 OCSP responder 인증서가 포함된 신뢰 지점을 사용하게 합니다. 클라이언트 인증서의 검증 경로 외부에 있는 responder 인증서를 검증하는 데에도 동일한 절차를 사용합니다.
- 클라이언트 인증서와 responder 인증서가 동일한 CA에서 발급된 것이면 하나의 신뢰 지점에서 둘을 모두 검증할 수 있습니다. 그러나 클라이언트 인증서와 responder 인증서가 서로 다른 CA에서 발급되었으면 각 인증서에 대해 하나씩 두 개의 신뢰 지점을 구성해야 합니다.
- 일반적으로 OCSP 서버(responder) 인증서는 OCSP 응답에 서명합니다. ASA에서는 응답을 받은 후 responder 인증서의 확인을 시도합니다. 일반적으로 CA는 손상 가능성을 최소화하기 위해 OCSP responder 인증서의 수명을 비교적 짧게 설정합니다. 또한 CA는 일반적으로 responder 인증서에 ocsp-no-check 확장을 포함하여, 해당 인증서에는 폐기 상태 검사가 필요하지 않음을 나타냅니다. 그러나 이 확장이 없을 경우 ASA에서는 신뢰 지점에 지정된 방식을 사용하여 폐기 상태 검사를 시도합니다. responder 인증서가 확인 불가능할 경우 폐기 검사는 실패합니다. 이러한 상황을 방지하려면 responder 인증서의 유효성을 검사하는 신뢰 지점을 구성하는 경우 **revocation-check none** 명령을 사용하고, 클라이언트 인증서를 구성하는 경우 **revocation-check ocsp** 명령을 사용합니다.
- ASA는 일치를 찾지 못하면 **ocsp url** 명령에 지정된 URL을 사용합니다. **ocsp url** 명령을 구성하지 않은 경우 ASA는 원격 사용자 인증서의 AIA 필드를 사용합니다. 인증서에 AIA 확장이 없으면 폐기 상태 검사가 실패합니다.

예

다음 예는 newtrust라는 신뢰 지점에 대한 인증서 일치 규칙을 만드는 방법을 보여줍니다. 규칙에는 맵 이름 mymap, 시퀀스 번호 4, 신뢰 지점 mytrust 및 URL 10.22.184.22가 있습니다.

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
ciscoasa(config-ca-trustpoint)#
```

다음 예는 crypto ca certificate map을 구성한 다음 일치 인증서 규칙을 구성하여, responder 인증서를 검증할 CA 인증서가 포함된 신뢰 지점을 식별합니다. newtrust 신뢰 지점에서 식별된 CA가 OCSP responder 인증서를 발급하지 않은 경우에는 이 인증서가 필요합니다.

1 단계 맵 규칙이 적용되는 클라이언트 인증서를 식별하는 인증서 맵을 구성합니다 . 다음 예에서 인증서 맵의 이름은 mymap 이고 시퀀스 번호는 1 입니다 . CN 특성이 mycert 인 subject-name 을 포함하는 클라이언트 인증서는 mymap 엔트리와 일치합니다 .

```
ciscoasa(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)#
```

2 단계 OCSP responder 인증서 검증에 사용할 CA 인증서를 포함하는 신뢰 지점을 구성합니다 . 자체 서명 인증서의 경우 이 신뢰 지점은 자체 서명 인증서 자체로서 , 가져온 후 로컬에서 신뢰 과정을 거치게 됩니다 . 외부 CA 등록을 통해 이 용도로 인증서를 가져올 수도 있습니다 . 프롬프트가 표시되면 CA 인증서를 붙여 넣습니다 .

```
ciscoasa(config-ca-cert-map)# exit
ciscoasa(config)# crypto ca trustpoint mytrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

3 단계 폐기 확인 방법으로 OCSP 를 사용하여 원래 신뢰 지점인 newtrust 를 구성합니다 . 그런 다음 인증서 맵 mymap, 자체 서명 신뢰 지점 mytrust(2 단계에서 구성) 를 포함하는 일치 규칙을 설정합니다 .

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)# crypto ca trustpoint newtrust
```

```
ciscoasa(config-ca-trustpoint)# revocation-check ocsp
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

클라이언트 인증서 인증에 newtrust 신뢰 지점을 사용하는 연결에서는 클라이언트 인증서가 mymap 인증서 맵에 지정된 특성 규칙과 일치하는지를 확인합니다. 일치하는 경우 ASA는 10.22.184.22에서 OCSP responder에 액세스한 다음, mytrust 신뢰 지점을 사용하여 responder 인증서를 검증합니다.

참고 newtrust 신뢰 지점은 클라이언트 인증서에 대해 OCSP를 통해 폐기 검사를 수행하도록 구성됩니다. 그러나 mytrust 신뢰 지점은 기본 revocation-check 방법(none)으로 구성됩니다. 그 결과 OCSP responder 인증서에 대해 폐기 검사가 수행되지 않습니다.

관련 명령

명령	설명
crypto ca certificate map	crypto ca certificate map을 만듭니다. 글로벌 컨피그레이션 모드에서 이 명령을 사용합니다.
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다. 글로벌 컨피그레이션 모드에서 이 명령을 사용합니다.
ocsp disable-nonce	OCSP 요청의 nonce 확장을 비활성화합니다.
ocsp url	신뢰 지점과 연결된 모든 인증서를 검사하는 데 사용할 OCSP 서버를 지정합니다.
revocation-check	폐기 검사에 사용할 방법 및 시도할 순서를 지정합니다.

match certificate allow expired-certificate

관리자가 만료 검사에서 특정 인증서를 제외하도록 허용하려면 ca-trustpool 컨피그레이션 모드에서 **match certificate allow expired-certificate** 명령을 사용합니다. 특정 인증서의 제외를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match certificate <map> allow expired-certificate

no match certificate <map> allow expired-certificate

구문 설명

allow	만료된 인증서를 허용하도록 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-trustpool 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

trustpool 일치 명령은 인증서 맵 객체를 활용하여 전역 trustpool 정책에 대한 인증서 관련 예외 또는 재지정을 구성합니다. 일치 규칙은 검증되는 인증서를 기준으로 작성됩니다.

관련 명령

명령	설명
match certificate skip revocation check	폐기 검사에서 특정 인증서를 제외합니다.

match certificate skip revocation-check

관리자가 폐기 검사에서 특정 인증서를 제외하도록 허용하려면 ca-trustpool 컨피그레이션 모드에서 **match certificate skip revocation-check** 명령을 사용합니다. 폐기 검사 제외를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match certificate map skip revocation-check

no match certificate map skip revocation-check

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-trustpool 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

trustpool 일치 명령은 인증서 맵 객체를 활용하여 전역 trustpool 정책에 대한 인증서 관련 예외 또는 재지정을 구성합니다. 일치 규칙은 검증되는 인증서를 기준으로 작성됩니다.

예

다음 예는 Subject DN 일반 이름 "mycompany123"의 인증서에 대해 유효성 검사를 건너뛰는 방법을 보여줍니다.

```
crypto ca certificate map mycompany 1
subject-name attr cn eq mycompany123
crypto ca trustpool policy
match certificate mycompany skip revocation-check
```

관련 명령

명령	설명
match certificate allow expired-certificate	만료 검사에서 특정 인증서를 제외합니다.

match cmd

ESMTP 명령 동사에 대한 일치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match cmd** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] cmd [verb *verb* **| line length gt** *bytes* **| RCPT count gt** *recipients_number*]

no match [not] cmd [verb *verb* **| line length gt** *bytes* **| RCPT count gt** *recipients_number*]

구문 설명

verb *verb*	ESMTP 명령 동사를 지정합니다.
line length gt *bytes*	줄의 길이를 지정합니다.
RCPT count gt *recipients_number*	수신자 이메일 주소의 수를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 ESMTP 트랜잭션에서 교환되는 verb(method) NOOP에 대한 ESMTP 검사 정책 맵에서 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-pmap)# match cmd verb NOOP
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match community

BGP(Border Gateway Protocol) 커뮤니티의 일치를 확인하려면 경로 맵 컨피그레이션 모드에서 **match community** 명령을 사용합니다. 컨피그레이션 파일에서 **match community** 명령을 제거하고, 소프트웨어가 BGP 커뮤니티 목록 엔트리를 제거하는 기본 상태로 시스템을 복원하려면 이 명령의 **no** 형식을 사용합니다.

match community {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact]}**

no match community {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact]}**

구문 설명

standard-list-number	하나 이상의 허용 또는 거부 커뮤니티 그룹을 식별하는 1~99의 표준 커뮤니티 목록 번호를 지정합니다.
expanded-list-number	하나 이상의 허용 또는 거부 커뮤니티 그룹을 식별하는 100~500의 확장 커뮤니티 목록 번호를 지정합니다.
community-list-name	커뮤니티 목록 이름.
exact	(선택 사항) 정확한 일치가 필요함을 나타냅니다. 모든 커뮤니티와 지정된 커뮤니티가 모두 있어야 합니다.

기본값

경로 맵으로 확인하는 커뮤니티 목록이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
경로 맵 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

경로 맵은 여러 부분으로 구성될 수 있습니다. **route-map** 명령과 관련된 **match** 명령과 하나 이상 일치하지 않는 경로는 무시됩니다. 즉, 경로가 아웃바운드 경로 맵에 대해 광고되지 않으며 인바운드 경로 맵에 대해 허용되지 않습니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 일치를 지정해야 합니다.

커뮤니티 목록 번호 기반의 매칭은 BGP에 해당되는 **match** 명령의 유형 중 하나입니다.

예

다음 예는 경로 매칭 커뮤니티 목록 1의 가중치를 100으로 설정하는 방법을 보여줍니다. 커뮤니티 109가 있는 경로는 가중치가 100으로 설정됩니다.

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)#  match community 1
ciscoasa(config-route-map)# set weight 100
```

다음 예는 경로 매칭 커뮤니티 목록 1의 가중치를 200으로 설정하는 방법을 보여줍니다. 커뮤니티 109만 있는 경로는 가중치가 200으로 설정됩니다.

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community 1 exact
ciscoasa(config-route-map)# set weight 200
```

다음 예는 커뮤니티 목록 LIST_NAME과 일치하는 경로의 가중치를 100으로 설정하는 방법을 보여줍니다. 커뮤니티 101만 있는 경로는 가중치가 100으로 설정됩니다.

```
ciscoasa(config)#  community-list LIST_NAME permit 101
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community LIST_NAME
ciscoasa(config-route-map)# set weight 100
```

다음 예는 확장 커뮤니티 목록 500과 일치하는 경로를 보여줍니다. 확장 커뮤니티 1이 있는 경로는 가중치가 150으로 설정됩니다.

```
ciscoasa(config)#  community-list 500 permit [0-9]*
ciscoasa(config)# route-map MAP_NAME permit 10
ciscoasa(config-route-map)# match extcommunity 500
ciscoasa(config-route-map)# set weight 150
```

관련 명령

명령	설명
set-weight	라우팅 테이블에 대한 BGP 가중치를 지정합니다.
community-list	BGP 커뮤니티 목록을 만들거나 구성합니다.

match default-inspection-traffic

클래스 맵의 검사 명령에 대한 기본 트래픽을 지정하려면 클래스 맵 컨피그레이션 모드에서 **match default-inspection-traffic** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match default-inspection-traffic

no match default-inspection-traffic

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

각 검사의 기본 트래픽에 대한 사용 지침 섹션을 참조하십시오.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

클래스 맵용 트래픽 클래스에 포함된 트래픽을 식별하는 데 **match** 명령이 사용됩니다. 이러한 명령에는 클래스 맵에 포함된 트래픽을 정의하는 다른 기준이 포함되어 있습니다. Modular Policy Framework를 사용하여 보안 기능을 구성하는 과정에서 **class-map** 글로벌 컨피그레이션 명령을 사용하여 트래픽 클래스를 정의할 수 있습니다. 클래스 맵 컨피그레이션 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다.

인터페이스에 트래픽 클래스를 적용하면, 해당 인터페이스에서 수신하는 패킷을 클래스 맵의 **match** 명령문으로 정의한 기준과 비교하게 됩니다. 지정된 기준과 일치하는 패킷은 트래픽 클래스에 포함되고, 해당 트래픽 클래스와 관련된 작업을 따르게 됩니다. 어떤 트래픽 클래스의 기준과도 일치하지 않는 패킷은 기본 트래픽 클래스에 할당됩니다.

match default-inspection-traffic 명령을 사용하면 개별 **inspect** 명령에 대한 기본 트래픽을 확인할 수 있습니다. **match default-inspection-traffic** 명령은 다른 match 명령 중 하나와 함께 사용할 수 있으며, 그러한 명령은 일반적으로 **permit ip** *src-ip dst-ip* 형식의 access-list입니다.

두 번째 **match** 명령을 **match default-inspection-traffic** 명령과 결합하는 규칙은, **match default-inspection-traffic** 명령을 사용하여 프로토콜과 포트 정보를 지정하고 두 번째 **match** 명령을 사용하여 IP 주소 등 나머지 정보를 모두 지정하는 것입니다. 두 번째 **match** 명령으로 지정된 프로토콜 또는 포트 정보는 **inspect** 명령에 대해 무시됩니다.

예를 들어 다음 예에서 지정된 포트 65535는 무시됩니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# match port 65535
```

기본 검사용 트래픽은 다음과 같습니다.

검사 유형	프로토콜 유형	소스 포트	목적지 포트
ctiqbe	tcp	N/A	1748
dcerpc	tcp	N/A	135
dns	udp	53	53
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
HTTP	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
im	tcp	N/A	1-65539
ipsec-pass-thru	udp	N/A	500
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
rpc	udp	111	111
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sip	tcp,udp	N/A	5060
skinny	tcp	N/A	2000
SMTP	tcp	N/A	25
sqlnet	tcp	N/A	1521
tftp	udp	N/A	69
xdmcp	udp	177	177

예

다음 예는 클래스 맵 및 **match default-inspection-traffic** 명령을 사용하여 트래픽 클래스를 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)#
```

관련 명령

명령	설명
class-map	인터페이스에 트래픽 클래스를 적용합니다.
clear configure class-map	모든 트래픽 맵 정의를 제거합니다.
match access-list	클래스 맵 내에서 액세스 목록 트래픽을 식별합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match dns-class

DNS Resource Record 또는 Question 섹션에서 Domain System Class에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match dns-class** 명령을 사용합니다. 구성한 클래스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] dns-class {eq *c_well_known* **|** *c_val*} {**range** *c_val1 c_val2*}

no match [not] dns-class {eq *c_well_known* **|** *c_val*} {**range** *c_val1 c_val2*}

구문 설명

eq	정확한 일치를 지정합니다.
c_well_known	잘 알려진 이름 IN으로 DNS 클래스를 지정합니다.
c_val	DNS 클래스 필드(0-65535)에서 임의의 값을 지정합니다.
range	범위를 지정합니다.
c_val1 c_val2	범위 일치에서 값을 지정합니다. 각 값의 범위는 0~65535입니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

기본적으로 이 명령은 DNS 메시지의 모든 필드(question 및 RR)를 검사하고 지정된 클래스를 확인합니다. DNS 쿼리와 응답을 모두 검사합니다.

match not header-flag QR 및 **match question** 명령을 이용하여 DNS 쿼리의 question 부분으로 일치 범위를 좁힐 수 있습니다.

이 명령은 DNS 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. DNS 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 DNS 검사 정책 맵에서 DNS 클래스에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-class eq IN
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match dns-type

Query 유형 및 RR 유형을 포함하여 DNS 유형에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match dns-type** 명령을 사용합니다. 구성한 dns 유형을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] dns-type {eq *t_well_known* **|** *t_val*} {**range** *t_val1 t_val2*}

no match [not] dns-type {eq *t_well_known* **|** *t_val*} {**range** *t_val1 t_val2*}

구문 설명

eq	정확한 일치를 지정합니다.
t_well_known	잘 알려진 이름(A, NS, CNAME, SOA, TSIG, IXFR 또는 AXFR)으로 DNS 유형을 지정합니다.
t_val	DNS 유형 필드(0-65535)에서 임의의 값을 지정합니다.
range	범위를 지정합니다.
t_val1 t_val2	범위 일치에서 값을 지정합니다. 각 값의 범위는 0~65535입니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

기본적으로 이 명령은 DNS 메시지의 모든 섹션(question 및 RR)을 검사하고 지정된 유형을 확인합니다. DNS 쿼리와 응답을 모두 검사합니다.

match not header-flag QR 및 **match question** 명령을 이용하여 DNS 쿼리의 question 부분으로 일치 범위를 좁힐 수 있습니다.

이 명령은 DNS 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. DNS 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 DNS 검사 정책 맵에서 DNS 유형에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-type eq a
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match domain-name

DNS 메시지 도메인 이름 목록에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match domain-name** 명령을 사용합니다. 구성한 섹션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] domain-name regex *regex_id*

match [not] domain-name regex class *class_id*

no match [not] domain-name regex *regex_id*

no match [not] domain-name regex class *class_id*

구문 설명

regex	정규식을 지정합니다.
regex_id	정규식 ID를 지정합니다.
class	여러 정규식 엔트리를 포함하는 클래스 맵을 지정합니다.
class_id	정규식 클래스 맵 ID를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 미리 정의된 목록에서 DNS 메시지에 있는 도메인 이름의 일치를 확인합니다. 매칭 전에 압축된 도메인 이름이 확장됩니다. 다른 DNS **match** 명령과 함께 사용하여 일치 조건을 특정 필드로 좁힐 수 있습니다.

이 명령은 DNS 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. DNS 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 DNS 검사 정책 맵에서 DNS 도메인 이름을 확인하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match domain-name regex
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match dscp

클래스 맵에서 IETF 정의 DSCP 값(IP 헤더의)을 식별하려면 클래스 맵 컨피그레이션 모드에서 **match dscp** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match dscp {*values*}

no match dscp {*values*}

구문 설명

values	IP 헤더에서 최대 8개의 서로 다른 IETF 정의 DSCP 값을 지정합니다. 범위는 0~63입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

클래스 맵용 트래픽 클래스에 포함된 트래픽을 식별하는 데 **match** 명령이 사용됩니다. 이러한 명령에는 클래스 맵에 포함된 트래픽을 정의하는 다른 기준이 포함되어 있습니다. Modular Policy Framework를 사용하여 보안 기능을 구성하는 과정에서 **class-map** 글로벌 컨피그레이션 명령을 사용하여 트래픽 클래스를 정의할 수 있습니다. 클래스 맵 컨피그레이션 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다.

인터페이스에 트래픽 클래스를 적용하면, 해당 인터페이스에서 수신하는 패킷을 클래스 맵의 **match** 명령문으로 정의한 기준과 비교하게 됩니다. 지정된 기준과 일치하는 패킷은 트래픽 클래스에 포함되고, 해당 트래픽 클래스와 관련된 작업을 따르게 됩니다. 어떤 트래픽 클래스의 기준과도 일치하지 않는 패킷은 기본 트래픽 클래스에 할당됩니다.

match dscp 명령을 사용하면 IP 헤더에서 IETF 정의 DSCP 값을 확인할 수 있습니다.

예

다음 예는 클래스 맵 및 **match dscp** 명령을 사용하여 트래픽 클래스를 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match dscp af43 cs1 ef
ciscoasa(config-cmap)#
```

관련 명령

명령	설명
class-map	인터페이스에 트래픽 클래스를 적용합니다.
clear configure class-map	모든 트래픽 맵 정의를 제거합니다.
match access-list	클래스 맵 내에서 액세스 목록 트래픽을 식별합니다.
match port	해당 인터페이스에서 수신하는 패킷에 대한 비교 기준으로서 TCP/UDP 포트를 지정합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

10 장

match ehlo-reply-parameter부터 match question까지의 명령

match ehlo-reply-parameter

ESMTP ehlo reply parameter에서 매치 조건을 구성하려면 정책 맵 구성 모드에서 **match ehlo-reply-parameter** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] ehlo-reply-parameter *parameter*

no match [not] ehlo-reply-parameter *parameter*

구문 설명

parameter	ehlo reply parameter를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
정책 맵 구성	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 ESMTP 검사 정책 맵에서 ehlo reply parameter에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match ehlo-reply-parameter auth
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match filename

FTP 전송용 파일 이름에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 구성 모드에서 **match filename** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] filename regex [*regex_name* | **class** *regex_class_name*]

no match [not] filename regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 맵 또는 정책 맵 구성	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 FTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. FTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 FTP 검사 클래스 맵에서 FTP 전송 파일 이름에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
/root
ciscoasa(config-cmap)# match username regex class ftp_regex_user
ciscoasa(config-cmap)# match filename regex ftp-file
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match filetype

FTP 전송용 파일 형식에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 구성 모드에서 **match filetype** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] filetype regex [*regex_name* | **class** *regex_class_name*]

no match [not] filetype regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
클래스 맵 또는 정책 맵 구성	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 FTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. FTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 FTP 검사 정책 맵에서 FTP 전송 파일 형식에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-pmap)# match filetype class regex ftp-regex-filetype
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match flow ip destination-address

클래스 맵에서 흐름 IP 수신 주소를 지정하려면 클래스 맵 구성 모드에서 **match flow ip destination-address** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match flow ip destination-address

no match flow ip destination-address

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

클래스 맵용 트래픽 클래스에 포함된 트래픽을 식별하는 데 **match** 명령이 사용됩니다. 이러한 명령에는 클래스 맵에 포함된 트래픽을 정의하는 다른 기준이 포함되어 있습니다. Modular Policy Framework를 사용하여 보안 기능을 구성하는 과정에서 **class-map** 글로벌 컨피그레이션 명령을 사용하여 트래픽 클래스를 정의할 수 있습니다. 클래스 맵 구성 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다.

인터페이스에 트래픽 클래스를 적용하면, 해당 인터페이스에서 수신하는 패킷을 클래스 맵의 **match** 명령문으로 정의한 기준과 비교하게 됩니다. 지정된 기준과 매치하는 패킷은 트래픽 클래스에 포함되고, 해당 트래픽 클래스와 관련된 작업을 따르게 됩니다. 어떤 트래픽 클래스의 기준과도 매치하지 않는 패킷은 기본 트래픽 클래스에 할당됩니다.

터널 그룹에서 흐름 기반 정책 작업을 활성화하려면 **match flow ip destination-address** 및 **match tunnel-group** 명령을 **class-map**, **policy-map**, **service-policy** 명령과 함께 사용합니다. 흐름을 정의하는 기준은 수신 IP 주소입니다. 고유한 IP 수신 주소로 이동하는 모든 트래픽은 흐름으로 간주됩니다. 정책 작업은 전체 트래픽 클래스가 아닌 각 흐름에 적용됩니다. QoS 작업 정책은 **match flow ip destination-address** 명령을 사용해 적용합니다. 터널 그룹 내 각 터널을 특정 속도로 폴리싱하려면 **match tunnel-group** 명령을 사용합니다.

예

다음 예는 터널 그룹 내에서 흐름 기반 폴리싱을 활성화하고 각 터널을 특정 속도로 제한하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

관련 명령

명령	설명
class-map	인터페이스에 트래픽 클래스를 적용합니다.
clear configure class-map	모든 트래픽 맵 정의를 제거합니다.
match access-list	클래스 맵 내에서 액세스 목록 트래픽을 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.
tunnel-group	VPN에 대한 연결별 레코드의 데이터베이스를 만들고 관리합니다.

match header(policy-map type inspect esmtp)

ESMTP 헤더에서 매치 조건을 구성하려면 policy-map type inspect esmtp 구성 모드에서 **match header** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] header [[length | line length] gt *bytes* **| to-fields count gt** *to_fields_number*]

no match [not] header [[length | line length] gt *bytes* **| to-fields count gt** *to_fields_number*]

구문 설명

length gt *bytes*	ESMTP 헤더 메시지의 길이를 매치하도록 지정합니다.
line length gt bytes	ESMTP 헤더 메시지의 줄의 길이를 매치하도록 지정합니다.
to-fields count gt *to_fields_number*	To: 필드의 수를 매치하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Policy-map type inspect esmtp 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 ESMTP 검사 정책 맵에서 헤더에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match header length gt 512
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match header(policy-map type inspect ipv6)

IPv6 헤더에서 매치 조건을 구성하려면 policy-map type inspect ipv6 컨피그레이션 모드에서 **match header** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [**not**] **header** {**ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** {**eq** | **range**} *number*}

no match [**not**] **header** {**ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** {**eq** | **range**} *number*}

구문 설명

ah	IPv6 Authentication 확장 헤더를 매치합니다.
count gt *number*	IPv6 확장 헤더의 최대 수를 지정합니다(0~255).
destination-option	IPv6 destination-option 확장 헤더를 매치합니다.
esp	IPv6 ESP(Encapsulation Security Payload) 확장 헤더를 매치합니다.
fragment	IPv6 fragment 확장 헤더를 매치합니다.
hop-by-hop	IPv6 hop-by-hop 확장 헤더를 매치합니다.
not	(선택 사항) 특정 파라미터를 매치하지 않습니다.
routing-address count gt *number*	IPv6 라우팅 헤더 유형 0 주소의 최대 수를 0~255 범위의 숫자보다 크게 설정합니다.
routing-type {**eq** | **range**} *number*	IPv6 라우팅 헤더 유형을 0~255 범위에서 매치합니다. 범위를 지정할 경우 공백으로 값을 구분합니다(예: **30 40**).

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 상황		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	상황	시스템
Policy-map type inspect ipv6 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

매치할 헤더를 지정합니다. 기본적으로 패킷은 기록됩니다(**log**). 패킷을 삭제하려면(그리고 선택적으로 기록하려면) 매치 구성 모드에서 **drop** 명령 및 선택적인 **log** 명령을 입력합니다.

매치할 각 확장에 대해 **match** 명령 및 선택적인 **drop** 명령을 다시 입력합니다.

예

다음 예는 hop-by-hop, destination-option, routing-address 및 routing type 0 헤더의 모든 IPv6 패킷을 삭제하고 기록할 검사 정책 맵을 만듭니다.

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
 match header routing-type eq 0
  drop log
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match header-flag

DNS 헤더 플래그에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match header-flag** 명령을 사용합니다. 구성한 헤더 플래그를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] header-flag [eq] {*f_well_known* | *f_value*}

no match [not] header-flag [eq] {*f_well_known* | *f_value*}

구문 설명

eq	정확한 매치를 지정합니다. 구성되지 않은 경우 **match-all** 비트 마스크 매치를 지정합니다.
f_well_known	잘 알려진 이름별로 DNS 헤더 플래그 비트를 지정합니다. 다중 플래그 비트를 입력할 수 있으며 논리적 운용 연구(OR)를 수행할 수 있습니다. QR(Query, note: QR=1, indicating a DNS response) AA(Authoritative Answer) TC(TrunCation) RD(Recursion Desired) RA(Recursion Available)
f_value	임의의 16비트 값을 16진수 형식으로 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 DNS 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. DNS 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 DNS 검사 정책 맵에서 DNS 헤더 플래그에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match header-flag AA
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match im-subscriber

SIP IM subscriber에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match im-subscriber** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] im-subscriber regex [*regex_name* | **class** *regex_class_name*]

no match [not] im-subscriber regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 SIP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. SIP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 SIP 검사 클래스 맵에서 SIP IM subscriber에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match im-subscriber regex class im_sender
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match interface

지정된 인터페이스 중에 next-hop이 있는 경로를 배포하려면 경로 맵 컨피그레이션 모드에서 **match interface** 명령을 사용합니다. match interface 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match interface *interface-name*

no match interface *interface-name*

구문 설명

interface-name	인터페이스의 이름입니다(물리적 인터페이스 아님). 여러 인터페이스 이름을 지정할 수 있습니다.

기본값

정의된 매치 인터페이스가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

명령 구문의 생략 기호(...)는 명령 입력에서 interface-type interface-number 인수에 대해 여러 값을 포함할 수 있음을 나타냅니다.

route-map global 구성 명령과 **match** 및 **set** 구성 명령을 통해 한 라우팅 프로토콜에서 다른 프로토콜로 경로 재배포의 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 **match** 및 **set** 명령이 있습니다. **match** 명령은 매치 기준(현재의 **route-map** 명령으로 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 set 작업, 즉 **match** 명령으로 적용된 기준이 충족되는 경우 수행할 특정 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

match route-map 구성 명령에는 여러 형식이 있습니다. **match** 명령은 어떤 순서로든 사용할 수 있습니다. **set** 명령으로 지정한 set 작업에 따라 경로를 재배포하려면 모든 **match** 명령을 "통과"해야 합니다. **match** 명령의 **no** 형식은 지정된 매치 기준을 제거합니다. **match** 명령으로 지정한 인터페이스가 둘 이상인 경우 **no match interface** *interface-name*을 사용하여 단일 인터페이스를 제거할 수 있습니다.

경로 맵은 여러 부분으로 구성될 수 있습니다. **route-map** 명령과 관련된 구문 중 하나라도 매치하지 않는 경로는 무시됩니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 매치를 지정해야 합니다.

예

다음 예는 next-hop이 밖에있는 경로가 배포되는 방법을 보여줍니다.

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match interface outside
```

관련 명령

명령	설명
match ip next-hop	지정된 액세스 목록 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 배포합니다.
match ip route-source	액세스 목록으로 지정한 주소의 라우터 및 액세스 서버에 의해 광고된 경로를 재배포합니다.
match metric	지정된 메트릭을 포함한 경로를 재배포합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

match invalid-recipients

ESMTP 잘못된 수신자 주소에서 매치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match invalid-recipients** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] invalid-recipients count gt *number*

no match [not] invalid-recipients count gt *number*

구문 설명

count gt *number*	잘못된 수신자 수를 매치하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 ESMTP 검사 정책 맵에서 잘못된 수신자 수에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match invalid-recipients count gt 1000
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match ip address

지정된 액세스 목록 중 하나를 통과한 경로 주소 또는 매치 패킷이 있는 경로를 재배포하려면 경로 맵 컨피그레이션 모드에서 **match ip address** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

match ip address {*acl...*} **prefix-list**

no match ip address {*acl...*} **prefix-list**

구문 설명

acl	액세스 목록의 이름을 지정합니다. 여러 액세스 목록을 지정할 수 있습니다.
prefix-list	매치하는 접두부 목록의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

route-map global 구성 명령과 **match** 및 **set** 구성 명령을 통해 한 라우팅 프로토콜에서 다른 프로토콜로 경로 재배포의 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 **match** 및 **set** 명령이 있습니다. **match** 명령은 매치 기준(현재의 **route-map** 명령으로 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 set 작업, 즉 **match** 명령으로 적용된 기준이 충족되는 경우 수행할 특정 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

예

다음 예는 내부 경로를 재배포하는 방법을 보여줍니다.

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에 next hop이 있는 경로를 배포합니다.
match ip next-hop	지정된 액세스 목록 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 배포합니다.
match ipv6 address	지정된 액세스 목록 중 하나를 통과한 IPv6 경로 주소 또는 매치 패킷이 있는 경로를 배포합니다.
match metric	지정된 메트릭을 포함한 경로를 재배포합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

match ipv6 address

지정된 액세스 목록 중 하나를 통과한 IPv6 경로 주소 또는 매치 패킷이 있는 경로를 재배포하려면 경로 맵 컨피그레이션 모드에서 **match ipv6 address** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

match ipv6 address {*acl...*} **prefix-list**

no match ipv6 address {*acl...*} **prefix-list**

구문 설명

acl	액세스 목록의 이름을 지정합니다. 여러 액세스 목록을 지정할 수 있습니다.
prefix-list	매치 접두부 목록의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

route-map global 구성 명령과 **match** 및 **set** 구성 명령을 통해 한 라우팅 프로토콜에서 다른 프로토콜로 경로 재배포의 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 **match** 및 **set** 명령이 있습니다. **match** 명령은 매치 기준(현재의 **route-map** 명령으로 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 set 작업, 즉 **match** 명령으로 적용된 기준이 충족되는 경우 수행할 특정 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

예

다음 예는 내부 경로의 재배포 방법을 보여줍니다. access-list acl_dmz1 extended permit ipv6 any <net> <mask>

```
ciscoasa(config)# access-list acl_dmz1 extended permit ipv6 any <net> <mask>
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에 next-hop이 있는 경로를 배포합니다.
match ip address	지정된 액세스 목록 중 하나를 통과한 경로 주소 또는 매치 패킷이 있는 경로를 배포합니다.
match ip next-hop	지정된 액세스 목록 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 배포합니다.
match metric	지정된 메트릭을 포함한 경로를 재배포합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

match ip next-hop

지정된 액세스 목록 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 재배포하려면 경로 맵 컨피그레이션 모드에서 **match ip next-hop** 명령을 사용합니다. next-hop 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match ip next-hop {*acl*...} | **prefix-list** *prefix_list*

no match ip next-hop {*acl*...} | **prefix-list** *prefix_list*

구문 설명

acl	ACL의 이름입니다. 여러 ACL을 지정할 수 있습니다.
prefix-list *prefix_list*	접두부 목록의 이름입니다.

기본값

next-hop 주소와의 매치 여부와 상관없이 경로를 자유롭게 배포할 수 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

명령 구문의 생략 기호(...)는 명령 입력에서 *acl* 인수에 대해 여러 값을 포함할 수 있음을 나타냅니다.

route-map global 구성 명령과 **match** 및 **set** 구성 명령을 통해 한 라우팅 프로토콜에서 다른 프로토콜로 경로 재배포의 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 **match** 및 **set** 명령이 있습니다. **match** 명령은 매치 기준(현재의 **route-map** 명령으로 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 set 작업, 즉 **match** 명령으로 적용된 기준이 충족되는 경우 수행할 특정 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

match route-map 구성 명령에는 여러 형식이 있습니다. **match** 명령은 어떤 순서로든 입력할 수 있습니다. **set** 명령으로 지정한 set 작업에 따라 경로를 재배포하려면 모든 **match** 명령을 "통과"해야 합니다. **match** 명령의 **no** 형식은 지정된 매치 기준을 제거합니다.

경로 맵을 통해 경로를 통과할 때, 경로 맵은 여러 부분으로 구성될 수 있습니다. **route-map** 명령과 관련된 구문 중 하나라도 매치하지 않는 경로는 무시됩니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 매치를 지정해야 합니다.

예

다음 예는 액세스 목록 acl_dmz1 또는 acl_dmz2를 통과한 next-hop 라우터 주소가 있는 경로를 배포하는 방법을 보여줍니다.

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에 next hop이 있는 경로를 배포합니다.
match ip next-hop	지정된 액세스 목록 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 배포합니다.
match metric	지정된 메트릭을 포함한 경로를 재배포합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

match ip route-source

ACL로 지정한 주소의 라우터 및 액세스 서버에 의해 광고된 경로를 재배포하려면 경로 맵 컨피그레이션 모드에서 **match ip route-source** 명령을 사용합니다. next-hop 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match ip route-source {*acl...*} | **prefix-list** *prefix_list*

no match ip route-source {*acl...*}

구문 설명

acl	ACL의 이름입니다. 여러 ACL을 지정할 수 있습니다.
prefix_list	접두부 목록의 이름입니다.

기본값

경로 소스에 대해 필터링을 수행하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

명령 구문의 생략 기호(...)는 명령 입력에서 access-list-name 인수에 대해 여러 값을 포함할 수 있음을 나타냅니다.

route-map global 구성 명령과 **match** 및 **set** 구성 명령을 통해 한 라우팅 프로토콜에서 다른 프로토콜로 경로 재배포의 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 **match** 및 **set** 명령이 있습니다. **match** 명령은 매치 기준(현재의 **route-map** 명령으로 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 set 작업, 즉 **match** 명령으로 적용된 기준이 충족되는 경우 수행할 특정 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

match route-map 구성 명령에는 여러 형식이 있습니다. **match** 명령은 어떤 순서로든 입력할 수 있습니다. **set** 명령으로 지정한 set 작업에 따라 경로를 재배포하려면 모든 **match** 명령을 "통과"해야 합니다. **match** 명령의 **no** 형식은 지정된 매치 기준을 제거합니다.

경로 맵은 여러 부분으로 구성될 수 있습니다. **route-map** 명령과 관련된 구문 중 하나라도 매치하지 않는 경로는 무시됩니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 매치를 지정해야 합니다. 특정 상황에서는 경로의 next-hop 및 source-router 주소가 동일하지 않습니다.

예

다음 예는 ACL acl_dmz1 및 acl_dmz2로 지정한 주소의 라우터 및 액세스 서버에 의해 광고된 경로를 배포하는 방법을 보여줍니다.

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에 next hop이 있는 경로를 배포합니다.
match ip next-hop	지정된 ACL 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 배포합니다.
match metric	지정된 메트릭을 포함한 경로를 재배포합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

match login-name

인스턴트 메시징의 클라이언트 로그인 이름에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match login-name** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] login-name regex [*regex_name* | **class** *regex_class_name*]

no match [not] login-name regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IM 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. IM 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 인스턴트 메시징 클래스 맵에서 클라이언트 로그인 이름에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match login-name regex login
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match media-type

H.323 미디어 유형에 대한 매치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match media-type** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] media-type [audio | data | video]

no match [not] media-type [audio | data | video]

구문 설명

audio	audio 미디어 유형을 매치하도록 지정합니다.
data	data 미디어 유형을 매치하도록 지정합니다.
video	video 미디어 유형을 매치하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 H.323 검사 클래스 맵에서 audio 미디어 유형에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match media-type audio
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match message id

GTP 메시지 ID에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match message id** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] message id [*message_id* | **range** *lower_range upper_range*]

no match [not] message id [*message_id* | **range** *lower_range upper_range*]

구문 설명

message_id	1~255자 사이의 영숫자 식별자를 지정합니다.
range *lower_range upper_range*	ID의 하한 및 상한을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 GTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. GTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 GTP 검사 클래스 맵에서 메시지 ID에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match message id 33
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match message length

GTP 메시지 ID에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match message length** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] message length min *min_length* **max** *max_length*

no match [not] message length min *min_length* **max** *max_length*

구문 설명

min *min_length*	메시지 ID의 최소 길이를 지정합니다. 값의 범위는 1~65536입니다.
max *max_length*	메시지 ID의 최대 길이를 지정합니다. 값의 범위는 1~65536입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 GTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. GTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 GTP 검사 클래스 맵에서 메시지 길이에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match message length min 8 max 200
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match message-path

Via 헤더 필드에 지정된 대로 SIP 메시지에 사용된 경로에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match message-path** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] message-path regex [*regex_name* | **class** *regex_class_name*]

no match [not] message-path regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 SIP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. SIP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 SIP 검사 클래스 맵에서 SIP 메시지에 사용된 경로에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match message-path regex class sip_message
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match metric

지정된 메트릭으로 경로를 재배포하려면 경로 맵 컨피그레이션 모드에서 **match metric** 명령을 사용합니다. 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match metric *number*

no match metric *number*

구문 설명

number	경로 메트릭은 IGRP five-part 메트릭일 수 있습니다. 유효한 값의 범위는 0~4294967295입니다.

기본값

메트릭 값에 대해 필터링이 수행되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

route-map global 구성 명령과 **match** 및 **set** 구성 명령을 통해 한 라우팅 프로토콜에서 다른 프로토콜로 경로 재배포의 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 **match** 및 **set** 명령이 있습니다. **match** 명령은 매치 기준(현재의 **route-map** 명령으로 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 set 작업, 즉 **match** 명령으로 적용된 기준이 충족되는 경우 수행할 특정 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

match route-map 구성 명령에는 여러 형식이 있습니다. **match** 명령은 어떤 순서로든 사용할 수 있으며, **set** 명령으로 지정한 set 작업에 따라 경로를 재배포하려면 모든 **match** 명령을 "통과"해야 합니다. **match** 명령의 **no** 형식은 지정된 매치 기준을 제거합니다.

경로 맵은 여러 부분으로 구성될 수 있습니다. **route-map** 명령과 관련된 구문 중 하나라도 매치하지 않는 경로는 무시됩니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 매치를 지정해야 합니다.

예

다음 예는 메트릭 5로 경로를 재배포하는 방법을 보여줍니다.

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match metric 5
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에 next hop이 있는 경로를 배포합니다.
match ip next-hop	지정된 액세스 목록 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 배포합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

match mime

ESMTP mime 인코딩 유형, mime 파일 이름 길이 또는 mime 파일 형식에 대한 매치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match mime** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] mime [encoding *type* **| filename length gt** *bytes* **| filetype** *regex***]**

no match [not] mime [encoding *type* **| filename length gt** *bytes* **| filetype** *regex***]**

구문 설명

encoding *type*	인코딩 유형을 매치하도록 지정합니다.
filename length gt *bytes*	파일 이름 길이를 매치하도록 지정합니다.
filetype *regex*	파일 형식을 매치하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 ESMTP 검사 정책 맵에서 mime 파일 이름 길이에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# match mime filename length gt 255
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match peer-ip-address

인스턴트 메시징의 피어 IP 주소에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match peer-ip-address** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] peer-ip-address *ip_address ip_address_mask*

no match [not] peer-ip-address *ip_address ip_address_mask*

구문 설명

ip_address	클라이언트나 서버의 호스트 이름 또는 IP 주소를 지정합니다.
ip_address_mask	클라이언트 또는 서버 IP 주소의 넷마스크를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IM 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. IM 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 인스턴트 메시징 클래스 맵에서 피어 IP 주소에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match peer-login-name

인스턴트 메시징의 피어 로그인 이름에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match peer-login-name** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] peer-login-name regex [*regex_name* | **class** *regex_class_name*]

no match [not] peer-login-name regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IM 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. IM 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 인스턴트 메시징 클래스 맵에서 피어 로그인 이름에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-login-name regex peerlogin
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match port

Modular Policy Framework를 사용할 경우, 클래스 맵 컨피그레이션 모드에서 **match port** 명령을 사용하여 작업을 적용할 TCP 또는 UDP 포트를 매치합니다. **match port** 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

no match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

구문 설명

eq *port*	단일 포트 이름 또는 번호를 지정합니다.
range *beg_port end_port*	시작 및 종료 포트 범위 값을 1에서 65535 사이에서 지정합니다.
tcp	TCP 포트를 지정합니다.
udp	UDP 포트를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Modular Policy Framework의 구성은 다음의 네 작업으로 구성됩니다.

1. **class-map** 또는 **class-map type management** 명령을 사용하여 작업을 적용할 Layer 3 및 4 트래픽을 식별합니다.

   class-map 명령을 입력한 후 **matchport** 명령을 입력하여 트래픽을 식별할 수 있습니다. 아니면 **match** 명령의 다른 유형(예: **match access-list**)을 입력할 수도 있습니다(**class-map type management** 명령은 match port 명령만 허용함). 클래스 맵에는 하나의 **match port** 명령만 포함할 수 있으며, 이를 다른 유형의 **match** 명령과 결합할 수 없습니다.
2. (애플리케이션 검사 전용) **policy-map type inspect** 명령을 사용하여 애플리케이션 검사 트래픽에 대한 특별 작업을 정의합니다.
3. **policy-map** 명령을 사용하여 Layer 3 및 4 트래픽에 작업을 적용합니다.
4. **service-policy** 명령을 사용하여 인터페이스에 대한 작업을 활성화합니다.

예

다음 예는 클래스 맵 및 **match port** 명령을 사용하여 트래픽 클래스를 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 8080
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match access-list	액세스 목록에 따라 트래픽을 매치합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match precedence

클래스 맵에서 우선 적용 값을 지정하려면 클래스 맵 컨피그레이션 모드에서 **match precedence** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match precedence *value*

no match precedence *value*

구문 설명

value	최대 4개의 우선 적용 값을 공백으로 구분하여 지정합니다. 범위는 0~7입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

클래스 맵용 트래픽 클래스에 포함된 트래픽을 식별하는 데 **match** 명령이 사용됩니다. 이러한 명령에는 클래스 맵에 포함된 트래픽을 정의하는 다른 기준이 포함되어 있습니다. Modular Policy Framework를 사용하여 보안 기능을 구성하는 과정에서 **class-map** 글로벌 컨피그레이션 명령을 사용하여 트래픽 클래스를 정의할 수 있습니다. 클래스 맵 구성 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다.

인터페이스에 트래픽 클래스를 적용하면, 해당 인터페이스에서 수신하는 패킷을 클래스 맵의 **match** 명령문으로 정의한 기준과 비교하게 됩니다. 지정된 기준과 매치하는 패킷은 트래픽 클래스에 포함되고, 해당 트래픽 클래스와 관련된 작업을 따르게 됩니다. 어떤 트래픽 클래스의 기준과도 매치하지 않는 패킷은 기본 트래픽 클래스에 할당됩니다.

IP 헤더에서 TOS 바이트로 표시되는 값을 지정하려면 **match precedence** 명령을 사용합니다.

예

다음 예는 클래스 맵 및 **match precedence** 명령을 사용하여 트래픽 클래스를 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match precedence 1
ciscoasa(config-cmap)#
```

관련 명령

명령	설명
class-map	인터페이스에 트래픽 클래스를 적용합니다.
clear configure class-map	모든 트래픽 맵 정의를 제거합니다.
match access-list	클래스 맵 내에서 액세스 목록 트래픽을 식별합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match protocol

MSN이나 Yahoo 등 특정 인스턴트 메시징 프로토콜에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match protocol** 명령을 사용합니다. 매치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] protocol {msn-im | yahoo-im}

no match [not] protocol {msn-im | yahoo-im}

구문 설명

msn-im	MSN 인스턴트 메시징 프로토콜을 매치하도록 지정합니다.
yahoo-im	Yahoo 인스턴트 메시징 프로토콜을 매치하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IM 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. IM 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 인스턴트 메시징 클래스 맵에서 Yahoo 인스턴트 메시징 프로토콜에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match protocol yahoo-im
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

match question

DNS 질문 또는 리소스 레코드에 대한 매치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match question** 명령을 사용합니다. 구성한 섹션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match {question | {resource-record answer | authority | additional}}

no match {question | {resource-record answer | authority | additional}}

구문 설명

question	DNS 메시지의 질문 부분입니다.
resource-record	DNS 메시지의 리소스 레코드 부분입니다.
answer	Answer RR 섹션을 지정합니다.
authority	Authority RR 섹션을 지정합니다.
additional	Additional RR 섹션을 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

기본적으로 이 명령은 DNS 헤더를 검사하고 지정된 필드를 매치합니다. 이 명령을 다른 DNS **match** 명령과 함께 사용하여 특정 질문 또는 RR 유형의 검사를 정의할 수 있습니다.

이 명령은 DNS 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. DNS 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 DNS 검사 정책 맵에서 DNS 질문에 대한 매치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match question
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 구성에 대한 정보를 표시합니다.

11 장

match regex through message-length 명령

match regex

정규식 클래스 맵에서 정규식을 식별하려면 class-map type regex 컨피그레이션 모드에서 **match regex** 명령을 사용합니다. 클래스 맵에서 정규식을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match regex *name*

no match regex *name*

구문 설명

name	**regex** 명령으로 추가한 정규식의 이름입니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Class-map type regex 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(2)	이 명령이 추가되었습니다.

사용 지침

regex 명령은 텍스트 매칭이 필요한 다양한 기능에 대해 사용할 수 있습니다. **class-map type regex** 명령 및 그 뒤에 여러 **match regex** 명령을 사용하여 여러 정규식을 단일 정규식 클래스 맵으로 그룹화할 수 있습니다.

예를 들면 검사 정책 맵을 사용하여 애플리케이션 검사에 대한 특별 작업을 구성할 수 있습니다 (**policy map type inspect** 명령 참조). 검사 정책 맵에서, 하나 이상의 **match** 명령을 포함하는 검사 클래스 맵을 만들어 작업을 수행할 트래픽을 식별할 수 있습니다. 또는 검사 정책 맵에서 **match** 명령을 직접 사용할 수도 있습니다. 일부 **match** 명령을 사용하면 정규식을 사용하여 패킷에서 텍스트를 식별할 수 있습니다. 예를 들어, HTTP 패킷 내부에서 URL 문자열을 확인할 수 있습니다.

예

다음은 HTTP 검사 정책 맵 및 관련 클래스 맵의 예입니다. 이 정책 맵은 서비스 정책에 의해 활성화되는 Layer 3/4 정책 맵에 의해 활성화됩니다.

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2

ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
```

```
ciscoasa(config-cmap)# match not request uri regex class URLs

ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test [a Layer 3/4 class map not shown]
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy test interface outside
```

관련 명령

명령	설명
class-map type regex	정규식 클래스 맵을 만듭니다.
regex	정규식을 추가합니다.
test regex	정규식을 테스트합니다.

match req-resp

HTTP 요청 및 응답에 대한 일치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match req-resp** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] req-resp content-type mismatch

no match [not] req-resp content-type mismatch

구문 설명

content-type	요청의 허용 유형에 대한 응답에서 콘텐츠 유형을 확인하도록 지정합니다.
mismatch	응답의 콘텐츠 유형 필드가 요청의 허용 필드에 있는 mime 유형 중 하나와 반드시 일치하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 다음 확인을 활성화합니다.

- 헤더 content-type의 값이 지원되는 콘텐츠 유형의 내부 목록에 있는지 확인합니다.
- 헤더 content-type이 데이터의 실제 콘텐츠 또는 메시지의 엔티티 본문 부분과 일치하는지 확인합니다.
- HTTP 응답의 콘텐츠 유형 필드가 해당 HTTP 요청 메시지의 **accept** 필드와 일치하는지 확인합니다.

메시지가 위의 검사 중 하나를 통과하지 못하면 ASA는 구성된 작업을 수행합니다.

다음은 지원되는 콘텐츠 유형 목록입니다.

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

이 목록의 일부 content-type에는 해당 정규식(magic number)이 없을 수 있으며, 그에 따라 메시지의 본문 부분이 검증되지 않습니다. 이 경우에는 HTTP 메시지가 허용됩니다.

예

다음 예는 HTTP 정책 맵에서 HTTP 메시지의 콘텐츠 유형을 기반으로 HTTP 트래픽을 제한하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# match req-resp content-type mismatch
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match request-command

특정 FTP 명령을 제한하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match request-command** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] request-command *ftp_command* [*ftp_command*...]

no match [not] request-command *ftp_command* [*ftp_command*...]

구문 설명

ftp_command	제한할 하나 이상의 FTP 명령을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 FTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. FTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 FTP 검사 정책 맵에서 특정 FTP 명령에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect ftp ftp_map1
ciscoasa(config-pmap)# match request-command stou
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match request-method

SIP 메서드 유형에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match request-method** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] request-method *method_type*

no match [not] request-method *method_type*

구문 설명

method_type	RFC 3261 및 지원되는 확장에 따라 메서드 유형을 지정합니다. 지원되는 메서드 유형: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 SIP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. SIP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 SIP 검사 클래스 맵에서 SIP 메시지에 사용된 경로에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match request-method ack
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match request method

HTTP 요청에 대한 일치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match request method** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] request {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

no match [not] request {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

구문 설명

built-in-regex	콘텐츠 유형, 메서드 또는 전송 인코딩에 대한 기본 regex를 지정합니다.
class *class_map name*	regex 유형 클래스 맵의 이름을 지정합니다.
regex *regex_name*	**regex** 명령을 사용하여 구성한 정규식의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

표 11-1 Built-in Regex 값

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify
options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search
setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

예

다음 예는 "GET" 또는 "PUT" 메서드로 "www\.example.com/.*\.asp" Ehsms "www\example[0-9][0-9]\.com"에 액세스를 시도하는 HTTP 연결을 허용하고 기록할 HTTP 검사 정책 맵을 정의하는 방법을 보여줍니다. 다른 모든 URL/메서드 조합은 자동으로 허용됩니다.

```
ciscoasa(config)# regex url1 "www\.example.com/.*\.asp
ciscoasa(config)# regex url2 "www\.example[0-9][0-9]\.com"
ciscoasa(config)# regex get "GET"
ciscoasa(config)# regex put "PUT"
ciscoasa(config)# class-map type regex match-any url_to_log
ciscoasa(config-cmap)# match regex url1
ciscoasa(config-cmap)# match regex url2
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type regex match-any methods_to_log
ciscoasa(config-cmap)# match regex get
ciscoasa(config-cmap)# match regex put
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type inspect http http_url_policy
ciscoasa(config-cmap)# match request uri regex class url_to_log
ciscoasa(config-cmap)# match request method regex class methods_to_log
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect http http_policy
ciscoasa(config-pmap)# class http_url_policy
ciscoasa(config-pmap-c)# log
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match route-type

지정된 유형의 경로를 재배포하려면 경로 맵 컨피그레이션 모드에서 **match route-type** 명령을 사용합니다. 경로 유형 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match route-type {local | internal | {external [type-1 | type-2]} | {nssa-external [type-1 | type-2]}}

no match route-type {local | internal | {external [type-1 | type-2]} | {nssa-external [type-1 | type-2]}}

구문 설명

external	OSPF 외부 경로 또는 EIGRP 외부 경로.
internal	OSPF 내부 영역 경로 또는 EIGRP 내부 경로.
local	로컬에서 생성된 BGP 경로.
nssa-external	외부 NSSA를 지정합니다.
type-1	(선택 사항) 경로 유형 1을 지정합니다.
type-2	(선택 사항) 경로 유형 2를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
경로 맵 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

route-map 글로벌 컨피그레이션 명령과 **match** 및 **set** 컨피그레이션 명령을 사용하면 하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 **match** 및 **set** 명령이 있습니다. **match** 명령은 일치 기준(현재의 **route-map** 명령으로 재배포가 허용되는 조건)을 지정합니다. **set** 명령은 set 작업, 즉 **match** 명령으로 적용된 기준이 충족되는 경우 수행할 특별한 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

match route-map 컨피그레이션 명령에는 여러 형식이 있습니다. **match** 명령은 어떤 순서로든 입력할 수 있습니다. **set** 명령으로 지정한 set 작업에 따라 경로를 재배포하려면 모든 **match** 명령을 "통과"해야 합니다. **match** 명령의 **no** 형식은 지정된 일치 기준을 제거합니다.

경로 맵은 여러 부분으로 구성될 수 있습니다. **route-map** 명령과 관련된 구문 중 하나 이상과 일치하지 않는 경로는 무시됩니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 일치를 지정해야 합니다.

OSPF의 경우, the **external type-1** 키워드는 type 1 외부 경로만을 확인하고 **external type-2** 키워드는 type 2 경로만을 확인합니다.

예

다음 예는 내부 경로를 재배포하는 방법을 보여줍니다.

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match route-type internal
```

관련 명령

명령	설명
match interface	지정된 인터페이스 중 하나에 next hop이 있는 경로를 배포합니다.
match ip next-hop	지정된 액세스 목록 중 하나를 통과한 next-hop 라우터 주소가 있는 경로를 배포합니다.
match metric	지정된 메트릭을 포함한 경로를 재배포합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
set metric	경로 맵의 대상 라우팅 프로토콜에서 메트릭 값을 지정합니다.

match rtp

클래스 맵에서 짝수 포트의 UDP 포트 범위를 지정하려면 클래스 맵 컨피그레이션 모드에서 **match rtp** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match rtp *starting_port range*

no match rtp *starting_port range*

구문 설명

starting_port	짝수 UDP 목적지 포트의 하한을 지정합니다. 범위는 2000~65535입니다.
range	RTP 포트의 범위를 지정합니다. 범위는 0~16383입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

클래스 맵용 트래픽 클래스에 포함된 트래픽을 식별하는 데 **match** 명령이 사용됩니다. 이러한 명령에는 클래스 맵에 포함된 트래픽을 정의하는 다른 기준이 포함되어 있습니다. Modular Policy Framework를 사용하여 보안 기능을 구성하는 과정에서 **class-map** 글로벌 컨피그레이션 명령을 사용하여 트래픽 클래스를 정의할 수 있습니다. 클래스 맵 컨피그레이션 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다.

인터페이스에 트래픽 클래스를 적용하면, 해당 인터페이스에서 수신하는 패킷을 클래스 맵의 **match** 명령문으로 정의한 기준과 비교하게 됩니다. 지정된 기준과 일치하는 패킷은 트래픽 클래스에 포함되고, 해당 트래픽 클래스와 관련된 작업을 따르게 됩니다. 어떤 트래픽 클래스의 기준과도 일치하지 않는 패킷은 기본 트래픽 클래스에 할당됩니다.

match rtp 명령을 사용하여 RTP 포트를 확인합니다(*starting_port* 및 *starting_port* + *range* 사이의 짝수 UDP 포트 번호).

예

다음 예는 클래스 맵 및 **match rtp** 명령을 사용하여 트래픽 클래스를 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match rtp 20000 100
ciscoasa(config-cmap)#
```

관련 명령

명령	설명
class-map	인터페이스에 트래픽 클래스를 적용합니다.
clear configure class-map	모든 트래픽 맵 정의를 제거합니다.
match access-list	클래스 맵 내에서 액세스 목록 트래픽을 식별합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match sender-address

ESMTP 발신자 이메일 주소에서 일치 조건을 구성하려면 정책 맵 컨피그레이션 모드에서 **match sender-address** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

match [not] sender-address [length gt *bytes* **| regex** *regex***]**

no match [not] sender-address [length gt *bytes* **| regex** *regex***]**

구문 설명

length gt *bytes*	발신자 이메일 주소 길이를 확인하도록 지정합니다.
regex *regex*	정규식을 확인하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 ESMTP 검사 정책 맵에서 길이가 320자를 초과하는 발신자 이메일 주소에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-pmap)# match sender-address length gt 320
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match server

FTP 서버에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match server** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] server regex [*regex_name* | **class** *regex_class_name*]

no match [not] server regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 FTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. FTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

ASA는 FTP 서버에 연결될 때 로그인 프롬프트 위에 표시되는 처음 220자 서버 메시지를 기반으로 메시지 이름을 확인합니다. 220자 서버 메시지에 여러 줄이 포함될 수 있습니다. 서버 일치는 DNS를 통해 확인되는 서버 이름의 FQDN을 기반으로 하지 않습니다.

예

다음 예는 FTP 검사 정책 맵에서 FTP 서버에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-pmap)# match server class regex ftp-server
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match service

특정 인스턴트 메시징 서비스에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match service** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] service {chat | file-transfer | games | voice-chat | webcam | conference}

no match [not] service {chat | file-transfer | games | voice-chat | webcam | conference}

구문 설명

chat	인스턴트 메시징 채팅 서비스를 확인하도록 지정합니다.
file-transfer	인스턴트 메시징 파일 전송 서비스를 확인하도록 지정합니다.
games	인스턴트 메시징 게임 서비스를 확인하도록 지정합니다.
voice-chat	인스턴트 메시징 음성 채팅 서비스를 확인하도록 지정합니다.
webcam	인스턴트 메시징 웹캠 서비스를 확인하도록 지정합니다.
conference	인스턴트 메시징 컨퍼런스 서비스를 확인하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IM 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. IM 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 인스턴트 메시징 클래스 맵에서 채팅 서비스에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match service chat
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match third-party-registration

타사 등록 요청자에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match third-party-registration** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] third-party-registration regex [*regex_name* | **class** *regex_class_name*]

no match [not] third-party-registration regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 SIP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. SIP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

third-party registration match 명령은 SIP registar 또는 SIP 프록시로 타인을 등록할 수 있는 사용자를 식별하는 데 사용됩니다. From 값과 To 값이 일치하지 않는 경우 REGISTER 메시지의 From 헤더 필드에서 식별됩니다.

예

다음 예는 SIP 검사 클래스 맵에서 서드파티 등록에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match third-party-registration regex class sip_regist
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match tunnel-group

전에 정의한 tunnel-group에 속하는 클래스 맵에서 트래픽을 확인하려면 클래스 맵 컨피그레이션 모드에서 **match tunnel-group** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match tunnel-group *name*

no match tunnel-group *name*

구문 설명

name	터널 그룹 이름에 대한 텍스트

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

클래스 맵용 트래픽 클래스에 포함된 트래픽을 식별하는 데 **match** 명령이 사용됩니다. 이러한 명령에는 클래스 맵에 포함된 트래픽을 정의하는 다른 기준이 포함되어 있습니다. Modular Policy Framework를 사용하여 보안 기능을 구성하는 과정에서 **class-map** 글로벌 컨피그레이션 명령을 사용하여 트래픽 클래스를 정의할 수 있습니다. 클래스 맵 컨피그레이션 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다.

인터페이스에 트래픽 클래스를 적용하면, 해당 인터페이스에서 수신하는 패킷을 클래스 맵의 **match** 명령문으로 정의한 기준과 비교하게 됩니다. 지정된 기준과 일치하는 패킷은 트래픽 클래스에 포함되고, 해당 트래픽 클래스와 관련된 작업을 따르게 됩니다. 어떤 트래픽 클래스의 기준과도 일치하지 않는 패킷은 기본 트래픽 클래스에 할당됩니다.

흐름 기반 정책 작업을 활성화하려면 **match flow ip destination-address** 및 **match tunnel-group** 명령을 **class-map**, **policy-map**, **service-policy** 명령과 함께 사용합니다. 흐름을 정의하는 기준은 수신 IP 주소입니다. 고유한 IP 수신 주소로 이동하는 모든 트래픽은 흐름으로 간주됩니다. 정책 작업은 전체 트래픽 클래스가 아닌 각 흐름에 적용됩니다. QoS 작업 정책은 **police** 명령을 사용해 적용합니다. 터널 그룹 내 각 터널을 특정 속도로 폴리싱하려면 **match tunnel-group** 명령과 함께 **match flow ip destination-address** 명령을 사용합니다.

예

다음 예는 터널 그룹 내에서 흐름 기반 폴리싱을 활성화하고 각 터널을 특정 속도로 제한하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
```

관련 명령

명령	설명
class-map	인터페이스에 트래픽 클래스를 적용합니다.
clear configure class-map	모든 트래픽 맵 정의를 제거합니다.
match access-list	클래스 맵 내에서 액세스 목록 트래픽을 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.
tunnel-group	IPsec 및 L2TP에 대한 연결 전용 레코드의 데이터베이스를 만들고 관리합니다.

match uri

SIP 헤더에서 URI에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match uri** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] uri {sip | tel} length gt *gt_bytes*

no match [not] uri {sip | tel} length gt *gt_bytes*

구문 설명

sip	SIP URI를 지정합니다.
tel	TEL URI를 지정합니다.
length gt *gt_bytes*	URI의 최대 길이를 지정합니다. 값의 범위는 0~65536입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 SIP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. SIP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 SIP 메시지에서 URI에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match uri sip length gt
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match url-filter

RTSP 메시지에서 URL 필터링에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match url-filter** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] url-filter regex [*regex_name* | **class** *regex_class_name*]

no match [not] url-filter regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 RTSP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다.

예

다음 예는 RTSP 검사 정책 맵에서 URL 필터링에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# regex badurl www.example.com/rtsp.avi
ciscoasa(config)# policy-map type inspect rtsp rtsp-map
ciscoasa(config-pmap)# match url-filter regex badurl
ciscoasa(config-pmap-p)# drop-connection
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match user group

Cloud Web Security의 화이트리스트에 대해 사용자 또는 그룹을 지정하려면 매개변수 컨피그레이션 모드에서 **match user group** 명령을 사용합니다. 우선 **class-map type inspect scansafe** 명령을 입력하여 매개변수 컨피그레이션 모드에 액세스할 수 있습니다. 일치를 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [**not**] {[**user** *username*] [**group** *groupname*]}

no match [**not**] {[**user** *username*] [**group** *groupname*]}

구문 설명

not	(선택 사항) Web Cloud Security를 사용하여 사용자 및/또는 그룹을 필터링하도록 지정합니다. 예를 들어, 그룹 "cisco"를 화이트리스트에 추가하되 사용자 "johncrichton" 및 "aerynsun"의 트래픽을 스캔하려면 이 두 사용자에 대해 **match not**을 지정할 수 있습니다.
user *username*	화이트리스트에 대해 사용자를 지정합니다.
group *groupname*	화이트리스트에 대해 그룹을 지정합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

AAA 규칙 또는 IDFW를 사용할 경우, 서비스 정책 규칙과 일치하는 특정 사용자 또는 그룹에서 오는 웹 트래픽이 스캐닝을 위해 Cloud Web Security 프록시 서버로 리디렉션되지 않도록 ASA를 구성할 수 있습니다. Cloud Web Security 스캐닝을 우회하는 경우, ASA에서는 프록시 서버에 연결하지 않은 채 원래 요청 웹 서버에서 직접 콘텐츠를 검색합니다. 웹 서버에서 응답을 수신하면 데이터를 클라이언트로 전송합니다. 이 과정을 트래픽의 "화이트리스팅"이라고 합니다.

Cloud Web Security로 전송하기 위해 ACL을 사용하여 트래픽의 클래스를 구성하는 경우 사용자 또는 그룹을 기반으로 트래픽을 제외하는 것과 동일한 결과를 얻을 수 있지만, 화이트리스트를 사용하는 방법이 좀 더 간단하다는 것을 알 수 있을 것입니다. 화이트리스트 기능은 IP 주소가 아니라 사용자 및 그룹만을 기반으로 합니다.

검사 정책 맵(**policy-map type inspect scansafe**)의 일부로서 화이트리스트를 만들었으면 **inspect scansafe** 명령을 사용하여 Cloud Web Security 작업을 지정할 때 이 맵을 사용할 수 있습니다.

예

다음 예는 HTTP 및 HTTPS 검사 정책 맵에 대해 동일한 사용자 및 그룹을 화이트리스트에 추가합니다.

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist

ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

관련 명령

명령	설명
class-map type inspect scansafe	화이트리스트에 있는 사용자 및 그룹에 대한 검사 클래스 맵을 만듭니다.
default user group	ASA에서 ASA로 들어오는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**] (parameters)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스에서 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청이 어느 조직에서 오는지를 나타내기 위해 ASA가 Cloud Web Security 프록시 서버에 전송하는 인증 키를 구성합니다.
policy-map type inspect scansafe	규칙에 대한 필수 매개변수를 구성하고 선택적으로 화이트리스트를 식별할 수 있도록 검사 정책 맵을 만듭니다.
retry-count	ASA 프록시 서버를 폴링하여 가용성 여부를 확인하기까지 Cloud Web Security에서 대기하는 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 컨텍스트 모드에서는 컨텍스트 단위로 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 정규화된 도메인 이름 또는 IP 주소를 구성합니다.
show conn scansafe	모든 Cloud Web Security 연결을 보여줍니다(대문자 Z 플래그로 표시됨).
show scansafe server	서버의 상태, 즉 현재 활성 서버인지, 백업 서버인지 또는 도달할 수 없는 서버인지를 보여줍니다.
show scansafe statistics	전체 및 현재 http 연결을 보여줍니다.
user-identity monitor	지정된 사용자 또는 그룹 정보를 AD 에이전트에서 다운로드합니다.
whitelist	트래픽의 클래스에 대해 화이트리스트 작업을 수행합니다.

match username

FTP 사용자 이름에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match username** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] username regex [*regex_name* | **class** *regex_class_name*]

no match [not] username regex [*regex_name* | **class** *regex_class_name*]

구문 설명

regex_name	정규식을 지정합니다.
class *regex_class_name*	정규식 클래스 맵을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 FTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. FTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 FTP 검사 클래스 맵에서 FTP 사용자 이름에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# match username regex class ftp_regex_user
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

match version

GTP 메시지 ID에 대한 일치 조건을 구성하려면 클래스 맵 또는 정책 맵 컨피그레이션 모드에서 **match message length** 명령을 사용합니다. 일치 조건을 제거하려면 이 명령의 **no** 형식을 사용합니다.

match [not] version [*version_id* | **range** *lower_range upper_range*]

no match [not] version [*version_id* | **range** *lower_range upper_range*]

구문 설명

vresion_id	버전을 지정합니다(0~255).
range *lower_range upper_range*	버전의 하한 및 상한을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 또는 정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 GTP 클래스 맵 또는 정책 맵에서 구성할 수 있습니다. GTP 클래스 맵에는 엔트리를 하나만 입력할 수 있습니다.

예

다음 예는 GTP 검사 클래스 맵에서 메시지 버전에 대한 일치 조건을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-cmap)# match version 1
```

관련 명령

명령	설명
class-map	Layer 3/4 클래스 맵을 만듭니다.
clear configure class-map	모든 클래스 맵을 제거합니다.
match any	클래스 맵의 모든 트래픽을 포함합니다.
match port	클래스 맵에서 특정 포트 번호를 식별합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

max-failed-attempts

특정 서버가 비활성화되기까지 서버 그룹에서 해당 서버에 대해 허용되는 재시도 실패 횟수를 지정하려면 aaa-server group 컨피그레이션 모드에서 **max-failed-attempts** 명령을 사용합니다. 이 지정을 제거하고 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

max-failed-attempts *number*

no max-failed-attempts

구문 설명

number	전에 **aaa-server** 명령으로 지정한 서버 그룹의 특정 서버에 대해 허용되는 연결 시도 실패 횟수를 지정하는 1~5의 정수입니다.

기본값

*number*의 기본값은 3입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
aaa-server group 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 실행하려면 먼저 AAA 서버 또는 그룹을 구성해두어야 합니다.

예

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 4
ciscoasa(config-aaa-server-group)#
```

관련 명령

명령	설명
aaa-server *server-tag* **protocol** *protocol*	그룹과 관련되고 그룹 내 모든 호스트에 공통된 AAA 서버 매개변수를 구성할 수 있도록 aaa-server group 컨피그레이션 모드로 들어갑니다.
clear configure aaa-server	모든 AAA server 컨피그레이션을 제거합니다.
show running-config aaa	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

max-forwards-validation

값이 0인 Max-forwards 헤더 필드에 대한 점검을 활성화하려면 매개변수 컨피그레이션 모드에서 **max-forwards-validation** 명령을 사용합니다. 매개변수 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

max-forwards-validation action {drop | drop-connection | reset | log} [log]

no max-forwards-validation action {drop | drop-connection | reset | log} [log]

구문 설명

drop	검증이 발생하는 경우 패킷을 삭제합니다.
drop-connection	위반이 발생하는 경우 연결을 삭제합니다.
reset	위반이 발생하는 경우 연결을 재설정합니다.
log	위반이 발생하는 경우 독립 로그 또는 추가 로그를 지정합니다. 작업과 연결 가능합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 목적지로의 홉(hop) 수를 계산합니다. 목적지에 도달하기 전에 0이 될 수 없습니다.

예

다음 예는 SIP 검사 정책 맵에서 max forwards validation을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# max-forwards-validation action log
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

max-header-length

HTTP 헤더 길이를 기반으로 HTTP 트래픽을 제한하려면 **http-map** 명령을 사용하여 액세스할 수 있는 HTTP 맵 컨피그레이션 모드에서 **max-header-length** 명령을 사용합니다. 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

no max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

구문 설명

action	메시지가 이 명령 검사에서 실패하면 작업이 수행됩니다.
allow	메시지를 허용합니다.
drop	연결을 닫습니다.
bytes	1~65535의 바이트 수입니다.
log	(선택 사항) syslog를 생성합니다.
request	메시지를 요청합니다.
reset	클라이언트와 서버에 TCP 재설정 메시지를 전송합니다.
response	(선택 사항) 메시지에 응답합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
HTTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

max-header-length 명령이 활성화되면 ASA는 구성된 제한 내에서 HTTP 헤더가 있는 메시지만 허용하고 그 외의 경우에는 지정된 작업을 수행합니다. ASA에서 TCP 연결을 재설정하고 선택적으로 syslog 엔트리를 만들도록 하려면 **action** 키워드를 사용합니다.

예

다음 예는 HTTP 요청을 100바이트가 넘지 않는 HTTP 헤더가 있는 경우로 제한합니다. 헤더가 너무 크면 ASA는 TCP 연결을 재설정하고 syslog 엔트리를 만듭니다.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-header-length request bytes 100 action log reset
ciscoasa(config-http-map)#
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
debug appfw	고급 HTTP 검사와 관련된 트래픽에 대한 자세한 정보를 표시합니다.
http-map	고급 HTTP 검사를 구성하기 위한 HTTP map을 정의합니다.
inspect http	애플리케이션 검사에 사용하기 위한 특정 HTTP map을 적용합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.

max-object-size

ASA가 WebVPN 세션에 대해 캐시할 수 있는 객체의 최대 크기를 설정하려면 캐시 모드에서 max-object-size 명령을 사용합니다. 크기를 변경하려면 명령을 다시 사용합니다.

max-object-size *integer range*

구문 설명

integer range	0 - 10000KB

기본값

1000KB

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
캐시 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

최대 객체 크기는 최소 객체 크기보다 커야 합니다. 캐시 압축이 활성화된 경우 ASA는 객체를 압축한 후 크기를 계산합니다.

예

다음 예는 4000KB의 최대 객체 크기를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# max-object-size 4000
ciscoasa(config-webvpn-cache)#
```

관련 명령

명령	설명
cache	WebVPN 캐시 모드로 들어갑니다.
cache-compressed	WebVPN 캐시 압축을 구성합니다.
disable	캐싱을 비활성화합니다.
expiry-time	캐싱 객체의 만료 시간을 구성합니다(재검증 없음).
lmfactor	최종 수정 타임스탬프만 있는 캐싱 객체의 재검증 정책을 설정합니다.
min-object-size	캐시할 객체의 최소 크기를 정의합니다.

max-retry-attempts

요청 시간이 초과되기까지 실패한 SSO 인증에 대해 ASA에서 재시도할 횟수를 구성하려면 특정 SSO 서버 유형에 대해 webvpn 컨피그레이션 모드에서 **max-retry-attempts** 명령을 사용합니다.

기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

max-retry-attempts *retries*

no max-retry-attempts

구문 설명

retries	실패한 SSO 인증 시도에 대해 ASA에서 재시도할 횟수. 범위는 1~5입니다.

기본값

이 명령의 기본값은 3입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
config-webvpn-sso-saml	• 예	—	• 예	—	—
config-webvpn-sso-siteminder	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

WebVPN에서만 사용 가능한 단일 로그인이 지원되므로, 사용자는 사용자 이름과 비밀번호를 한 번만 입력하여 다양한 서버의 서로 다른 보안 서비스에 안전하게 액세스할 수 있습니다. 현재 ASA는 SiteMinder 유형의 SSO 서버 및 SAML POST 유형의 SSO 서버를 지원합니다.

이 명령은 두 SSO 서버 유형에 모두 적용됩니다.

SSO 인증을 지원하도록 ASA를 구성했으면 선택적으로 두 가지 시간 제한 매개변수를 조정할 수 있습니다.

- 실패한 SSO 인증 시도에 대해 ASA에서 재시도할 횟수(**max-retry-attempts** 명령 사용)
- 실패한 SSO 인증 시도 시간 제한(초 단위)(**request-timeout** 명령 참조)

예

webvpn-sso-siteminder 컨피그레이션 모드에서 입력하는 다음 예는 my-sso-server라는 SiteMinder SSO 서버에 대해 4회의 인증 재시도를 구성합니다.

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)# max-retry-attempts 4
ciscoasa(config-webvpn-sso-siteminder)#
```

관련 명령

명령	설명
policy-server-secret	SiteMinder SSO 서버에 대한 인증 요청을 암호화하기 위해 사용되는 비밀 키를 만듭니다.
request-timeout	실패한 SSO 인증 시도 시간 제한(초 단위)을 지정합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso-server	단일 로그인 서버를 만듭니다.
web-agent-url	ASA에서 SiteMinder SSO 인증 요청을 수행하는 SSO 서버 URL을 지정합니다.

max-uri-length

HTTP 요청 메시지의 URI 길이를 기반으로 HTTP 트래픽을 제한하려면 **http-map** 명령을 사용하여 액세스할 수 있는 HTTP 맵 컨피그레이션 모드에서 **max-uri-length** 명령을 사용합니다. 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

no max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

구문 설명

action	메시지가 이 명령 검사에서 실패하면 작업이 수행됩니다.
allow	메시지를 허용합니다.
drop	연결을 닫습니다.
bytes	1~65535의 바이트 수입니다.
log	(선택 사항) syslog를 생성합니다.
reset	클라이언트와 서버에 TCP 재설정 메시지를 전송합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
HTTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

max-uri-length 명령이 활성화되면 ASA는 구성된 제한 내에서 URI가 있는 메시지만 허용하고 그 외의 경우에는 지정된 작업을 수행합니다. ASA에서 TCP 연결을 재설정하고 syslog 엔트리를 만들도록 하려면 **action** 키워드를 사용합니다.

길이가 구성한 값과 같거나 작은 URI가 허용됩니다. 그러지 않은 경우 지정된 작업이 수행됩니다.

예

다음 예는 HTTP 요청을 100바이트가 넘지 않는 URI가 있는 경우로 제한합니다. URI가 너무 크면 ASA는 TCP 연결을 재설정하고 syslog 엔트리를 만듭니다.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-uri-length 100 action reset log
ciscoasa(config-http-map)#
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
debug appfw	고급 HTTP 검사와 관련된 트래픽에 대한 자세한 정보를 표시합니다.
http-map	고급 HTTP 검사를 구성하기 위한 HTTP map을 정의합니다.
inspect http	애플리케이션 검사에 사용하기 위한 특정 HTTP map을 적용합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.

maximum-paths

라우팅 테이블에 설치할 수 있는 병렬 BGP 경로의 최대 수를 제어하려면 주소군 컨피그레이션 모드에서 **maximum-paths** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

maximum-paths [**ibgp**] *number-of-paths*

no maximum-paths [**ibgp**] *number-of-paths*

구문 설명

ibgp	(선택 사항) 라우팅 테이블에 설치할 수 있는 내부 BGP 경로의 최대 수를 제어할 수 있습니다.
number-of-paths	라우팅 테이블에 설치할 경로의 수.

기본값

기본적으로 BGP는 라우팅 테이블에 최적의 경로를 하나만 설치합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

maximum-paths 명령은 BGP 피어링 세션에 대해 equal-cost 또는 unequal-cost 다중 경로 로드 공유를 구성하는 데 사용됩니다. BGP 라우팅 테이블에 다중 경로로서 경로를 설치하려는 경우 해당 경로는 이미 설치된 다른 경로와 동일한 next hop을 가질 수 없습니다. BGP 다중 경로 로드 공유가 구성되어도 BGP 라우팅 프로세스에서는 여전히 BGP 피어에 대한 최적의 경로를 광고합니다. equal-cost 경로의 경우 최저 라우터 ID가 있는 이웃의 경로가 최적의 경로로서 광고됩니다.

BGP equal-cost 다중 경로 로드 공유를 구성하려면 모든 경로 특성이 동일해야 합니다. 경로 특성에는 가중치, 로컬 우선, 자동 시스템 경로(길이만이 아니라 전체 특성), 발신지 코드, MED(Multi Exit Discriminator) 및 IGP(Interior Gateway Protocol) 거리가 포함됩니다.

예

다음의 컨피그레이션 예는 두 개의 병렬 iBGP 경로를 설치합니다.

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

관련 명령

명령	설명
show bgp	BGP 라우팅 테이블의 엔트리를 표시합니다.

mcc

IMSI 접두사 필터링을 위해 모바일 국가 코드 및 모바일 네트워크 코드를 식별하려면 GTP 맵 컨피그레이션 모드에서 **mcc** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

mcc *country_code* **mnc** *network_code*

no mcc *country_code* **mnc** *network_code*

구문 설명

country_code	모바일 국가 코드를 식별하는 0이 아닌 3자리 값입니다. 1자리 또는 2자리 엔트리는 3자리 값을 만들기 위해 앞에 0이 추가됩니다.
network_code	네트워크 코드를 식별하는 2자리 또는 3자리 값입니다.

기본값

기본적으로 ASA는 유효한 MCC/MNC 조합을 확인하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
GTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IMSI 접두사 필터링에 사용됩니다. 수신된 패킷의 IMSI에 있는 MCC 및 MNC가 이 명령으로 구성된 MCC/MNC와 비교된 후 일치하지 않을 경우 삭제됩니다.

IMSI 접두사 필터링을 활성화하려면 이 명령을 사용해야 합니다. 허용되는 MCC 및 MNC 조합을 지정하려면 다양한 인스턴스를 구성할 수 있습니다. 기본적으로 ASA에서는 MNC 및 MCC 조합의 유효성을 확인하지 않으므로, 구성된 조합의 유효성을 사용자가 직접 확인해야 합니다. MCC 및 MNC 코드에 대해 자세히 알아보려면 ITU E.212 권장 사항, *Identification Plan for Land Mobile Stations*를 참조하십시오.

예

다음 예는 MCC 111과 MNC 222의 IMSI 접두사 필터링을 위한 트래픽을 식별합니다.

```
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# mcc 111 mnc 222
ciscoasa(config-gtpmap)#
```

관련 명령

명령	설명
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
debug gtp	GTP 검사에 대한 상세 정보를 표시합니다.
gtp-map	GTP 맵을 정의하고 GTP 맵 컨피그레이션 모드를 활성화합니다.
inspect gtp	애플리케이션 검사에 사용할 특정 GTP 맵을 적용합니다.
show service-policy inspect gtp	GTP 컨피그레이션을 표시합니다.

mdm-proxy

MDM proxy 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **mdm-proxy** 명령을 사용합니다. MDM 명령 모드에서 입력한 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

mdm-proxy

no mdm-proxy

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

mdm-proxy 명령은 Cisco Mobile Enablement 솔루션의 구성 요소인 Mobile Device Management 프록시를 구성합니다. MDM 프록시는 ASA를 AnyConnect Device Management Client와 ISE MDM Server 간 프록시로 구성함으로써, 오프프레미스 모바일 디바이스도 온프레미스 모바일 디바이스와 정확히 동일한 방법으로 엔터프라이즈 모바일 디바이스 관리를 받도록 합니다.

MDM 프록시를 구성하려면 다음(config-mdm-proxy 모드에서)을 지정합니다.

- **accounting-server-group** - 어카운팅 서버 그룹의 이름을 입력합니다.
- **authentication-server-group** -인증 서버 그룹의 이름을 입력합니다.
- **password-management** - 비밀번호 관리를 활성화합니다.
- **trustpoint** - ASA가 MDM 클라이언트를 대신하여 MDM 서버에서 인증을 받기 위해 사용할 인증서와 연결된 신뢰 지점의 이름을 입력합니다.
- **port** - MDM 등록 및 체크인을 위한 포트를 구성합니다.
- **session-limit** - 동시 MDM 세션의 최대 수를 설정합니다.
- **session-timeout** - MDM 등록 및 체크인 세션에 대한 최대 기간을 설정합니다.
- **enable** - 지정한 인터페이스에서 MDM 프록시를 활성화합니다.

예

다음 예는 ASA에서 MDM 프록시를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# authentication-server-group MDM
ciscoasa(config-mdm-proxy)# accounting-server-group MDM
ciscoasa(config-mdm-proxy)# trustpoint ASDM_TrustPoint1
ciscoasa(config-mdm-proxy)# password-management
ciscoasa(config-mdm-proxy)# port enrollment 443 checkin 444
ciscoasa(config-mdm-proxy)# enable outside
ciscoasa(config-mdm-proxy)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure mdm-proxy	MDM proxy 컨피그레이션을 제거합니다.
show running-config mdm-proxy	MDM 프록시에 대해 실행 중인 컨피그레이션을 표시합니다.
show mdm-proxy	MDM 프록시 통계 및 세션을 표시합니다.

media-termination

Phone Proxy 기능에 미디어를 연결하는 데 사용할 미디어 터미네이션 인스턴스를 지정하려면 글로벌 컨피그레이션 모드에서 **media-termination** 명령을 사용합니다.

Phone Proxy 컨피그레이션에서 미디어 터미네이션 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

media-termination *instance_name*

no media-termination *instance_name*

구문 설명

instance_name	미디어 터미네이션 주소가 사용되는 인터페이스의 이름을 지정합니다. 인터페이스당 미디어 터미네이션 주소를 하나만 구성할 수 있습니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(4)	이 명령이 추가되었습니다.
8.2(1)	미디어 터미네이션 주소와 함께 NAT를 사용하도록 이 명령이 업데이트되었습니다. 명령 구문에서 **rtp-min-port** 및 **rtp-max-ports** 키워드가 제거되고 별도의 명령으로 포함되었습니다.

사용 지침

ASA에는 다음 조건을 충족하는 미디어 터미네이션용 IP 주소가 있어야 합니다.

미디어 터미네이션 인스턴스의 경우 모든 인터페이스용 전역 미디어 터미네이션 주소를 구성할 수도 있고 각 인터페이스용 미디어 터미네이션 주소를 구성할 수도 있습니다. 그러나 전역 미디어 터미네이션 주소 및 각 인터페이스용으로 구성된 미디어 터미네이션 주소를 동시에 사용할 수는 없습니다.

여러 인터페이스용 미디어 터미네이션 주소를 구성하려면 IP Phone으로 통신할 때 ASA에서 사용하는 각 인터페이스에서 주소를 구성해야 합니다.

IP 주소는 공개적으로 라우팅 가능한 주소이며, 해당 인터페이스에서 주소 범위 내의 사용되지 않는 IP 주소입니다.

미디어 터미네이션 인스턴스를 만들고 미디어 터미네이션 주소를 구성할 때 반드시 따라야 할 전제 조건의 전체 목록은 CLI 컨피그레이션 가이드를 참조하십시오.

예

다음 예는 미디어 연결에 사용할 IP 주소를 지정하기 위해 media-termination address 명령을 사용하는 방법을 보여줍니다.

```
ciscoasa(config-phone-proxy)# media-termination mta_instance1
```

관련 명령

명령	설명
phone-proxy	Phone Proxy 인스턴스를 구성합니다.

media-type

구리 또는 파이버 기가비트 이더넷에 대한 미디어 유형을 설정하려면 인터페이스 컨피그레이션 모드에서 **media-type** 명령을 사용합니다. ASA 5500 Series Adaptive Security Appliance용 4GE SSM에서는 파이버 SFP 커넥터를 사용할 수 있습니다. 미디어 유형 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

media-type {**rj45** | **sfp**}

no media-type [**rj45** | **sfp**]

구문 설명

rj45	(기본값) 미디어 유형을 구리 RJ-45 커넥터로 설정합니다.
sfp	미디어 유형을 파이버 SFP 커넥터로 설정합니다.

기본값

기본값은 **rj45**입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.04	이 명령이 추가되었습니다.

사용 지침

sfp 설정은 고정 속도(1000Mbps)를 사용합니다. 따라서 **speed** 명령으로는 인터페이스에서 링크 매개변수를 협상할지 여부를 설정할 수 있습니다. **duplex** 명령은 **sfp**에 대해 지원되지 않습니다.

예

다음 예는 미디어 유형을 SFP로 설정합니다.

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)# media-type sfp
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
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어갑니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show running-config interface	인터페이스 컨피그레이션을 보여줍니다.
speed	인터페이스 속도를 설정합니다.

member

리소스 클래스에 컨텍스트를 할당하려면 컨텍스트 컨피그레이션 모드에서 **member** 명령을 사용합니다. 클래스에서 컨텍스트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

member *class_name*

no member *class_name*

구문 설명

class_name	**class** 명령으로 만든 클래스 이름을 지정합니다.

기본값

기본적으로 컨텍스트는 기본 클래스에 할당됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
컨텍스트 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

컨텍스트별 최대 제한이 적용되는 경우를 제외하고, 기본적으로 모든 보안 컨텍스트는 ASA의 리소스에 무제한으로 액세스할 수 있습니다. 그러나 하나 이상의 컨텍스트에서 너무 많은 리소스를 사용하고 있으며 그로 인해 다른 컨텍스트의 연결이 거부되는 것과 같은 상황이 벌어진다면, 컨텍스트별 리소스 사용을 제한하는 리소스 관리를 구성할 수 있습니다. ASA에서는 컨텍스트를 리소스 클래스에 지정하는 방법으로 리소스를 관리합니다. 각 컨텍스트는 해당 클래스에서 설정한 리소스 제한을 적용합니다.

예

다음 예는 컨텍스트 테스트를 gold 클래스에 할당합니다.

```
ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold
```

관련 명령

명령	설명
class	리소스 클래스를 만듭니다.
context	보안 컨텍스트를 구성합니다.
limit-resource	리소스에 대한 제한을 설정합니다.
show resource allocation	클래스 간에 리소스를 할당한 방법을 보여줍니다.
show resource types	제한을 설정할 수 있는 리소스 유형을 보여줍니다.

member-interface

이중화 인터페이스에 물리적 인터페이스를 할당하려면 인터페이스 컨피그레이션 모드에서 **member-interface** 명령을 사용합니다. 이 명령은 이중화 인터페이스 유형에만 사용할 수 있습니다. 이중화 인터페이스에 두 개의 멤버 인터페이스를 할당할 수 있습니다. 멤버 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다. 이중화 인터페이스에서 두 멤버 인터페이스를 모두 제거할 수는 없습니다. 이중화 인터페이스에는 최소 하나의 멤버 인터페이스가 필요합니다.

member-interface *physical_interface*

no member-interface *physical_interface*

구문 설명

physical_interface	인터페이스 ID(예: **gigabitethernet 0/1**)를 식별합니다. 허용되는 값은 **interface** 명령을 참조하십시오. 두 멤버 인터페이스 모두 물리적 유형이 같아야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

두 멤버 인터페이스 모두 물리적 유형이 같아야 합니다. 예를 들면 모두 Ethernet이어야 합니다.

해당 이름을 구성하지 않은 경우 물리적 인터페이스를 이중화 인터페이스에 추가할 수 없습니다. 먼저 **no nameif** 명령을 사용하여 이름을 제거해야 합니다.

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

이중화 인터페이스 쌍의 일부인 물리적 인터페이스에서 이용할 수 있는 유일한 컨피그레이션은 **speed** 및 **duplex** 명령, **description** 명령, **shutdown** 명령과 같은 물리적 매개변수입니다. 또한 **default** 및 **help**와 같은 런타임 명령을 입력할 수도 있습니다.

액티브 인터페이스를 종료할 경우 스탠바이 인터페이스가 액티브 상태로 됩니다.

액티브 인터페이스를 변경하려면 **redundant-interface** 명령을 입력합니다.

이중화 인터페이스에서는 맨 처음 추가되는 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 또는 멤버 인터페이스 MAC 주소와 관계없이 사용되는 이중화 인터페이스에 MAC 주소를 할당할 수 있습니다(**mac-address** 명령 또는 **mac-address auto** 명령 참조). 액티브 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작하면 같은 MAC 주소가 유지되므로 트래픽이 중단되지 않습니다.

예

다음 예에서는 2개의 이중화 인터페이스를 생성합니다.

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

관련 명령

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
debug redundant-interface	이중화 인터페이스 이벤트 또는 오류와 관련된 디버그 메시지를 표시합니다.
interface redundant	이중화 인터페이스를 만듭니다.
redundant-interface	액티브 멤버 인터페이스를 변경합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

memberof

이 사용자가 멤버로 속한 그룹 이름의 목록을 지정하려면 사용자 이름 특성 컨피그레이션 모드에서 **memberof** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

memberof *group_1*[,*group_2*,...*group_n*]

no memberof *group_1*[,*group_2*,...*group_n*]

구문 설명

group_1 through group_n	이 사용자가 속한 그룹을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
사용자 특성 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

이 사용자가 속한 그룹 이름의 목록을 쉼표로 구분하여 입력합니다.

예

글로벌 컨피그레이션 모드에서 입력하는 다음 예는 newuser라는 사용자 이름을 만든 다음, newuser를 DevTest 및 관리 그룹의 멤버로 지정합니다.

```
ciscoasa(config)# username newuser nopassword
ciscoasa(config)# username newuser attributes
ciscoasa(config-username)# memberof DevTest,management
ciscoasa(config-username)#
```

관련 명령

명령	설명
clear configure username	전체 사용자 이름 데이터베이스를 지우거나 지정된 사용자 이름만 지웁니다.
show running-config username	지정된 사용자 또는 모든 사용자에 대해 현재 실행 중인 사용자 이름 컨피그레이션을 표시합니다.
username	사용자 이름의 데이터베이스를 만들고 관리합니다.

memory delayed-free-poisoner enable

delayed free-memory poisoner 툴을 활성화하려면 특별 권한 EXEC 모드에서 **memory delayed-free-poisoner enable** 명령을 사용합니다. delayed free-memory poisoner 툴을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. delayed free-memory poisoner 툴을 사용하면 애플리케이션에서 릴리스된 이후 여유 메모리의 변경 사항을 모니터링할 수 있습니다.

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

memory delayed-free-poisoner enable 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

delayed free-memory poisoner 툴 활성화는 메모리 사용 및 시스템 성능에 큰 영향을 미칩니다. 이 명령은 Cisco TAC의 감독하에서만 사용해야 합니다. 시스템 사용량이 많은 기간 중에는 운영 환경에서 실행해서는 안 됩니다.

이 툴을 활성화하면 ASA에서 실행 중인 애플리케이션의 여유 메모리 요청이 FIFO 큐에 기록됩니다. 각 요청이 큐에 기록되므로, 더 낮은 수준의 메모리 관리에서 요구하지 않는 각각의 관련 메모리 바이트는 0xcc 값으로 기록됨으로써 "중독(poisoned)"됩니다.

애플리케이션에서 여유 메모리 풀에 있는 것보다 더 많은 메모리를 요구할 때까지 여유 메모리 요청이 큐에 머물러 있게 됩니다. 메모리가 필요해지면 첫 번째 여유 메모리 요청이 큐에서 풀링되고 중독된 메모리가 검증됩니다.

수정되지 않은 메모리는 더 낮은 수준의 메모리 풀로 반환되고, 초기 요청을 한 애플리케이션의 메모리 요청을 툴에서 다시 실행합니다. 요청 애플리케이션을 위한 충분한 메모리가 확보될 때까지 이 과정이 계속됩니다.

중독된 메모리가 수정되면 시스템은 강제로 충돌을 일으키고 진단 출력을 생성하여 충돌의 원인을 확인합니다.

delayed free-memory poisoner 툴은 정기적으로 큐의 모든 요소에 대해 자동으로 검증을 수행합니다. **memory delayed-free-poisoner validate** 명령을 사용하여 검증을 수동으로 시작할 수도 있습니다.

명령의 **no** 형식을 사용하면, 큐의 요청에서 참조하는 모든 메모리가 검증 없이 여유 메모리 풀로 반환되고 모든 통계 카운터가 지워집니다.

예

다음 예는 delayed free-memory poisoner 툴을 활성화합니다.

```
ciscoasa# memory delayed-free-poisoner enable
```

다음은 delayed free-memory poisoner 툴에서 잘못된 메모리 재사용을 감지하는 경우의 샘플 출력입니다.

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.

    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15

Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........

An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.

assertion "0" failed: file "delayfree.c", line 191
```

표 11-2에서는 출력의 중요한 부분에 대해 설명합니다.

표 11-2 잘못된 메모리 사용 출력 설명

필드	설명
heap region	요청 애플리케이션에서 사용할 수 있는 메모리의 주소 영역 및 영역의 크기입니다. 이 크기는 요청된 크기와 같지 않으며, 메모리 요청이 수행될 때 시스템에서 메모리를 나누는 방법에 따라 더 작을 수 있습니다.
memory address	오류가 감지된 메모리의 위치입니다.
byte offset	byte offset은 heap region의 시작 부분과 관련이 있으며, 결과가 이 주소에서 시작된 데이터 구조를 유지하는 데 사용된 경우 수정된 필드를 찾는 데 사용될 수 있습니다. 값이 0이거나 heap region 바이트 수보다 큰 경우, 더 낮은 수준의 힙 패키지에 있는 예기치 못한 값이 문제임을 나타낼 수 있습니다.

표 11-2 잘못된 메모리 사용 출력 설명 (계속)

필드	설명
allocated by/freed by	마지막 malloc/calloc/realloc 및 무료 통화가 메모리의 이 특정 영역과 관련하여 이루어진 명령 주소.
Dumping...	감지된 결함이 힙 메모리 영역의 시작 부분과 얼마나 가까운가에 따라, 하나 또는 두 개 메모리 영역의 덤프. 시스템 힙 헤더 뒤의 8바이트는 각종 시스템 헤더 값의 해시 및 큐 결합을 유지하기 위해 이 툴에서 사용하는 메모리입니다. 다른 시스템 힙 트레일러가 나타날 때까지 영역에 있는 다른 모든 바이트는 0xcc로 설정해야 합니다.

관련 명령

명령	설명
clear memory delayed-free-poisoner	delayed free-memory poisoner 툴 큐 및 통계를 지웁니다.
memory delayed-free-poisoner validate	delayed free-memory poisoner 툴 큐에서 요소를 강제로 검증합니다.
show memory delayed-free-poisoner	delayed free-memory poisoner 툴 큐 사용의 요약을 표시합니다.

memory delayed-free-poisoner validate

memory delayed-free-poisoner 큐의 모든 요소를 강제로 검증하려면 특별 권한 EXEC 모드에서 **memory delayed-free-poisoner validate** 명령을 사용합니다.

memory delayed-free-poisoner validate

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

delayed free-memory poisoner 툴을 활성화하려면 **memory delayed-free-poisoner enable** 명령을 사용한 후 **memory delayed-free-poisoner validate** 명령을 실행해야 합니다.

memory delayed-free-poisoner validate 명령을 실행하면 **memory delayed-free-poisoner** 큐의 각 요소에 대해 검증이 수행됩니다. 요소에 예기치 않은 값이 있으면 시스템은 강제로 충돌을 일으키고 진단 출력을 생성하여 충돌의 원인을 확인합니다. 예기치 않은 값이 없으면 요소들이 큐에 그대로 유지되고 툴에 의해 정상적으로 처리됩니다. **memory delayed-free-poisoner validate** 명령은 큐에 있는 메모리를 시스템 메모리 풀로 반환하지 않습니다.

참고 delayed free-memory poisoner 툴은 정기적으로 큐의 모든 요소에 대해 자동으로 검증을 수행합니다.

예

다음 예를 실행하면 **memory delayed-free-poisoner** 큐의 모든 요소에 대해 검증이 수행됩니다.

```
ciscoasa# memory delayed-free-poisoner validate
```

관련 명령

명령	설명
clear memory delayed-free-poisoner	delayed free-memory poisoner 툴 큐 및 통계를 지웁니다.
memory delayed-free-poisoner enable	delayed free-memory poisoner 툴을 활성화합니다.
show memory delayed-free-poisoner	delayed free-memory poisoner 툴 큐 사용의 요약을 표시합니다.

memory caller-address

메모리 문제를 격리하도록 호출 추적 또는 호출자 PC를 위해 프로그램 메모리의 특정 범위를 구성하려면 특별 권한 EXEC 모드에서 **memory caller-address** 명령을 사용합니다. 호출자 PC는 원시 메모리 할당을 호출한 프로그램의 주소입니다. 주소 범위를 제거하려면 이 명령의 **no** 형식을 사용합니다.

memory caller-address *startPC endPC*

no memory caller-address

구문 설명

endPC	메모리 블록의 끝 주소 범위를 지정합니다.
startPC	메모리 블록의 시작 주소 범위를 지정합니다.

기본값

메모리 추적을 위해 실제 호출자 PC가 기록됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정
7.0	이 명령이 추가되었습니다.

사용 지침

특정 메모리 블록으로 메모리 문제를 격리하려면 **memory caller-address** 명령을 사용합니다.

몇몇 경우에는 원시 메모리 할당의 실제 호출자 PC가 프로그램의 여러 곳에서 사용되는 알려진 라이브러리 함수입니다. 프로그램의 개별 장소를 격리하려면 라이브러리 함수의 시작 및 종료 프로그램 주소를 구성하여, 라이브러리 함수 호출자의 프로그램 주소를 기록합니다.

참고 호출자 주소 추적이 활성화되면 ASA에서 일시적으로 성능이 저하될 수 있습니다.

예

다음 예는 **memory caller-address** 명령으로 구성된 주소 범위 및 **show memory-caller address** 명령의 실행 결과를 보여줍니다 .

```
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
```

관련 명령

명령	설명
memory profile enable	메모리 사용의 모니터링(메모리 프로파일링)을 활성화합니다.
memory profile text	프로파일링할 메모리의 텍스트 범위를 구성합니다.
show memory	최대 물리적 메모리와 현재 운영 체제에서 이용 가능한 여유 메모리에 대한 요약 정보를 표시합니다.
show memory binsize	특정 bin 크기에 할당된 청크에 대한 요약 정보를 표시합니다.
show memory profile	ASA의 메모리 사용(프로파일링)에 대한 정보를 표시합니다.
show memory-caller address	ASA에 구성된 주소 범위를 표시합니다.

memory profile enable

메모리 사용(메모리 프로파일링)의 모니터링을 활성화하려면 특별 권한 EXEC 모드에서 **memory profile enable** 명령을 사용합니다. 메모리 프로파일링을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

memory profile enable peak *peak_value*

no memory profile enable peak *peak_value*

구문 설명

peak_value	메모리 사용의 스냅샷이 피크 사용 버퍼에 저장되는 메모리 사용 임계값을 지정합니다. 시스템의 피크 메모리 요구 사항을 결정하기 위해 나중에 이 버퍼의 내용을 분석할 수 있습니다.

기본값

메모리 프로파일링은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정
7.0	이 명령이 추가되었습니다.

사용 지침

메모리 프로파일링을 활성화하기 전에 먼저 **memory profile text** 명령을 사용해 프로파일링할 메모리 텍스트 범위를 구성해야 합니다.

일부 메모리는 사용자가 **clear memory profile** 명령을 입력할 때까지 프로파일링 시스템에 의해 보류됩니다. **show memory status** 명령의 결과를 확인해보십시오.

참고 메모리 프로파일링이 활성화되면 ASA에서 일시적으로 성능이 저하될 수 있습니다.

다음 예는 메모리 프로파일링을 활성화합니다.

```
ciscoasa# memory profile enable
```

관련 명령

명령	설명
memory profile text	프로파일링할 메모리의 텍스트 범위를 구성합니다.
show memory profile	ASA의 메모리 사용(프로파일링)에 대한 정보를 표시합니다.

memory profile text

프로파일링할 메모리의 프로그램 텍스트 범위를 구성하려면 특별 권한 EXEC 모드에서 **memory profile text** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

memory profile text {*startPC endPC* | **all** *resolution*}

no memory profile text {*startPC endPC* | **all** *resolution*}

구문 설명

all	메모리 블록의 전체 텍스트 범위를 지정합니다.
endPC	메모리 블록의 끝 텍스트 범위를 지정합니다.
resolution	소스 텍스트 영역에 대한 추적의 확인 정도(resolution)를 지정합니다.
startPC	메모리 블록의 시작 텍스트 범위를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정
7.0	이 명령이 추가되었습니다.

사용 지침

텍스트 범위가 작은 경우, 확인 정도 "4"가 일반적으로 명령에 대한 호출을 추적합니다. 텍스트 범위가 더 큰 경우, 첫 번째 통과에는 대략적인 확인 정도로 충분할 것입니다. 다음번 패스에서 더 작은 영역의 집합으로 범위를 좁힐 수 있습니다.

memory profile text 명령으로 텍스트 범위를 입력한 후 **memory profile enable** 명령을 입력하여 메모리 프로파일링을 시작해야 합니다. 메모리 프로파일링은 기본적으로 비활성화되어 있습니다.

참고 메모리 프로파일링이 활성화되면 ASA에서 일시적으로 성능이 저하될 수 있습니다.

예

다음 예는 확인 정도 4로 프로파일링할 메모리의 텍스트 범위를 구성하는 방법을 보여줍니다.

```
ciscoasa# memory profile text 0x004018b4 0x004169d0 4
```

다음 예는 텍스트 범위의 컨피그레이션 및 메모리 프로파일링의 상태(OFF)를 보여줍니다.

```
ciscoasa# show memory profile
InUse profiling: OFF
Peak profiling: OFF
Profile:
0x004018b4-0x004169d0(00000004)
```

참고 메모리 프로파일링을 시작하려면 **memory profile enable** 명령을 입력해야 합니다. 메모리 프로파일링은 기본적으로 비활성화되어 있습니다.

관련 명령

명령	설명
clear memory profile	메모리 프로파일링 기능에 의해 보유된 버퍼를 지웁니다.
memory profile enable	메모리 사용의 모니터링(메모리 프로파일링)을 활성화합니다.
show memory profile	ASA의 메모리 사용(프로파일링)에 대한 정보를 표시합니다.
show memory-caller address	ASA에 구성된 주소 범위를 표시합니다.

memory-size

WebVPN의 다양한 구성 요소가 액세스할 수 있는 메모리의 양을 ASA에서 구성하려면 webvpn 모드에서 **memory-size** 명령을 사용합니다. KB 단위를 사용하거나 전체 메모리의 백분율을 사용하여 메모리의 양을 구성할 수 있습니다. 구성한 메모리 크기를 제거하려면 이 명령의 **no** 형식을 사용합니다.

참고 새 메모리 크기 설정을 적용하려면 재시동해야 합니다.

memory-size {percent | kb} *size*

no memory-size [{percent | kb} *size***]**

구문 설명

kb	KB 단위로 메모리의 양을 지정합니다.
percent	ASA에서 총 메모리의 백분율로 메모리의 양을 지정합니다.
size	KB 단위로 또는 총 메모리의 백분율로 메모리의 양을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

구성된 메모리의 양이 즉시 할당됩니다. 이 명령을 구성하기 전에 show memory를 사용하여 사용 가능한 메모리의 양을 확인하십시오. 컨피그레이션에서 총 메모리의 백분율을 사용하는 경우 구성된 값이 사용 가능한 백분율보다 낮아야 합니다. 컨피그레이션에서 KB 값을 사용하는 경우 구성된 값이 KB 단위의 사용 가능한 메모리의 양보다 낮아야 합니다.

예

다음 예는 30퍼센트의 WebVPN 메모리 크기를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# reload
```

관련 명령

명령	설명
show memory webvpn	WebVPN 메모리 사용 통계를 표시합니다.

memory tracking enable

힙 메모리 요청의 추적을 활성화하려면 특별 권한 EXEC 모드에서 **memory tracking enable** 명령을 사용합니다. 메모리 추적을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

memory tracking enable

no memory tracking enable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	—	• 예	• 예

명령 기록

릴리스	수정
7.0(8)	이 명령이 추가되었습니다.

사용 지침

힙 메모리 요청을 추적하려면 **memory tracking enable** 명령을 사용합니다. 메모리 추적을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

예

다음 예는 힙 메모리 요청의 추적을 활성화합니다.

```
ciscoasa# memory tracking enable
```

관련 명령

명령	설명
clear memory tracking	현재 수집된 모든 정보를 지웁니다.
show memory tracking	현재 할당된 메모리를 보여줍니다.
show memory tracking address	툴로 추적한 현재 할당된 각 메모리 부문에 대한 크기, 위치 및 최고 호출자 함수를 나열합니다.
show memory tracking dump	지정된 메모리 주소의 크기, 위치, 부분적인 호출 스택 및 메모리 덤프를 보여줍니다.
show memory tracking detail	툴이 내부에서 어떻게 동작하는지를 알아내기 위해 사용할 수 있는 각종 내부 세부 정보를 보여줍니다.

merge-dacl

다운로드 가능한 ACL과 RADIUS 패킷으로부터 Cisco AV 쌍에서 수신한 ACL을 병합하려면 aaa-server group 컨피그레이션 모드에서 **merge-dacl** 명령을 사용합니다. 다운로드 가능한 ACL과 RADIUS 패킷으로부터 Cisco AV 쌍에서 수신한 ACL의 병합을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

merge dacl {**before_avpair** | **after_avpair**}

no merge dacl

구문 설명

after_avpair	다운로드 가능한 ACL 엔트리를 Cisco AV 쌍 엔트리보다 나중에 배치해야 함을 지정합니다. 이 옵션은 VPN 연결에만 적용됩니다. VPN 사용자의 경우 ACL은 Cisco AV 쌍 ACL, 다운로드 가능한 ACL, ASA에 구성된 ACL의 형태로 존재할 수 있습니다. 이 옵션은 다운로드 가능한 ACL과 AV 쌍 ACL의 병합 여부를 결정하며 ASA에 구성된 ACL에는 적용되지 않습니다.
before_avpair	다운로드 가능한 ACL 엔트리를 Cisco AV 쌍 엔트리보다 먼저 배치해야 함을 지정합니다.

기본값

기본 설정은 다운로드 가능한 ACL을 Cisco AV 쌍 ACL과 병합하지 않도록 지정하는 **no merge dacl** 입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
AAA-server group 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

AV 쌍과 다운로드 가능한 ACL이 모두 수신되는 경우 AV 쌍이 우선 사용됩니다.

예

다음 예는 다운로드 가능한 ACL 엔트리를 Cisco AV 쌍 엔트리보다 먼저 배치해야 함을 지정합니다.

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

관련 명령

명령	설명
aaa-server host	서버 및 그 서버가 속한 AAA 서버 그룹을 지정합니다.
aaa-server protocol	서버 그룹 이름과 프로토콜을 지정합니다.
max-failed-attempts	다음 서버를 시도하기 전에 그룹의 AAA 서버로 보낼 수 있는 최대 요청 횟수를 지정합니다.

message-length(DNS Map)

구성된 최대 길이를 충족하지 못하는 DNS 패킷을 필터링하려면 매개변수 컨피그레이션 모드에서 **message-length** 명령을 사용합니다. 명령을 제거하려면 **no** 형식을 사용합니다.

message-length maximum {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}}

no message-length maximum {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}}

구문 설명

length	DNS 메시지에서 허용되는 최대 바이트 수(512~65535).
client {*length* | **auto**}	클라이언트 DNS 메시지에서 허용되는 최대 바이트 수(512~65535). 또는 **auto**는 최대 길이를 Resource Record의 값으로 설정합니다.
server {*length* | **auto**}	서버 DNS 메시지에서 허용되는 최대 바이트 수(512~65535). 또는 **auto**는 최대 길이를 Resource Record의 값으로 설정합니다.

기본값

기본 검사는 DNS 최대 메시지 길이를 512로, 클라이언트 길이를 **auto**로 설정합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(2)	이 명령이 추가되었습니다.

사용 지침

최대 DNS 메시지 길이를 DNS 검사 맵의 매개변수로서 구성할 수 있습니다.

예

다음 예는 DNS 검사 정책 맵에서 최대 DNS 메시지 길이를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length 512
ciscoasa(config-pmap-p)# message-length client auto
```

관련 명령

명령	설명
parameter	정책 맵 컨피그레이션 모드에 있는 동안 parameter 컨피그레이션 모드로 들어갑니다.
policy-map type inspect dns	DNS 검사 정책 맵을 만듭니다.

message-length(GTP Map)

구성된 최대 및 최소 길이를 충족하지 못하는 GTP 패킷을 필터링하려면 **gtp-map** 명령을 사용하여 액세스할 수 있는 GTP 맵 컨피그레이션 모드에서 **message-length** 명령을 사용합니다. 명령을 제거하려면 **no** 형식을 사용합니다.

message-length min *min_bytes* **max** *max_bytes*

no message-length min *min_bytes* **max** *max_bytes*

구문 설명

max	UDP 페이로드에서 허용되는 최대 바이트 수를 지정합니다.
max_bytes	UDP 페이로드의 최대 바이트 수. 범위는 1~65536입니다.
min	UDP 페이로드에서 허용되는 최소 바이트 수를 지정합니다.
min_bytes	UDP 페이로드의 최소 바이트 수. 범위는 1~65536입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
GTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령으로 지정하는 길이는 GTP 헤더와 메시지의 나머지를 합한 것으로, UDP 패킷의 페이로드입니다.

예

다음 예는 길이가 20~300바이트인 메시지를 허용합니다.

```
ciscoasa(config)# gtp-map gtp-policy
ciscoasa(config-gtpmap)# permit message-length min 20 max 300
ciscoasa(config-gtpmap)#
```

관련 명령

명령	설명
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
debug gtp	GTP 검사에 대한 상세 정보를 표시합니다.
gtp-map	GTP 맵을 정의하고 GTP 맵 컨피그레이션 모드를 활성화합니다.
inspect gtp	애플리케이션 검사에 사용할 특정 GTP 맵을 적용합니다.
show service-policy inspect gtp	GTP 컨피그레이션을 표시합니다.

12 장

mfib forwarding through mus server 명령

mfib forwarding

인터페이스에서 MFIB 포워딩을 다시 활성화하려면 인터페이스 컨피그레이션 모드에서 **mfib forwarding** 명령을 사용합니다. 인터페이스에서 MFIB 포워딩을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

mfib forwarding

no mfib forwarding

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

multicast-routing 명령은 기본적으로 모든 인터페이스에서 MFIB 포워딩을 활성화합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

멀티캐스트 라우팅을 활성화하면 기본적으로 모든 인터페이스에서 MFIB 포워딩이 활성화됩니다. 특정 인터페이스에서 MFIB 포워딩을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 실행 중인 컨피그레이션에서는 명령의 **no** 형식만 표시됩니다.

인터페이스에서 MFIB 포워딩이 비활성화되면, 다른 방법을 통해 특별히 구성하지 않는 한 해당 인터페이스에서는 멀티캐스트 패킷을 허용하지 않습니다. MFIB 포워딩이 비활성화되면 IGMP 패킷도 차단됩니다.

예

다음 예는 지정한 인터페이스에서 MFIB 포워딩을 비활성화합니다.

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

관련 명령

명령	설명
multicast-routing	멀티캐스트 라우팅을 활성화합니다.
pim	인터페이스에서 PIM을 활성화합니다.

migrate

LAN-to-LAN(IKEv1) 또는 원격 액세스 컨피그레이션(SSL 또는 IKEv1)을 IKEv2로 마이그레이션하려면 글로벌 컨피그레이션 모드에서 **migrate** 명령을 사용합니다.

migrate {**l2l** | **remote-access** {**ikev2** | **ssl**} | **overwrite**}

구문 설명

l2l	IKEv1 LAN-to-LAN 컨피그레이션을 IKEv2로 마이그레이션합니다.
remote-access	원격 액세스 컨피그레이션을 지정합니다.
ikev2	원격 액세스 IKEv1 컨피그레이션을 IKEv2로 마이그레이션합니다.
ssl	원격 액세스 SSL 컨피그레이션을 IKEv2로 마이그레이션합니다.
overwrite	기존의 IKEv2 컨피그레이션을 덮어씁니다.

기본값

기본값 또는 동작이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

migrate l2l 명령은 모든 LAN-to-LAN IKEv1 컨피그레이션을 IKEv2로 마이그레이션합니다.

overwrite 키워드를 사용하는 경우 ASA에서는 기존의 IKEv2 컨피그레이션을 병합하는 대신 마이그레이션된 명령으로 덮어씁니다.

migrate remote-access 명령은 IKEv1 또는 SSL 설정을 IKEv2로 마이그레이션하지만, 사용자는 여전히 다음과 같은 컨피그레이션 작업을 수행할 수 있습니다.

- webvpn 컨피그레이션 모드에서 AnyConnect 클라이언트 패키지 파일을 로드합니다.
- AnyConnect 클라이언트 프로필을 구성하고 그룹 정책을 위해 지정합니다.
- IKEv1 연결에 사용된 사용자화 객체를 IKEv2 연결에 사용된 터널 객체와 연결합니다.
- **crypto ikev2 remote-access trust-point** 명령을 사용하여 사용자 인증 ID 인증서(신뢰 지점)를 지정합니다. ASA는 신뢰 지점을 사용하여 IKEv2로 연결된 원격 AnyConnect 클라이언트에 대해 자체 인증을 수행합니다.

- 기본 터널 그룹 또는 그룹 정책 외에 추가로 구성했을 수 있는 모든 터널 그룹 또는 그룹 정책에 대해 IKEv2 및/또는 SSL을 지정합니다. IKEv2 또는 SSL을 허용하기 위해 DefaultWEBVPNGroup 터널 그룹 및 기본 그룹 정책이 구성됩니다.
- 클라이언트가 기본 그룹 이외의 그룹에 연결할 수 있도록 터널 그룹에서 그룹 별칭 또는 그룹 URL을 구성합니다.
- 외부 그룹 정책 및/또는 사용자 레코드를 업데이트합니다.
- 클라이언트 동작을 변경하기 위한 다른 전역, 터널 그룹, 그룹 정책 설정.
- **crypto ikev2 enable** <*interface*> [**client-services** [*port*]] 명령을 사용하여 클라이언트가 파일을 다운로드하거나 IKEv2용 소프트웨어 업그레이드를 수행하기 위해 사용할 포트를 구성합니다.

관련 명령

명령	설명
crypto ikev2 enable	IPsec 피어가 통신하는 인터페이스에서 IKEv2 협상을 활성화합니다.
show run crypto ikev2	IKEv2 컨피그레이션 정보를 표시합니다.

min-object-size

ASA가 WebVPN 세션에 대해 캐시할 수 있는 객체의 최소 크기를 설정하려면 캐시 모드에서 min-object-size 명령을 사용합니다. 크기를 변경하려면 명령을 다시 사용합니다. 최소 객체 크기를 설정하려면 영(0)의 값을 입력합니다.

min-object-size *integer range*

구문 설명

integer range	0~10000KB

기본값

기본 크기는 0KB입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
캐시 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

최소 객체 크기는 최대 객체 크기보다 작아야 합니다. 캐시 압축이 활성화된 경우 ASA는 객체를 압축한 후 크기를 계산합니다.

예

다음 예는 40KB의 최대 객체 크기를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# min-object-size 40
ciscoasa(config-webvpn-cache)#
```

관련 명령

명령	설명
cache	WebVPN 캐시 모드로 들어갑니다.
cache-compressed	WebVPN 캐시 압축을 구성합니다.
disable	캐싱을 비활성화합니다.
expiry-time	캐싱 객체의 만료 시간을 구성합니다(재검증 없음).
lmfactor	최종 수정 타임스탬프만 있는 캐싱 객체의 재검증 정책을 설정합니다.
max-object-size	캐시할 객체의 최대 크기를 정의합니다.

mkdir

디렉토리를 만들려면 특별 권한 EXEC 모드에서 **mkdir** 명령을 사용합니다.

mkdir [/noconfirm] [disk0: | disk1: | flash:]*path*

구문 설명

noconfirm	(선택 사항) 확인 프롬프트를 억제합니다.
disk0*:*	(선택 사항) 내장 플래시 메모리 및 그 뒤에 콜론을 지정합니다.
disk1:	(선택 사항) 외장 플래시 메모리 카드 및 그 뒤에 콜론을 지정합니다.
flash:	(선택 사항) 내장 플래시 메모리 및 그 뒤에 콜론을 지정합니다. ASA 5500 Series Adaptive Security 어플라이언스에서 **flash** 키워드는 **disk0**의 별칭을 갖게 됩니다.
path	만들 디렉토리의 이름 및 경로입니다.

기본값

경로를 지정하지 않으면 디렉토리는 현재의 작업 디렉토리에 생성됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

동일한 이름의 디렉토리가 이미 존재하면 새 디렉토리가 생성되지 않습니다.

예

다음 예는 "backup"이라는 이름의 새 디렉토리를 만드는 방법을 보여줍니다.

```
ciscoasa# mkdir backup
```

관련 명령

명령	설명
cd	현재의 작업 디렉토리를 지정한 디렉토리로 변경합니다.
dir	디렉토리 내용을 표시합니다.
rmdir	지정한 디렉토리를 제거합니다.
pwd	현재의 작업 디렉토리를 표시합니다.

mobile-device portal

모든 모바일 디바이스에 대해 클라이언트리스 VPN 액세스 웹 포털을 미니 포털에서 전체 브라우저 포털로 변경하려면 webvpn 컨피그레이션 모드에서 **mobile-device portal** 명령을 사용합니다. Windows CE와 같은 구형 운영 체제에서 운영되는 스마트폰에 대해서만 이 컨피그레이션을 만들면 됩니다. 최신 스마트폰은 기본적으로 full-browser 포털을 사용하므로 이 옵션을 구성할 필요가 없습니다.

mobile-device portal {full}

no mobile-device portal {full}

구문 설명

mobile-device portal {full}	모든 모바일 디바이스에 대해 클라이언트리스 VPN 액세스 포털을 미니 포털에서 전체 브라우저 포털로 변경합니다.

명령 기본값

이 명령을 실행하기 전에는 기본적으로 일부 모바일 디바이스에서 미니 포털을 통해 클라이언트리스 VPN 액세스를 얻고 다른 모바일 디바이스에서는 전체 포털을 사용합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(5)	8.2(5)와 8.4(2)에서 동시에 이 명령을 추가했습니다.
8.4(2)	8.2(5)와 8.4(2)에서 동시에 이 명령을 추가했습니다.

사용 지침

Cisco TAC(Technical Assistance Center)에서 권장하는 경우에만 이 명령을 사용하십시오.

예

모든 모바일 디바이스에 대해 클라이언트리스 VPN 액세스 포털을 전체 브라우저 포털로 변경합니다.

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

관련 명령

명령	설명
show running-config webvpn	webvpn에 대해 실행 중인 컨피그레이션을 표시합니다.

mode

보안 컨텍스트 모드를 단일 또는 다중으로 설정하려면 글로벌 컨피그레이션 모드에서 **mode** 명령을 사용합니다. 단일 ASA를 보안 컨텍스트로 알려진 다중 가상 디바이스로 분할할 수 있습니다. 각 컨텍스트는 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스로서 작동합니다. 다중 컨텍스트는 여러 대의 독립형 어플라이언스가 있는 것과 비슷합니다. 단일 모드에서는 ASA가 단일 컨피그레이션을 갖게 되며 단일 디바이스로서 작동합니다. 다중 모드에서는 각각 고유한 컨피그레이션이 있는 다중 컨텍스트를 만들 수 있습니다. 허용되는 컨텍스트의 개수는 라이센스에 따라 다릅니다.

mode {**single** | **multiple**} [**noconfirm**]

구문 설명

multiple	다중 컨텍스트 모드를 설정합니다.
noconfirm	(선택 사항) 확인 프롬프트 없이 모드를 설정합니다. 이 옵션은 자동화된 스크립트에 유용합니다.
single	컨텍스트 모드를 single로 설정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

다중 컨텍스트 모드에서는 ASA에 보안 정책, 인터페이스 및 독립형 디바이스에서 구성할 수 있는 거의 모든 옵션을 식별하는, 각 컨텍스트에 대한 컨피그레이션이 포함됩니다(컨텍스트 컨피그레이션을 식별하려면 **config-url** 명령 참조). 시스템 관리자는 시스템 컨피그레이션(단일 모드 컨피그레이션과 마찬가지로 시작 컨피그레이션)에서 컨텍스트를 구성하여 컨텍스트를 추가하고 관리할 수 있습니다. 시스템 컨피그레이션은 ASA를 위한 기본적인 설정을 나타냅니다. 시스템 컨피그레이션은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 컨텍스트 다운로드) 관리 컨텍스트로 지정된 컨텍스트 중 하나를 사용합니다.

mode 명령을 사용하여 컨텍스트 모드를 변경하면 재부팅하라는 프롬프트가 표시됩니다.

컨텍스트 모드(single 또는 multiple)는 재부팅할 때 유지되더라도 컨피그레이션 파일에 저장되지 않습니다. 컨피그레이션을 다른 디바이스에 복사하려면 **mode** 명령을 사용하여 새 디바이스의 모드를 일치하게 설정합니다.

단일 모드에서 다중 모드로 전환할 때 ASA는 실행 중 컨피그레이션을 2개 파일로 변환합니다(내장 플래시 메모리의 루트 디렉토리에서). 2개 파일은 각각 시스템 컨피그레이션인 new startup 컨피그레이션과 관리 컨텍스트인 admin.cfg입니다. 원래의 실행 중 컨피그레이션은 old_running.cfg로 내장 플래시 메모리의 루트 디렉토리에 저장됩니다. 원래의 시작 컨피그레이션은 저장되지 않습니다. ASA는 관리 컨텍스트 엔트리를 "admin"이라는 이름으로 시스템 컨피그레이션에 자동 추가합니다.

다중 모드에서 단일 모드로 변환하는 경우 먼저 완전한 시작 컨피그레이션(사용 가능한 경우)을 ASA에 복사할 수 있습니다. 다중 모드에서 상속된 시스템 컨피그레이션은 단일 모드 디바이스에서 완전하게 작동하는 컨피그레이션이 아닙니다.

다중 컨텍스트 모드에서 모든 기능이 지원되는 것은 아닙니다. 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

예

다음 예는 모드를 multiple로 설정합니다.

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

Booting system, please wait...
```

다음 예는 모드를 single로 설정합니다.

```
ciscoasa(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode



Rebooting....

Booting system, please wait...
```

관련 명령

명령	설명
context	시스템 컨피그레이션에서 컨텍스트를 구성하고 컨텍스트 컨피그레이션 모드로 들어갑니다.
show mode	현재의 컨텍스트 모드(single 또는 multiple)를 표시합니다.

monitor-interface

특정 인터페이스에서 상태 모니터링을 활성화하려면 글로벌 컨피그레이션 모드에서 **monitor-interface** 명령을 사용합니다. 인터페이스 모니터링을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

monitor-interface {*if_name* | **service-module**}

no monitor-interface {*if_name* | **service-module**}

구문 설명

if_name	모니터링할 인터페이스의 이름을 지정합니다.
service-module	서비스 모듈을 모니터링합니다. ASA FirePOWER 모듈 같은 하드웨어 모듈 오류로 인해 장애 조치가 일어나지 않도록 하려면, 이 명령의 **no** 형식을 사용하여 모듈 모니터링을 비활성화할 수 있습니다.

기본값

물리적 인터페이스 및 서비스 모듈의 모니터링은 기본적으로 활성화되고, 논리적 인터페이스의 모니터링은 기본적으로 비활성화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.3(1)	service-module 키워드가 추가되었습니다.

사용 지침

ASA에 대해 모니터링할 수 있는 인터페이스의 수는 플랫폼에 따라 다르며 **show failover** 명령의 출력으로 확인할 수 있습니다.

Hello 메시지는 ASA 장애 조치 쌍 간의 모든 인터페이스 폴링 빈도 기간 중에 교환됩니다. 장애 조치 인터페이스 폴링 시간은 3~15초입니다. 예를 들어 폴링 시간을 5초로 설정하면, 해당 인터페이스에서 5개의 연속 hello 메시지가 수신되지 않는 경우(25초) 인터페이스에 대한 테스트가 시작됩니다.

모니터링한 장애 조치 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없다는 의미이기도 합니다.
- Normal - 인터페이스에서 트래픽을 수신 중입니다.
- Testing - 5번의 폴링 시간 동안 hello 메시지가 인터페이스에서 수신되지 않습니다.
- Link Down - 인터페이스 또는 VLAN의 관리 상태가 중단되었습니다.

- No Link - 인터페이스의 물리적 링크가 중단되었습니다.
- Failed - 인터페이스에 트래픽이 수신되지 않았으나, 피어 인터페이스에는 트래픽이 수신되었습니다.

액티브/액티브 장애 조치의 경우 이 명령이 컨텍스트 내에서 유일하게 유효합니다.

예

다음 예는 "inside"라는 인터페이스에서 모니터링을 활성화합니다.

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure monitor-interface	모든 인터페이스에 대해 기본 인터페이스 상태 모니터링을 복원합니다.
failover interface-policy	오류로 인해 장애 조치가 발생하는 모니터링 대상 인터페이스의 수 또는 비율을 지정합니다.
failover polltime	인터페이스에서 hello 메시지 간의 간격을 지정합니다(액티브/스탠바이 장애 조치).
polltime interface	인터페이스에서 hello 메시지 간의 간격을 지정합니다(액티브/액티브 장애 조치).
show running-config monitor-interface	실행 중인 컨피그레이션에서 **monitor-interface** 명령을 표시합니다.

more

파일의 내용을 표시하려면 특별 권한 EXEC 모드에서 **more** 명령을 사용합니다.

more {**/ascii** | **/binary**| **/ebcdic** | **disk0**: | **disk1**: | **flash**: | **ftp**: | **http**: | **https**: | **system**: | **tftp**:}*filename*

구문 설명

/ascii	(선택 사항) 이진 모드에서 이진 파일 및 ASCII 파일을 표시합니다.
/binary	(선택 사항) 이진 모드에서 파일을 표시합니다.
/ebcdic	(선택 사항) EBCDIC에서 이진 파일을 표시합니다.
disk0*:*	(선택 사항) 내장 플래시 메모리의 파일을 표시합니다.
disk1:	(선택 사항) 외장 플래시 메모리 카드의 파일을 표시합니다.
filename	사용할 파일의 이름을 지정합니다.
flash:	(선택 사항) 내장 플래시 메모리 및 그 뒤에 콜론을 지정합니다. ASA 5500 Series Adaptive Security 어플라이언스에서 **flash** 키워드는 **disk0**의 별칭을 갖게 됩니다.
ftp:	(선택 사항) FTP 서버의 파일을 표시합니다.
http:	(선택 사항) 웹사이트의 파일을 표시합니다.
https:	(선택 사항) 보안 웹사이트의 파일을 표시합니다.
system:	(선택 사항) 파일 시스템을 표시합니다.
tftp:	(선택 사항) TFTP 서버의 파일을 표시합니다.

기본값

ASCII 모드

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

more filesystem: 명령은 로컬 디렉토리의 별칭 또는 파일 시스템을 입력하라는 프롬프트를 표시합니다.

참고 **more** 명령을 사용하여 저장한 컨피그레이션 파일을 보는 경우 컨피그레이션 파일의 터널 그룹 비밀번호가 일반 텍스트로 나타납니다.

예

다음 예는 "test.cfg"라는 이름의 로컬 파일 내용을 표시하는 방법을 보여줍니다.

```
ciscoasa# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005

XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

관련 명령

명령	설명
cd	지정한 디렉토리로 변경합니다.
pwd	현재의 작업 디렉토리를 표시합니다.

mount(CIFS)

CIFS(Common Internet File System)에서 보안 어플라이언스에 액세스하도록 하려면 글로벌 컨피그레이션 모드에서 **mount** 명령을 사용합니다. 이 명령을 사용하면 mount cifs 컨피그레이션 모드로 들어갈 수 있습니다. CIFS 네트워크 파일 시스템을 마운트 해제하려면 이 명령의 **no** 형식을 사용합니다.

mount *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

[**no**] **mount** *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

구문 설명

domain *domain-name*	(선택 사항) CIFS 파일 시스템의 경우에만, 이 인수는 Windows NT 도메인 이름을 지정합니다. 최대 63자를 사용할 수 있습니다.
name	로컬 CA에 할당할 기존 파일 시스템의 이름을 지정합니다.
no	이미 마운트된 CIFS 파일 시스템을 제거하고 액세스할 수 없도록 처리합니다.
password *password*	파일 시스템 마운팅을 위한 권한 있는 비밀번호를 식별합니다.
server *server-name*	CIFS 파일 시스템 서버의 사전 정의된 이름(또는 점으로 구분된 10진수 표기법의 IP 주소)을 지정합니다.
share *sharename*	서버 내에서 파일 데이터에 액세스할 수 있도록 이름 기준으로 특정 서버 공유(폴더)를 명시적으로 식별합니다.
status enable/disable	파일 시스템의 상태를 마운트된 상태 또는 마운트 해제된 상태(사용 가능 또는 사용 불가능)로 식별합니다.
type	마운트할 파일 시스템의 CIFS 유형을 지정합니다. 대체 **type** 키워드의 경우 **mount (FTP)** 명령을 참조하십시오.
type cifs	마운트하는 파일 시스템이 CIFS임을 지정합니다. 이 파일 시스템은 CIFS 공유 디렉토리에 볼륨 마운팅 기능을 제공합니다.
user *username*	파일 시스템 마운팅을 위한 권한 있는 사용자 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Mount cifs 컨피그레이션	• 예	• 예	• 예	—	• 예
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

mount 명령은 IFS(Installable File System)를 사용하여 CIFS 파일 시스템을 마운트합니다. 파일 시스템 API인 IFS는 보안 어플라이언스가 파일 시스템용 드라이버를 인식하여 로드하도록 지원합니다.

mount 명령은 보안 어플라이언스의 CIFS 파일 시스템을 UNIX 파일 트리에 연결합니다. 반대로 **no mount** 명령은 분리합니다.

mount 명령으로 지정한 *mount-name*은 보안 어플라이언스에 이미 마운트된 파일 시스템을 참조하기 위해 다른 CLI 명령에서 사용됩니다. 예를 들어 Local Certificate Authority용 파일 스토리지를 설정하는 **database** 명령을 이용해 데이터베이스 파일을 비 플래시 스토리지에 저장하려면 마운트된 기존 파일 시스템의 마운트 이름이 필요합니다.

CIFS 원격 파일 액세스 프로토콜은 애플리케이션이 로컬 디스크 및 네트워크 파일 서버에서 데이터를 공유하는 방식과 호환됩니다. 인터넷의 전역 DNS를 사용하여 TCP/IP를 통해 실행되는 CIFS는 Microsoft에서 제공하는 공개적인 플랫폼 간 SMB(Server Message Block) 프로토콜의 고급 버전이며, Windows 운영 체제의 기본 파일 공유 프로토콜입니다.

mount 명령을 사용한 후에는 항상 루트 셸에서 빠져나와야 합니다. mount-cifs-config 모드의 **exit** 키워드는 사용자를 글로벌 컨피그레이션 모드로 되돌립니다.

다시 연결하려면 연결을 스토리지에 다시 매핑해야 합니다.

참고 CIFS 및 FTP 파일 시스템의 마운트는 지원됩니다 (**mount** *name* **type ftp** 명령 참조.). NFS(Network File System) 볼륨의 마운트는 현재 릴리스에서 지원되지 않습니다.

예

다음 예는 *cifs://amer;chief:big-boy@myfiler02/my_share*를 *cifs_share* 레이블로 마운트합니다.

```
ciscoasa(config)# mount cifs_share type CIFS
ciscoasa (config-mount-cifs)# server myfiler02a
```

관련 명령

명령	설명
debug cifs	CIFS 디버그 메시지를 기록합니다.
debug ntdomain	웹 VPN NT 도메인 디버그 메시지를 기록합니다.
debug webvpn cifs	WebVPN CIFS 디버그 메시지를 기록합니다.
dir all-filesystems	ASA에 마운트된 모든 파일 시스템의 파일을 표시합니다.

mount(FTP)

FTP(File Transfer Protocol) 파일 시스템이 보안 어플라이언스에 액세스할 수 있도록 하려면 FTP 컨피그레이션 모드로 들어가기 위한 글로벌 컨피그레이션 모드에서 **mount** *name* **type ftp** 명령을 사용합니다. FTP 네트워크 파일 시스템의 마운트 해제에는 **no mount** *name* **type ftp** 명령이 사용됩니다.

[**no**] **mount** *name* **type ftp server** *server-name* **path** *pathname* **status enable | status disable mode active | mode passive username** *username* **password** *password*

구문 설명

exit	mount-ftp 컨피그레이션 모드에서 빠져나와 글로벌 컨피그레이션 모드로 돌아갑니다.
ftp	마운트하는 파일 시스템이 FTP임을 지정합니다. FTP는 FTP 공유 디렉토리를 마운트할 수 있는 FTP 볼륨 마운팅 기능으로 VFS(Virtual File System)를 개선하는 Linux 커널 모듈입니다.
mode	FTP 전송 모드를 active 또는 passive로 지정합니다.
no	이미 마운트된 FTP 파일 시스템을 제거하여 액세스할 수 없도록 처리합니다.
password *password*	파일 시스템 마운팅을 위한 권한 있는 비밀번호를 식별합니다.
path *pathname*	지정한 FTP 파일 시스템 서버에 대한 디렉토리 경로 이름을 지정합니다. 경로 이름에는 공백을 포함할 수 없습니다.
server *server-name*	FTPFS 파일 시스템 서버의 사전 정의된 이름(또는 점으로 구분된 10진수 표기법의 IP 주소)을 지정합니다.
status enable/disable	파일 시스템의 상태를 마운트된 상태 또는 마운트 해제된 상태(사용 가능 또는 사용 불가능)로 식별합니다.
username *username*	파일 시스템 마운팅을 위한 권한 있는 사용자 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Mount-ftp 컨피그레이션	• 예	• 예	• 예	—	• 예
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

mount *name* **type ftp** 명령은 IFS(Installable File System)를 사용하여 지정한 네트워크 파일 시스템을 마운트합니다. 파일 시스템 API인 IFS는 보안 어플라이언스가 파일 시스템용 드라이버를 인식하여 로드하도록 지원합니다.

FTP 파일 시스템이 실제로 마운트되었는지 확인하려면 **dir all-filesystems** 명령을 사용합니다.

mount 명령으로 지정한 mount-name은 보안 어플라이언스에 이미 마운트된 파일 시스템을 참조하기 위해 다른 CLI 명령에서 사용됩니다. 예를 들어 Local Certificate Authority용 파일 스토리지를 설정하는 **database** 명령을 이용해 데이터베이스 파일을 비 플래시 스토리지에 저장하려면 마운트된 파일 시스템의 마운트 이름이 필요합니다.

참고 FTP 유형의 마운트를 만들 때 **mount** 명령을 사용하려면 FTP 서버에 UNIX 디렉토리 목록 스타일이 있어야 합니다. Microsoft FTP 서버에는 기본적으로 MS-DOS 디렉토리 목록 스타일이 있습니다.

참고 CIFS 및 FTP 파일 시스템의 마운트는 지원됩니다 (**mount** *name* **type ftp** 명령 참조.). NFS(Network File System) 볼륨의 마운트는 현재 릴리스에서 지원되지 않습니다.

예

다음 예는 *ftp://amor;chief:big-kid@myfiler02*를 *my ftp* 레이블로 마운트합니다.

```
ciscoasa(config)# mount myftp type ftp server myfiler02a path status enable username chief
password big-kid
```

관련 명령

명령	설명
debug webvpn	WebVPN 디버깅 메시지를 기록합니다.
ftp mode passive	ASA의 FTP 클라이언트와 FTP 서버 간 상호 작용을 제어합니다.

mroute

정적 멀티캐스트 경로를 구성하려면 글로벌 컨피그레이션 모드에서 **mroute** 명령을 사용합니다. 정적 멀티캐스트 경로를 제거하려면 이 명령의 **no** 형식을 사용합니다.

mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

구문 설명

dense *output_if_name*	(선택 사항) dense 모드 출력의 인터페이스 이름입니다. **dense** *output_if_name* 키워드와 인수 쌍은 SMR stub 멀티캐스트 라우팅(igmp 포워딩)에 대해서만 지원됩니다.
distance	(선택 사항) 경로의 관리 거리입니다. 거리의 값이 낮은 경로가 우선권을 갖습니다. 기본값은 0입니다.
in_if_name	mroute의 들어오는 인터페이스 이름을 지정합니다.
rpf_addr	mroute의 들어오는 인터페이스를 지정합니다. RPF address PIM neighbor, PIM join, graft, and prune 메시지가 이곳으로 전송되면 *rpf-addr* 인수는 직접 연결된 시스템의 호스트 IP 주소이거나 네트워크/서브넷 번호일 수 있습니다. 경로인 경우, 직접 연결된 시스템을 찾기 위해 유니캐스트 라우팅 테이블로부터 재귀적 조회가 수행됩니다.
smask	멀티캐스트 소스 네트워크 주소 마스크를 지정합니다.
src	멀티캐스트 소스의 IP 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 멀티캐스트 소스가 어디에 있는지를 통계적으로 구성할 수 있습니다. ASA는 유니캐스트 패킷을 특정 소스로 전송할 때 사용하는 것과 동일한 인터페이스에서 멀티캐스트 패킷을 수신할 것으로 예상합니다. 멀티캐스트 라우팅을 지원하지 않는 경로를 우회하는 등의 일부 경우에는 멀티캐스트 패킷이 유니캐스트 패킷과 다른 경로를 사용할 수 있습니다.

고정 멀티캐스트 경로가 알려지거나 재배포되지 않습니다.

멀티캐스트 경로 테이블의 내용을 표시하려면 **show mroute** 명령을 사용합니다. 실행 중인 컨피그레이션에서 mroute 명령을 표시하려면 **show running-config mroute** 명령을 사용합니다.

예

다음 예는 **mroute** 명령을 사용하여 고정 멀티캐스트 경로를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# mroute 172.16.0.0 255.255.0.0 inside
```

관련 명령

명령	설명
clear configure mroute	컨피그레이션에서 **mroute** 명령을 제거합니다.
show mroute	IPv4 멀티캐스트 라우팅 테이블을 표시합니다.
show running-config mroute	컨피그레이션에서 **mroute** 명령을 표시합니다.

mschapv2-capable

RADIUS 서버에 대한 MS-CHAPv2 인증 요청을 활성화하려면 aaa-server host 컨피그레이션 모드에서 **mschapv2-capable** 명령을 사용합니다. MS-CHAPv2를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

mschapv2-capable

no mschapv2-capable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

MS-CHAPv2는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

VPN 연결을 위해 ASA 및 RADIUS 서버 사이에 사용되는 프로토콜로 MS-CHAPv2를 활성화하려면 tunnel-group general-attributes에서 비밀번호 관리가 활성화되어 있어야 합니다. 비밀번호 관리를 활성화하면 ASA에서 RADIUS 서버로 MS-CHAPv2 인증 요청이 생성됩니다. 자세한 내용은 **password-management** 명령 설명을 참조하십시오.

터널 그룹에서 이중 인증을 사용하고 비밀번호 관리를 활성화하는 경우 기본 및 보조 인증 요청은 MS-CHAPv2 요청 속성을 포함합니다. RADIUS 서버가 MS-CHAPv2를 지원하지 않는 경우 **no mschapv2-capable** 명령을 사용하여 서버가 non-MS-CHAPv2 인증 요청을 보내도록 구성할 수 있습니다.

예

다음 예는 RADIUS 서버 authsrv1.cisco.com에 대해 MS-CHAPv2를 비활성화합니다.

```
ciscoasa(config)# aaa-server rsaradius protocol radius
ciscoasa(config-aaa-server-group)# aaa-server rsaradius (management) host
authsrv1.cisco.com
ciscoasa(config-aaa-server-host)# key secretpassword
ciscoasa(config-aaa-server-host)# authentication-port 21812
ciscoasa(config-aaa-server-host)# accounting-port 21813
ciscoasa(config-aaa-server-host)# no mschapv2-capable
```

관련 명령

명령	설명
aaa-server host	AAA 서버 그룹에 대해 AAA 서버를 식별합니다.
password-management	password-management 명령을 구성하면 ASA에서는 원격 사용자가 로그인할 때 사용자의 현재 비밀번호가 곧 만료되는지 또는 이미 만료되었는지를 알려줍니다. 그런 다음 ASA에서는 사용자에게 비밀번호를 변경할 기회를 제공합니다.
secondary-authentication-server-group	보조 AAA 서버 그룹을 지정합니다(SDI 서버 그룹은 사용 불가).

msie-proxy except-list

클라이언트 디바이스에서 로컬 바이패스에 대해 브라우저 프록시 예외 목록 설정을 구성하려면 group-policy 컨피그레이션 모드에서 **msie-proxy except-list** 명령을 입력합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

msie-proxy except-list {value *server*[*:port*] **| none}**

no msie-proxy except-list

구문 설명

none	IP 주소/호스트 이름 또는 포트가 없음을 나타내며, 예외 목록의 상속을 차단합니다.
value *server:port*	이 클라이언트 디바이스에 적용되는 MSIE 서버 및 포트의 IP 주소 또는 이름을 지정합니다. 포트 번호는 선택 사항입니다.

기본값

기본적으로 msie-proxy except-list는 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

프록시 서버 IP 주소 또는 호스트 이름과 포트 번호를 포함하는 줄은 길이가 100자 미만이어야 합니다.

프록시 설정에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide 릴리스 3.1* 또는 사용 중인 모바일 디바이스의 릴리스 정보를 참조하십시오.

예

다음 예는 IP 주소 192.168.20.1, 포트 880, 그룹 정책 FirstGroup으로 구성된 Microsoft Internet Explorer 프록시 예외 목록을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
show running-configuration group-policy	구성된 group-policy 특성의 값을 보여줍니다.
clear configure group-policy	구성된 모든 group-policy 특성을 제거합니다.

msie-proxy local-bypass

클라이언트 디바이스에 대한 브라우저 프록시 로컬 바이패스 설정을 구성하려면 group-policy 컨피그레이션 모드에서 **msie-proxy local-bypass** 명령을 입력합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

msie-proxy local-bypass {enable | disable}

no msie-proxy local-bypass {enable | disable}

구문 설명

disable	클라이언트 디바이스에 대한 브라우저 프록시 로컬 바이패스 설정을 비활성화합니다.
enable	클라이언트 디바이스에 대한 브라우저 프록시 로컬 바이패스 설정을 활성화합니다.

기본값

기본적으로 msie-proxy local-bypass는 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

프록시 설정에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide 릴리스 3.1* 또는 사용 중인 모바일 디바이스의 릴리스 정보를 참조하십시오.

예

다음 예는 그룹 정책 FirstGroup에 대해 Microsoft Internet Explorer 프록시 로컬 바이패스를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
show running-configuration group-policy	구성된 group-policy 특성의 값을 보여줍니다.
clear configure group-policy	구성된 모든 group-policy 특성을 제거합니다.

msie-proxy lockdown

이 기능을 활성화하면 AnyConnect VPN 세션 중에 브라우저의 Connections 탭이 숨겨집니다. 이 기능을 비활성화하면 Connections 탭이 그대로 표시됩니다.

AnyConnect VPN 세션 중에 Connections 탭을 숨기거나 그대로 표시하려면 group-policy 컨피그레이션 모드에서 **msie-proxy lockdown** 명령을 사용합니다.

msie-proxy lockdown [enable | disable]

구문 설명

disable	브라우저의 Connections 탭을 그대로 표시합니다.
enable	AnyConnect VPN 세션 중에 브라우저의 Connections 탭을 숨깁니다.

기본값

기본 그룹 정책에서 이 명령의 기본값은 enable입니다. 각 그룹 정책은 기본 그룹 정책에서 기본값을 상속합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
8.2(3)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 AnyConnect VPN 세션 중에 사용자 레지스트리가 임시로 변경됩니다. AnyConnect는 VPN 세션을 마치면 레지스트리를 세션 이전의 상태로 돌려놓습니다.

사용자가 프록시 서비스를 지정하거나 LAN 설정을 변경하지 못하게 하려면 이 기능을 활성화할 수 있습니다. 사용자가 이러한 설정에 액세스하지 못하게 하면 AnyConnect 세션 중에 엔드포인트 보안이 강화됩니다.

프록시 설정에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide 릴리스 3.1* 또는 사용 중인 모바일 디바이스의 릴리스 정보를 참조하십시오.

예

다음 예는 AnyConnect 세션 중에 Connections 탭을 숨깁니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

다음 예는 Connections 탭을 그대로 둡니다.

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

관련 명령

명령	설명
msie-proxy except-list	클라이언트 디바이스에서 브라우저에 대한 프록시 서버의 예외 목록을 지정합니다.
msie-proxy local-bypass	클라이언트 디바이스에 구성된 로컬 브라우저 프록시 설정을 우회합니다.
msie-proxy method	클라이언트 디바이스에 대한 브라우저 프록시 작업을 지정합니다.
msie-proxy pac-url	프록시 서버를 정의하는 프록시 자동 컨피그레이션 파일을 검색하기 위한 URL을 지정합니다.
msie-proxy server	클라이언트 디바이스에서 브라우저에 대한 프록시 서버를 구성합니다.
show running-config group-policy	실행 중인 컨피그레이션에서 그룹 정책 설정을 표시합니다.

msie-proxy method

클라이언트 디바이스에 대한 브라우저 프록시 작업("methods")을 구성하려면 group-policy 컨피그레이션 모드에서 **msie-proxy method** 명령을 입력합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

참고 이 구문을 적용할 자격에 대한 사용 지침 섹션을 참조하십시오.

구문 설명

auto-detect	클라이언트 디바이스용 브라우저에서 자동 프록시 서버 감지 사용을 활성화합니다.
no-modify	이 클라이언트 디바이스에서 브라우저의 HTTP 브라우저 프록시 서버 설정을 변경하지 않고 그대로 둡니다.
no-proxy	이 클라이언트 디바이스에서 브라우저의 HTTP 프록시 설정을 비활성화합니다.
use-pac-url	**msie-proxy pac-url** 명령으로 지정한 프록시 자동 컨피그레이션 파일 URL에서 HTTP 프록시 서버 설정을 검색하도록 브라우저에 지시합니다.
use-server	**msie-proxy server** 명령으로 구성한 값을 사용하도록 브라우저에서 HTTP 프록시 서버 설정을 지정합니다.

기본값

기본 메서드는 use-server입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.0(2)	use-pac-url 옵션이 추가되었습니다.

사용 지침

프록시 서버 IP 주소 또는 호스트 이름과 포트 번호를 포함하는 줄은 최대 100자를 포함할 수 있습니다.

이 명령은 다음 옵션의 조합을 지원합니다.

- **[no] msie-proxy method no-proxy**
- **[no] msie-proxy method no-modify**
- **[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]**

텍스트 편집기를 사용하여 브라우저용 프록시 자동 컨피그레이션(.pac) 파일을 만들 수 있습니다. .pac 파일은 URL의 내용에 따라 하나 이상의 사용할 프록시 서버를 지정하는 논리가 포함된 JavaScript 파일입니다. .pac 파일은 웹 서버에 상주합니다. **use-pac-url**을 지정하면, 브라우저는 .pac 파일을 사용하여 프록시 설정을 결정합니다. .pac 파일을 검색할 URL을 지정하려면 **msie-proxy pac-url** 명령을 사용합니다.

프록시 설정에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide 릴리스 3.1* 또는 사용 중인 모바일 디바이스의 릴리스 정보를 참조하십시오.

예

다음 예는 그룹 정책 FirstGroup에 대해 auto-detect를 Microsoft Internet Explorer 프록시 설정으로서 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

다음 예는 클라이언트 PC용 서버로서 서버 QAserver, 포트 1001을 사용하도록 그룹 정책 FirstGroup에 대해 Microsoft Internet Explorer 프록시 설정을 구성합니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server QAserver:port 1001
ciscoasa(config-group-policy)# msie-proxy method use-server
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
msie-proxy pac-url	프록시 자동 컨피그레이션 파일을 검색하기 위한 URL을 지정합니다.
msie-proxy server	클라이언트 디바이스용 브라우저 프록시 서버 및 포트를 구성합니다.
show running-configuration group-policy	구성된 group-policy 특성의 값을 보여줍니다.
clear configure group-policy	구성된 모든 group-policy 특성을 제거합니다.

msie-proxy pac-url

프록시 정보를 어디서 찾을지를 브라우저에 알려주려면 group-policy 컨피그레이션 모드에서 **msie-proxy pac-url** 명령을 입력합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

msie-proxy pac-url {**none** | **value** *url*}

no msie-proxy pac-url

구문 설명

none	URL 값이 없음을 지정합니다.
value *url*	브라우저가 사용할 프록시 서버를 정의하는 프록시 자동 컨피그레이션 파일을 가져올 수 있는 웹사이트의 URL을 지정합니다.

기본값

기본값은 none입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

요건

프록시 자동 컨피그레이션 기능을 사용하려면 원격 사용자는 Cisco AnyConnect VPN Client를 사용해야 합니다. 프록시 자동 컨피그레이션 URL의 사용을 활성화하려면 **msie-proxy method** 명령을 **use-pac-url** 옵션과 함께 구성해야 합니다.

이 명령을 사용해야 하는 이유

많은 네트워크 환경에서 웹 브라우저를 특별한 네트워크 리소스에 연결하는 HTTP 프록시를 정의합니다. 브라우저에 프록시가 지정되어 있고 클라이언트가 HTTP 트래픽을 프록시로 전달하는 경우에만 HTTP 트래픽이 네트워크 리소스에 도달할 수 있습니다. 엔터프라이즈 네트워크로 터널링할 때 필요한 프록시는 광대역 연결을 통해 인터넷에 연결할 때 또는 서드파티 네트워크에 있을 때 필요한 프록시와 다를 수 있기 때문에 SSLVPN 터널은 HTTP 프록시의 정의를 복잡하게 만듭니다.

또한 대규모 네트워크를 보유한 회사는 프록시 서버를 둘 이상 구성하고, 상황에 따라 사용자에게 선택권을 제공해야 할 수 있습니다. .pac 파일을 통해 관리자는 엔터프라이즈 전체에서 모든 클라이언트 컴퓨터가 여러 프록시 중 어떤 것을 사용해야 할지 결정하는 단일 스크립트 파일을 작성할 수 있습니다.

다음은 PAC 파일을 사용하는 방법을 보여주는 몇 가지 예입니다.

- 로드 밸런싱 목록에서 무작위로 프록시 선택
- 서버 유지 관리 일정에 맞게 시간별 또는 요일별로 돌아가며 프록시 사용
- 기본 프록시에 장애가 발생하는 경우 사용할 백업 프록시 서버 지정
- 로컬 서브넷을 기반으로 사용자 로밍을 위한 가장 가까운 프록시 지정

프록시 자동 컨피그레이션 기능 사용 방법

텍스트 편집기를 사용하여 브라우저용 프록시 자동 컨피그레이션(.pac) 파일을 만들 수 있습니다. .pac 파일은 URL의 내용에 따라 하나 이상의 사용할 프록시 서버를 지정하는 논리가 포함된 JavaScript 파일입니다. .pac 파일을 검색할 URL을 지정하려면 **msie-proxy pac-url** 명령을 사용합니다. **msie-proxy method** 명령에서 **use-pac-url**을 지정하면 브라우저는 .pac 파일을 사용하여 프록시 설정을 결정합니다.

프록시 설정에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide 릴리스 3.1* 또는 사용 중인 모바일 디바이스의 릴리스 정보를 참조하십시오.

예

다음 예는 그룹 정책 FirstGroup에 대해 URL www.example.com에서 프록시 설정을 가져오도록 브라우저를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

다음 예는 그룹 정책 FirstGroup에 대해 프록시 자동 컨피그레이션 기능을 비활성화합니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url none
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
msie-proxy method	클라이언트 디바이스에 대한 브라우저 프록시 작업("methods")을 지정합니다.
msie-proxy server	클라이언트 디바이스용 브라우저 프록시 서버 및 포트를 구성합니다.
show running-configuration group-policy	구성된 group-policy 특성의 값을 보여줍니다.
clear configure group-policy	구성된 모든 group-policy 특성을 제거합니다.

msie-proxy server

클라이언트 디바이스에 대한 브라우저 프록시 서버 및 포트를 구성하려면 group-policy 컨피그레이션 모드에서 **msie-proxy server** 명령을 입력합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

msie-proxy server {value *server*[*:port*] **| none}**

no msie-proxy server

구문 설명

none	프록시 서버에 대해 지정된 IP 주소/호스트 이름 또는 포트가 없음을 나타내며, 서버의 상속을 차단합니다.
value *server:port*	이 클라이언트 디바이스에 적용되는 MSIE 서버 및 포트의 IP 주소 또는 이름을 지정합니다. 포트 번호는 선택 사항입니다.

기본값

기본적으로 msie-proxy 서버가 지정되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

프록시 서버 IP 주소 또는 호스트 이름과 포트 번호를 포함하는 줄은 길이가 100자 미만이어야 합니다.

프록시 설정에 대한 자세한 내용은 *Cisco AnyConnect Secure Mobility Client Administrator Guide 릴리스 3.1* 또는 사용 중인 모바일 디바이스의 릴리스 정보를 참조하십시오.

예

다음 예는 그룹 정책 FirstGroup에 대해 Microsoft Internet Explorer 프록시 서버로서 포트 880을 사용하는 IP 주소 192.168.10.1을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
show running-configuration group-policy	구성된 group-policy 특성의 값을 보여줍니다.
clear configure group-policy	구성된 모든 group-policy 특성을 제거합니다.

mtu

인터페이스에 대한 MTU(Maximum Transmission Unit)를 지정하려면 글로벌 컨피그레이션 모드에서 **mtu** 명령을 사용합니다. 이더넷 인터페이스에 대해 MTU 블록 크기를 1500으로 재설정하려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 IPv4 및 IPv6 트래픽을 지원합니다.

mtu *interface_name bytes*

no mtu *interface_name bytes*

구문 설명

bytes	MTU의 바이트 수. 유효한 값의 범위는 64~9198바이트입니다(ASAv의 경우 9000).
interface_name	내부 또는 외부 네트워크 인터페이스 이름.

기본값

이더넷 인터페이스의 경우 기본 *바이트*는 1500입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	—	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

mtu 명령을 사용하면 연결에서 전송되는 데이터 크기를 설정할 수 있습니다. MTU 값보다 큰 데이터는 전송 전에 분할됩니다.

ASA는 경로를 따라 다양한 링크의 최대 허용 MTU 크기에서 호스트가 동적으로 차이를 검색하여 조정하도록 허용하는 IP 경로 MTU 검색(RFC 1191에 정의됨)을 지원합니다. 때로는 패킷이 인터페이스에 대해 설정한 MTU보다 크지만 "Don't Fragment"(DF) 비트가 설정되어 있기 때문에, ASA에서 데이터그램을 전달하지 못합니다. 네트워크 소프트웨어는 전송 호스트로 메시지를 전송하여 문제에 대해 경고합니다. 호스트는 경로를 따라 모든 링크에서 최소 패킷 크기에 맞도록 목적지로 보낼 패킷을 조각화해야 합니다.

이더넷 인터페이스용 블록에서 기본 MTU는 1500바이트입니다(최대 크기이기도 함). 이 값은 대부분의 애플리케이션에서 충분하지만, 네트워크 상태에 따라 더 낮은 값을 사용할 수 있습니다.

L2TP(Layer 2 Tunneling Protocol)를 사용할 때에는 L2TP 헤더 및 IPsec 헤더 길이에 따라 MTU 크기를 1380으로 설정하는 것이 좋습니다.

IPv6 지원 인터페이스에서 허용되는 최소 MTU는 1280바이트입니다. 그러나 인터페이스에서 IPsec이 사용되는 경우, IPsec 암호화의 오버헤드 때문에 MTU 값을 1380 미만으로 설정해서는 안 됩니다. 인터페이스를 1380바이트 미만으로 설정하면 패킷이 삭제될 수 있습니다.

예

다음 예는 인터페이스에 대해 MTU를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
ciscoasa(config)# mtu inside 8192
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

관련 명령

명령	설명
clear configure mtu	구성된 MTU(Maximum Transmission Unit) 값을 모든 인터페이스에서 지웁니다.
show running-config mtu	현재의 MTU 블록 크기를 표시합니다.

mtu cluster

클러스터 제어 링크의 MTU를 설정하려면 글로벌 컨피그레이션 모드에서 **mtu cluster** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

mtu cluster *bytes*

no mtu cluster [*bytes*]

구문 설명

bytes	클러스터 제어 링크 인터페이스의 MTU를 지정합니다(64~65,535바이트). 기본 MTU는 1500바이트입니다.

명령 기본값

기본 MTU는 1500바이트입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

MTU는 1600바이트 이상으로 설정하는 것이 좋습니다. 이 경우 **jumbo-frame reservation** 명령을 사용하여 점보 프레임 예약을 활성화해야 합니다.

이 명령은 글로벌 컨피그레이션 명령일 뿐만 아니라 유닛 간에 복제되지 않은 부트스트랩 컨피그레이션의 일부입니다.

예

다음 예는 클러스터 제어 링크 MTU를 9000바이트로 설정합니다.

```
ciscoasa(config)# mtu cluster 9000
```

관련 명령

명령	설명
cluster-interface	클러스터 제어 링크 인터페이스를 식별합니다.
jumbo frame-reservation	점보 이더넷 프레임의 사용을 활성화합니다.

multicast boundary

관리 가능한 범위의 멀티캐스트 주소에 대한 멀티캐스트 경계를 구성하려면 인터페이스 컨피그레이션 모드에서 **multicast boundary** 명령을 사용합니다. 경계를 제거하려면 이 명령의 **no** 형식을 사용합니다. 멀티캐스트 경계는 멀티캐스트 데이터 패킷 흐름을 제한하고 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있게 합니다.

multicast boundary *acl* [**filter-autorp**]

no multicast boundary *acl* [**filter-autorp**]

구문 설명

acl	액세스 목록 이름 또는 번호를 지정합니다. 액세스 목록은 경계의 영향을 받는 주소 범위를 정의합니다. 이 명령에서는 표준 ACL만 사용하십시오. 확장 ACL은 지원되지 않습니다.
filter-autorp	경계 ACL에 의해 거부되는 Auto-RP 메시지를 필터링합니다. 지정하지 않으면 모든 Auto-RP 메시지가 통과됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

acl 인수로 정의한 범위에서 멀티캐스트 그룹 주소를 필터링하기 위해 인터페이스에서 관리적으로 범위가 지정된 경계를 구성하려면 이 명령을 사용합니다. 표준 액세스 목록은 영향을 받는 주소의 범위를 정의합니다. 이 명령을 구성하면, 멀티캐스트 데이터 패킷이 어떤 방향으로도 경계를 넘어 흐를 수 없습니다. 멀티캐스트 데이터 패킷의 흐름을 제한하면 서로 다른 관리 도메인에서 동일한 멀티캐스트 그룹 주소를 재사용할 수 있습니다.

filter-autorp 키워드를 구성하면, 관리적으로 범위가 지정된 경계에서는 또한 Auto-RP 검색 및 알림 메시지를 검토하고, 경계 ACL에서 거부한 Auto-RP 패킷에서 모든 Auto-RP 그룹 범위 알림을 제거합니다. Auto-RP 그룹 범위 알림은 Auto-RP 그룹 범위의 모든 주소가 경계 ACL에 의해 허용된 경우에만 경계에서 허용 및 통과됩니다. 주소가 하나라도 허용되지 않은 경우 전체 그룹 범위가 필터링되고 Auto-RP 메시지가 전달되기 전에 Auto-RP 메시지에서 삭제됩니다.

예

다음 예는 관리적으로 범위가 지정된 모든 주소에 대해 경계를 설정하고 Auto-RP 메시지를 필터링합니다.

```
ciscoasa(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
ciscoasa(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# multicast boundary boundary_test filter-autorp
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

multicast-routing

ASA에서 IP 멀티캐스트 라우팅을 활성화하려면 글로벌 컨피그레이션 모드에서 **multicast routing** 명령을 사용합니다. IP 멀티캐스트 라우팅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

multicast-routing

no multicast-routing

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

multicast-routing 명령은 모든 인터페이스에서 기본적으로 PIM 및 IGMP를 활성화합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

multicast-routing 명령은 모든 인터페이스에서 PIM 및 IGMP를 활성화합니다.

참고 PIM은 PAT에서 지원되지 않습니다. PIM 프로토콜은 포트를 사용하지 않고 PAT는 포트를 사용하는 프로토콜에서만 작동합니다.

보안 어플라이언스가 PIM RP인 경우 보안 어플라이언스의 변환되지 않은 외부 주소를 RP 주소로 사용합니다.

멀티캐스트 라우팅 테이블의 엔트리 개수는 시스템의 RAM에 의해 제한됩니다. 표 12-1에는 보안 어플라이언스의 RAM을 기준으로 특정 멀티캐스트 테이블에 대한 최대 엔트리 개수가 나열되어 있습니다. 이 제한에 도달하면 새로운 엔트리가 삭제됩니다.

표 12-1 멀티캐스트 테이블 엔트리 제한

테이블	16MB	128MB	128+ MB
MFIB	1000	3000	5000
IGMP Groups	1000	3000	5000
PIM Routes	3000	7000	12000

예

다음 예는 ASA에서 IP 멀티캐스트 라우팅을 활성화합니다.

```
ciscoasa(config)# multicast-routing
```

관련 명령

명령	설명
igmp	인터페이스에서 IGMP를 활성화합니다.
pim	인터페이스에서 PIM을 활성화합니다.

mus

ASA가 WSA를 식별하는 IP 범위 및 인터페이스를 지정하려면 글로벌 컨피그레이션 모드에서 **mus** 명령을 사용합니다. 서비스를 끄려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 IPv4 및 IPv6 트래픽을 지원합니다. 지정된 서브넷 및 인터페이스에 있는 WSA만 등록됩니다.

mus *IPv4 address IPv4 mask interface_name*

no mus *IPv4 address IPv4 mask interface_name*

참고 이 명령이 예상대로 작동하려면 AnyConnect Secure Mobility Client용 AnyConnect Secure Mobility 라이센싱 지원을 제공하는 AsyncOS for Web 버전 7.0 릴리스가 필요합니다. 또한 AnyConnect Secure Mobility, ASA 8.3 및 ASDM 6.3을 지원하는 AnyConnect 릴리스도 필요합니다.

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

다음 명령이 가능합니다.

- A.B.C.D - ASA에 액세스할 수 있는 WSA의 IP 주소.
- host - 클라이언트는 가상의 호스트에 요청을 전송하여 Web Security Appliance에 대한 연결을 주기적으로 확인합니다. 기본적으로 가상의 호스트 URL은 mus.cisco.com입니다. AnyConnect Security Mobility가 활성화되면 Web Security Appliance는 가상의 호스트로 전송될 예정인 요청을 가로채서 클라이언트에 회신합니다.
- password - WSA 비밀번호를 구성합니다.
- server - WSA 서버를 구성합니다.

예

다음 예는 1.2.3.x 서브넷의 WSA 서버가 *inside* 인터페이스의 보안 모빌리티 솔루션에 액세스하도록 허용합니다.

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

관련 명령

명령	설명
mus password	AnyConnect Secure Mobility 통신을 위한 공유 암호를 설정합니다.
mus server	ASA가 WSA 통신을 위해 수신 대기하는 포트를 지정합니다.
show webvpn mus	활성 WSA 연결 보안 어플라이언스에 대한 정보를 표시합니다.

mus host

ASA에서 MUS 호스트 이름을 지정하려면 글로벌 컨피그레이션 모드에서 **mus host** 명령을 입력합니다. 이것은 ASA에서 AnyConnect 클라이언트로 전송되는 원격 분석 URL입니다. AnyConnect 클라이언트는 이 URL을 사용하여 MUS 관련 서비스용 사설 네트워크에서 WSA에 접속합니다. 이 명령으로 입력한 명령을 제거하려면 **no mus host** 명령을 사용합니다.

mus host *host name*

no mus host

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

특정 포트에 대해 AnyConnect Secure Mobility를 활성화할 수 있습니다. WSA 포트 값의 범위는 1~21000입니다. 명령에서 포트를 지정하지 않으면 포트 11999가 사용됩니다.

이 명령을 실행하기 전에 AnyConnect Secure Mobility 공유 암호를 구성해야 합니다.

참고 이 명령이 예상대로 작동하려면 AnyConnect Secure Mobility Client용 AnyConnect Secure Mobility 라이센싱 지원을 제공하는 AsyncOS for Web 버전 7.0 릴리스가 필요합니다. 또한 AnyConnect Secure Mobility, ASA 8.3 및 ASDM 6.3을 지원하는 AnyConnect 릴리스도 필요합니다.

예

다음 예는 AnyConnect Secure Mobility 호스트 및 WebVPN 명령 하위 모드를 입력하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mus 0.0.0.0 0.0.0.0 inside
ciscoasa(config-webvpn)# mus password abcdefgh123
ciscoasa(config-webvpn)# mus server enable 960 # non-default port
ciscoasa(config-webvpn)# mus host mus.cisco.com
```

관련 명령

명령	설명
mus	ASA가 WSA를 식별하는 IP 범위 및 인터페이스를 지정합니다.
mus password	AnyConnect Secure Mobility 통신을 위한 공유 암호를 설정합니다.
show webvpn mus	활성 WSA 연결 보안 어플라이언스에 대한 정보를 표시합니다.

mus password

AnyConnect Secure Mobility 통신을 위한 공유 암호를 설정하려면 글로벌 컨피그레이션 모드에서 **mus password** 명령을 입력합니다. 공유 암호를 제거하려면 **no mus password** 명령을 사용합니다.

mus password

no mus password

참고 이 명령이 예상대로 작동하려면 AnyConnect Secure Mobility Client용 AnyConnect Secure Mobility 라이센싱 지원을 제공하는 AsyncOS for Web 버전 7.0 릴리스가 필요합니다. 또한 AnyConnect Secure Mobility, ASA 8.3 및 ASDM 6.3을 지원하는 AnyConnect 릴리스도 필요합니다.

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

유효한 비밀번호는 정규식 [0-9, a-z, A-Z,:;_/-]{8,20}으로 정의됩니다. 공유 암호의 전체 길이는 최소 8자, 최대 20자입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

이 WebVPN 하위 모드에서는 WebVPN용 전역 설정을 구성할 수 있습니다. AnyConnect Secure Mobility 통신을 위한 공유 암호를 설정할 수 있습니다.

예

다음 예는 AnyConnect Secure Mobility 비밀번호 및 WebVPN 명령 하위 모드를 입력하는 방법을 보여줍니다.

```
ciscoasa(config)# mus password <password_string>
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
mus	ASA가 WSA를 식별하는 IP 범위 및 인터페이스를 지정합니다.
mus server	ASA가 WSA 통신을 위해 수신 대기하는 포트를 지정합니다.
show webvpn mus	활성 WSA 연결 보안 어플라이언스에 대한 정보를 표시합니다.

mus server

ASA가 WSA 통신을 수신 대기하는 포트를 지정하려면 글로벌 컨피그레이션 모드에서 **mus server** 명령을 입력합니다. 이 명령으로 입력한 명령을 제거하려면 **no mus server** 명령을 사용합니다.

mus server enable

no mus server enable

참고 이 명령이 예상대로 작동하려면 AnyConnect Secure Mobility Client용 AnyConnect Secure Mobility 라이센싱 지원을 제공하는 AsyncOS for Web 버전 7.0 릴리스가 필요합니다. 또한 AnyConnect Secure Mobility, ASA 8.3 및 ASDM 6.3을 지원하는 AnyConnect 릴리스도 필요합니다.

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

AnyConnect Secure Mobility 서비스에서 사용하는 포트를 지정해야 합니다. ASA와 WSA 간 통신은 관리자가 1~21000 범위의 값으로 지정한 포트에서 안전한 SSL 연결을 통해 이루어집니다.

이 명령을 실행하기 전에 AnyConnect Secure Mobility 공유 암호를 구성해야 합니다.

예

다음 예는 AnyConnect Secure Mobility 비밀번호 및 WebVPN 명령 하위 모드를 입력하는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# mus server enable?
webvpn mode commands/options
    port Configure WSA port
ciscoasa(config-webvpn)# mus server enable port 12000
```

관련 명령

명령	설명
mus	ASA가 WSA를 식별하는 IP 범위 및 인터페이스를 지정합니다.
mus password	AnyConnect Secure Mobility 통신을 위한 공유 암호를 설정합니다.
show webvpn mus	활성 WSA 연결 보안 어플라이언스에 대한 정보를 표시합니다.

파트 3

N~R 명령

13 장

nac-authentication-server-group through num-packets 명령

nac-authentication-server-group(deprecated)

Network Admission Control 상태 검증에 사용할 인증 서버의 그룹을 식별하려면, tunnel-group general-attributes 컨피그레이션 모드에서 **nac-authentication-server-group** 명령을 사용합니다. 기본 원격 액세스 그룹에서 인증 서버 그룹을 상속하려면, 상속할 대체 그룹 정책에 액세스한 다음 이 명령의 **no** 형식을 사용합니다.

nac-authentication-server-group *server-group*

no nac-authentication-server-group

구문 설명

server-group	**aaa-server host** 명령을 사용하여 ASA에서 구성한 상태 검증 서버 그룹의 이름입니다. 이름은 해당 명령에서 지정한 server-tag 변수와 일치해야 합니다.

기본값

이 명령에는 인수나 키워드가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.0(1)	이 명령은 사용이 중단되었습니다. nac-policy-nac-framework 컨피그레이션 모드의 **authentication-server-group** 명령이 이를 대체했습니다.

사용 지침

NAC를 지원하려면 Access Control Server를 하나 이상 구성합니다. ACS 그룹의 이름을 지정하려면 **aaa-server** 명령을 사용합니다. 그런 다음 서버 그룹에 대한 동일한 이름을 사용하여 **nac-authentication-server-group** 명령을 사용합니다.

예

다음 예는 acs-group1을 NAC 상태 검증에 사용할 인증 서버 그룹으로 식별합니다.

```
ciscoasa(config-group-policy)# nac-authentication-server-group acs-group1
ciscoasa(config-group-policy)
```

다음 예는 기본 원격 액세스 그룹에서 인증 서버 그룹을 상속합니다.

```
ciscoasa(config-group-policy)# no nac-authentication-server-group
ciscoasa(config-group-policy)
```

관련 명령

명령	설명
aaa-server	AAA 서버 또는 그룹의 레코드를 만들고 호스트별 AAA 서버 특성을 설정합니다.
debug eap	NAC 메시징을 디버그하기 위해 EAP 이벤트의 로깅을 활성화합니다.
debug eou	NAC 메시징을 디버그하기 위해 EAPoUDP(EAP over UDP) 이벤트의 로깅을 활성화합니다.
debug nac	NAC 이벤트의 로깅을 활성화합니다.
nac	그룹 정책에서 Network Admission Control을 활성화합니다.

nac-policy

Cisco NAC(Network Admission Control) 정책을 만들거나 액세스하려면 글로벌 컨피그레이션 모드에서 **nac-policy** 명령을 사용합니다. 컨피그레이션에서 NAC 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

nac-policy *nac-policy-name* **nac-framework**

[**no**] **nac-policy** *nac-policy-name* **nac-framework**

구문 설명

nac-policy-name	NAC 정책의 이름입니다. NAC 정책의 이름을 지정하려면 최대 64자의 문자열을 입력합니다. **show running-config nac-policy** 명령은 이미 보안 어플라이언스에 있는 각 NAC 정책의 이름과 컨피그레이션을 표시합니다.
nac-framework	원격 호스트용 네트워크 액세스 정책을 제공할 수 있도록 NAC 프레임워크의 사용을 지정합니다. ASA용 NAC Framework 서비스를 제공하려면 네트워크에 Cisco Access Control Server가 있어야 합니다. 이 유형을 지정하면, 현재 config--nac-policy-nac-framework 컨피그레이션 모드에 있다는 프롬프트가 표시됩니다. 이 모드에서는 NAC Framework 정책을 구성할 수 있습니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.
9.1(2)	이 명령은 사용이 중단되었습니다.

사용 지침

그룹 정책에 할당할 각 NAC Appliance에 대해 이 명령을 한 번 사용합니다. 그런 다음 **nac-settings** 명령을 사용하여 NAC 정책을 해당되는 각 그룹 정책에 할당합니다. IPsec 또는 Cisco AnyConnect VPN 터널을 설정하면, ASA에서는 사용 중인 그룹 정책과 연결된 NAC 정책을 적용합니다.

NAC 정책이 하나 이상의 그룹 정책에 이미 할당된 경우 **no nac-policy** *name* 명령을 사용하여 제거할 수 없습니다.

예

다음 명령은 nac-framework1이라는 NAC Framework 정책을 만들고 액세스합니다.

```
ciscoasa(config)# nac-policy nac-framework1 nac-framework
ciscoasa(config-nac-policy-nac-framework)
```

다음 명령은 nac-framework1이라는 NAC Framework 정책을 제거합니다.

```
ciscoasa(config)# no nac-policy nac-framework1
ciscoasa(config-nac-policy-nac-framework)
```

관련 명령

명령	설명
show running-config nac-policy	ASA에 대한 각 NAC 정책의 컨피그레이션을 표시합니다.
show nac-policy	ASA에 대한 NAC 정책 사용 통계를 표시합니다.
clear nac-policy	NAC 정책 사용 통계를 재설정합니다.
nac-settings	NAC 정책을 그룹 정책에 할당합니다.
clear configure nac-policy	실행 중인 컨피그레이션에서 그룹 정책에 할당된 것을 제외한 모든 NAC 정책을 제거합니다.

nac-settings

NAC 정책을 그룹 정책에 할당하려면 그룹 정책 컨피그레이션 모드에서 **nac-settings** 명령을 사용합니다.

nac-settings {**value** *nac-policy-name* | **none**}

[**no**] **nac-settings** {**value** *nac-policy-name* | **none**}

구문 설명

nac-policy-name	그룹 정책에 할당할 NAC 정책입니다. 이름을 지정한 NAC 정책이 ASA의 컨피그레이션에 있어야 합니다. **show running-config nac-policy** 명령은 각 NAC 정책의 이름과 컨피그레이션을 표시합니다.
none	그룹 정책에서 *nac-policy-name*을 제거하고 이 그룹 정책에 대해 NAC 정책을 사용하지 못하게 합니다. 그룹 정책은 기본 그룹 정책에서 nac-settings 값을 상속하지 않습니다.
value	이름을 지정할 NAC 정책을 그룹 정책에 할당합니다.

기본값

이 명령에는 인수나 키워드가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.
9.1(2)	이 명령은 사용이 중단되었습니다.

사용 지침

NAC 정책의 이름과 유형을 지정한 다음 NAC 정책을 그룹 정책에 할당하려면 **nac-policy** 명령을 사용합니다.

show running-config nac-policy 명령은 각 NAC 정책의 이름과 컨피그레이션을 표시합니다.

사용자가 NAC 정책을 그룹 정책에 할당하면 ASA에서는 자동으로 그룹 정책에 대해 NAC를 활성화합니다.

예

다음 명령은 그룹 정책에서 *nac-policy-name*을 제거합니다. 그룹 정책은 기본 그룹 정책에서 *nac-settings* 값을 상속합니다.

```
ciscoasa(config-group-policy)# no nac-settings
ciscoasa(config-group-policy)
```

다음 명령은 그룹 정책에서 *nac-policy-name*을 제거하고 이 그룹 정책에 대해 NAC 정책을 사용하지 못하게 합니다. 그룹 정책은 기본 그룹 정책에서 nac-settings 값을 상속하지 않습니다.

```
ciscoasa(config-group-policy)# nac-settings none
ciscoasa(config-group-policy)
```

관련 명령

명령	설명
nac-policy	Cisco NAC 정책을 만들고 액세스하며, 해당 유형을 지정합니다.
show running-config nac-policy	ASA에 대한 각 NAC 정책의 컨피그레이션을 표시합니다.
show nac-policy	ASA에 대한 NAC 정책 사용 통계를 표시합니다.
show vpn-session_summary.db	숫자 IPsec, WebVPN 및 NAC 세션을 표시합니다.
show vpn-session.db	NAC 결과를 비롯하여 VPN 세션에 대한 정보를 표시합니다.

name

이름을 IP 주소와 연결하려면 글로벌 컨피그레이션 모드에서 **name** 명령을 사용합니다. 텍스트 이름의 사용을 비활성화하되 컨피그레이션에서는 제거하지 않으려면 이 명령의 **no** 형식을 사용합니다.

name *ip_address name* [**description** *text*]]

no name *ip_address* [*name* [**description** *text*]]

구문 설명

description	(선택 사항) IP 주소 이름에 대한 설명을 지정합니다.
ip_address	명명된 호스트의 IP 주소를 지정합니다.
name	IP 주소에 할당된 이름을 지정합니다. a~z, A~Z, 0~9, 대시 또는 밑줄 문자를 사용해야 하며, *name*은 63자 이하여야 합니다. 또한 *name*은 숫자로 시작할 수 없습니다.
text	설명에 대한 텍스트를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.0(4)	설명을 선택 사항으로 포함하도록 이 명령이 개선되었습니다.
8.3(1)	**nat** 명령 또는 **access-list** 명령에서 더 이상 명명된 IP 주소를 사용할 수 없습니다. 대신 **object network** 이름을 사용해야 합니다. 객체 그룹의 **network-object** 명령에서 **object network** 이름을 사용할 수 있지만, **name** 명령으로 지정한 명명된 IP 주소도 여전히 사용할 수 있습니다.

사용 지침

이름과 IP 주소의 연결을 활성화하려면 **names** 명령을 사용합니다. 하나의 IP 주소에는 하나의 이름만 연결할 수 있습니다.

먼저 **names** 명령을 사용한 다음 **name** 명령을 사용해야 합니다. **names** 명령을 사용한 후 **write memory** 명령을 사용하기 전에 **name** 명령을 사용합니다.

name 명령을 사용하면 IP 주소에 대한 텍스트 이름 및 맵 텍스트 문자열로 호스트를 식별할 수 있습니다. **no name** 명령을 사용하면 텍스트 이름의 사용을 비활성화하되 컨피그레이션에서는 제거하지 않을 수 있습니다. 컨피그레이션에서 이름의 목록을 지우려면 **clear configure name** 명령을 사용합니다.

name 값의 표시를 비활성화하려면 **no names** 명령을 사용합니다.

name 및 **names** 명령 모두 컨피그레이션에 저장됩니다.

name 명령으로는 이름을 네트워크 마스크에 할당할 수 없습니다. 예를 들면 다음 명령은 거부될 수 있습니다.

```
ciscoasa(config)# name 255.255.255.0 class-C-mask
```

참고 마스크가 필요한 명령 중에는 이름을 허용된 네트워크 마스크로 처리할 수 있는 명령이 없습니다.

예

다음 예는 **names** 명령으로 **name** 명령의 사용을 활성화할 수 있음을 보여줍니다. **name** 명령에서는 192.168.42.3을 가리키는 데 **sa_inside**를 사용하고 209.165.201.3을 가리키는 데 **sa_outside**를 사용합니다. IP 주소를 네트워크 인터페이스에 할당할 때 **ip address** 명령에서 이러한 이름을 사용할 수 있습니다. **no names** 명령을 사용하면 **name** 명령 값이 표시되지 않습니다. **names** 명령을 연속해서 다시 사용하면 **name** 명령 값이 다시 표시됩니다.

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside

ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224

ciscoasa(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224

ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224
```

관련 명령

명령	설명
clear configure name	컨피그레이션에서 이름의 목록을 지웁니다.
names	이름과 IP 주소의 연결을 활성화합니다.
show running-config name	IP 주소와 연결된 이름을 표시합니다.

name(dynamic-filter blacklist or whitelist)

Botnet Traffic Filter 블랙리스트 또는 화이트리스트에 도메인 이름을 추가하려면 dynamic-filter blacklist or whitelist 컨피그레이션 모드에서 **name** 명령을 사용합니다. 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다. 고정 데이터베이스에서는 블랙리스트 또는 화이트리스트에 추가할 도메인 이름 또는 IP 주소로 동적 데이터베이스를 확장할 수 있습니다.

name *domain_name*

no name *domain_name*

구문 설명

domain_name	블랙리스트에 이름을 추가합니다. 여러 엔트리에 대해 이 명령을 여러 번 입력할 수 있습니다. 최대 1,000개의 블랙리스트 엔트리를 추가할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Dynamic-filter blacklist or whitelist 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

dynamic-filter whitelist or blacklist 컨피그레이션 모드로 들어가면 **address** 및 **name** 명령을 사용하여, 화이트리스트에서 좋은 이름으로 태그하거나 블랙리스트에서 나쁜 이름으로 태그할 도메인 이름 또는 IP 주소(호스트 또는 서브넷)를 수동으로 입력할 수 있습니다.

여러 엔트리에 대해 이 명령을 여러 번 입력할 수 있습니다. 최대 1,000개의 블랙리스트 엔트리 및 1,000개의 화이트리스트 엔트리를 추가할 수 있습니다.

고정 데이터베이스에 도메인 이름을 추가하면, ASA에서는 1분간 기다린 후 해당 도메인 이름에 대한 DNS 요청을 전송하고 도메인 이름/IP 주소 쌍을 *DNS 호스트 캐시*에 추가합니다(이 작업은 백그라운드 프로세스가 아니며 ASA를 계속해서 구성하는 데 영향을 주지 않습니다).

ASA에 대해 구성된 도메인 이름 서버가 없거나 사용 불가능한 경우, 대신 Botnet Traffic Filter 스누핑과 함께 DNS 패킷 검사를 활성화할 수 있습니다(**inspect dns dynamic-filter-snooping** 명령 참조). DNS 스누핑을 사용하는 경우 감염된 호스트가 고정 데이터베이스의 특정 이름에 대해 DNS 요청을 전송하면 ASA는 DNS 패킷 내부에서 도메인 이름 및 연결된 IP 주소를 찾아보고, 이름과 IP 주소를 DNS 역방향 조회 캐시에 추가합니다. DNS 역방향 조회 캐시에 대한 자세한 내용은 **inspect dns dynamic-filter-snooping** 명령을 참조하십시오.

DNS 호스트 캐시의 엔트리는 DNS 서버에서 제공하는 TTL(Time to Live) 값을 갖습니다. 허용되는 최대 TTL 값은 1일(24시간)입니다. DNS 서버가 더 큰 TTL을 제공하면 최대 1일로 잘리게 됩니다.

DNS 호스트 캐시의 경우 엔트리가 시간 초과되면 ASA에서는 주기적으로 엔트리의 새로 고침을 요청합니다.

예

다음 예는 블랙리스트 및 화이트리스트용 엔트리를 만듭니다.

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

관련 명령

명령	설명
address	블랙리스트 또는 화이트리스트에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 Botnet Traffic Filter 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	Botnet Traffic Filter 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	ASA에서 DNS 서버에 DNS 요청을 전송하여 지원되는 명령에 대한 이름 조회를 수행하도록 합니다.
dns server-group	ASA용 DNS 서버를 식별합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 편집합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 수동으로 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 수동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않는 경우 트래픽의 클래스 또는 모든 트래픽에 대해 Botnet Traffic Filter를 활성화합니다.
dynamic-filter updater-client enable	동적 데이터베이스의 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스의 사용을 활성화합니다.
dynamic-filter whitelist	Botnet Traffic Filter 화이트리스트를 편집합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑과 함께 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 Botnet Traffic Filter 규칙을 보여줍니다.
show dynamic-filter data	동적 데이터베이스를 마지막으로 다운로드한 시기, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등 동적 데이터베이스에 대한 정보를 보여줍니다.

명령	설명
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 보여줍니다. 또는 **detail** 키워드를 사용하는 경우 실제 IP 주소와 이름을 보여줍니다.
show dynamic-filter reports	상위 10개 봇넷 사이트, 포트 및 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결의 수 및 그러한 연결 중 화이트리스트, 블랙리스트 및 그레이리스트와 일치하는 수를 보여줍니다.
show dynamic-filter updater-client	서버 IP 주소, ASA에서 서버에 연결할 다음 시간, 마지막으로 설치된 데이터베이스 버전 등 업데이터 서버에 대한 정보를 보여줍니다.
show running-config dynamic-filter	Botnet Traffic Filter 실행 중인 컨피그레이션을 보여줍니다.

nameif

인터페이스용 이름을 제공하려면 인터페이스 컨피그레이션 모드에서 **nameif** 명령을 사용합니다. 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다. ASA에서는 모든 컨피그레이션 명령에 인터페이스 유형 및 ID(예: gigabitethernet0/1) 대신 인터페이스 이름이 사용됩니다. 따라서 트래픽이 인터페이스를 통과하려면 인터페이스 이름이 필요합니다.

nameif *name*

no nameif

구문 설명

name	길이가 최대 48자인 이름을 설정합니다. 이름은 대/소문자를 구분하지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 글로벌 컨피그레이션 명령에서 인터페이스 컨피그레이션 모드 명령으로 변경되었습니다.

사용 지침

하위 인터페이스의 경우 **nameif** 명령을 입력하기 전에 **vlan** 명령으로 VLAN을 할당해야 합니다.

이 명령을 새 값과 함께 다시 입력하여 이름을 변경할 수 있습니다. **no** 형식은 입력하지 마십시오. 그러면 해당 이름을 참조하는 모든 명령이 삭제됩니다.

예

다음 명령은 두 인터페이스의 이름을 "inside" 및 "outside"로 구성합니다.

```
ciscoasa(config)# interface gigabitethernet0/1
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 gigabitethernet0/0
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 xlate	연결이 재설정되도록 기존 연결의 모든 변환을 재설정합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드로 들어갑니다.
security-level	인터페이스에 대한 보안 수준을 설정합니다.
vlan	하위 인터페이스에 VLAN ID를 할당합니다.

names

이름과 IP 주소의 연결을 활성화하려면 글로벌 컨피그레이션 모드에서 **names** 명령을 사용합니다. 하나의 IP 주소에는 하나의 이름만 연결할 수 있습니다. **name** 값의 표시를 비활성화하려면 **no names** 명령을 사용합니다.

names

no names

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이름과 IP 주소의 연결을 활성화하려면 **names** 명령을 사용합니다. 하나의 IP 주소에는 하나의 이름만 연결할 수 있습니다.

먼저 **names** 명령을 사용한 다음 **name** 명령을 사용해야 합니다. **names** 명령을 사용한 후 **write memory** 명령을 사용하기 전에 **name** 명령을 사용합니다.

name 값의 표시를 비활성화하려면 **no names** 명령을 사용합니다.

name 및 **names** 명령 모두 컨피그레이션에 저장됩니다.

예

다음 예는 **names** 명령으로 **name** 명령의 사용을 활성화할 수 있음을 보여줍니다. **name** 명령에서는 192.168.42.3을 가리키는 데 **sa_inside**를 사용하고 209.165.201.3을 가리키는 데 **sa_outside**를 사용합니다. IP 주소를 네트워크 인터페이스에 할당할 때 **ip address** 명령에서 이러한 이름을 사용할 수 있습니다. **no names** 명령을 사용하면 **name** 명령 값이 표시되지 않습니다. **names** 명령을 연속해서 다시 사용하면 **name** 명령 값이 다시 표시됩니다.

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside

ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
```

```
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224

ciscoasa(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224

ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224
```

관련 명령

명령	설명
clear configure name	컨피그레이션에서 이름의 목록을 지웁니다.
name	이름과 IP 주소를 연결합니다.
show running-config name	IP 주소와 연결된 이름의 목록을 표시합니다.
show running-config names	IP 주소 대 이름 변환을 표시합니다.

name-separator

특정 문자를 이메일과 VPN 사용자 이름 및 비밀번호 사이의 구분자로 지정하려면 해당되는 이메일 프록시 모드에서 **name-separator** 명령을 사용합니다. 기본값인 ":"으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

name-separator [*symbol*]

no name-separator

구문 설명

symbol	(선택 사항) 이메일과 VPN 사용자 이름 및 비밀번호를 구분하는 문자입니다. "@,"(앳) "|"(파이프), ":"(콜론), "#"(해시), ","(쉼표) 및 ";"(세미콜론) 중에서 선택할 수 있습니다.

기본값

기본값은 ":"(콜론)입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Pop3s	• 예	—	• 예	—	—
Imap4s	• 예	—	• 예	—	—
Smtps	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이름 구분 기호는 서버 구분 기호와 달라야 합니다.

예

다음 예는 POP3S의 이름 구분 기호로 해시(#)를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# name-separator #
```

관련 명령

명령	설명
server-separator	이메일 및 서버 이름을 구분합니다.

name-server

하나 이상의 DNS 서버를 식별하려면 dns server-group 컨피그레이션 모드에서 **name-server** 명령을 사용합니다. 하나 이상의 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다. ASA에서는 DNS를 사용하여 SSL VPN 컨피그레이션 또는 인증서 컨피그레이션의 서버 이름을 확인합니다(지원되는 명령 목록은 "사용 지침" 참조). 서버 이름(예: AAA)을 정의하는 다른 기능은 DNS 확인을 지원하지 않습니다. IP 주소를 입력하거나 **name** 명령을 사용하여 IP 주소에 대한 이름을 수동으로 확인해야 합니다.

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

구문 설명

ip_address	DNS 서버 IP 주소를 지정합니다. 최대 6개의 주소를 별도의 명령으로 지정할 수도 있고, 편의를 위해 6개의 주소를 공백으로 구분하여 한 명령으로 지정할 수 있습니다. 한 명령으로 여러 서버를 입력하면 ASA에서는 컨피그레이션에 각 서버를 별도의 명령으로 저장합니다. ASA는 응답을 받을 때까지 각 DNS 서버를 순서대로 시도합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
dns server-group 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

DNS 조회를 활성화하려면 dns server-group 컨피그레이션 모드에서 **domain-name** 명령을 구성합니다. DNS 조회를 활성화하지 않으면 DNS 서버가 사용되지 않습니다.

DNS 확인을 지원하는 SSL VPN 명령에는 다음이 포함됩니다.

- **server (pop3s)**
- **server (imap4s)**
- **server (smtps)**
- **port-forward**
- **url-list**

DNS 확인을 지원하는 인증서 명령에는 다음이 포함됩니다.

- **enrollment url**
- **url**

name 명령을 사용하여 이름과 IP 주소를 수동으로 입력할 수 있습니다.

예

다음 예는 3개의 DNS 서버를 "dnsgroup1" 그룹에 추가합니다.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

ASA는 다음과 같이 별도의 명령으로 컨피그레이션을 저장합니다.

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

두 개의 서버를 더 추가하려면 하나의 명령으로 입력할 수 있습니다.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

dns 서버 그룹 컨피그레이션을 확인하려면 글로벌 컨피그레이션 모드에서 **show running-config dns** 명령을 입력합니다.

```
ciscoasa(config)# show running-config dns
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
name-server 10.5.1.1
name-server 10.8.3.8
...
```

또는 별도의 두 명령으로 입력할 수 있습니다.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# name-server 10.5.1.1
ciscoasa(config)# name-server 10.8.3.8
```

여러 서버를 삭제하려면 여러 명령으로 입력할 수도 있고 다음과 같이 하나의 명령으로 입력할 수도 있습니다.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# no name-server 10.5.1.1 10.8.3.8
```

관련 명령

명령	설명
domain-name	기본 도메인 이름을 설정합니다.
retries	ASA에서 응답을 받지 못할 때 DNS 서버 리스트를 재시도할 횟수를 지정합니다.
timeout	다음 DNS 서버를 시도하기까지 대기하는 시간을 지정합니다.
show running-config dns server-group	하나 또는 기존의 모든 dns-server-group 컨피그레이션을 보여줍니다.

nat(global)

IPv4 또는 IPv6에 대해 Twice NAT를 구성하거나 IPv4와 IPv6 간에 Twice NAT를 구성하려면 (NAT64) 글로벌 컨피그레이션 모드에서 **nat** 명령을 사용합니다. Twice NAT 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

고정 NAT의 경우:

nat [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}]
source static {*real_obj* | **any**} {*mapped_obj* | **interface** [**ipv6**] | **any**}}
[**destination static** {*mapped_obj* | **interface** [**ipv6**]} {*real_obj* | **any**}]
[**service** {*real_src_mapped_dest_svc_obj* | **any**} *mapped_src_real_dest_svc_obj*] [**net-to-net**]
[**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*]

no nat [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}]
source static {*real_obj* | **any**} {*mapped_obj* | **interface** [**ipv6**] | **any**}}
[**destination static** {*mapped_obj* | **interface** [**ipv6**]} {*real_obj* | **any**}]
[**service** {*real_src_mapped_dest_svc_obj* | **any**} *mapped_src_real_dest_svc_obj*] [**net-to-net**]
[**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*]

동적 NAT의 경우:

nat [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}]
source dynamic {*real_obj* | **any**}
{[*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]]]
[**interface** [**ipv6**]]}
[**destination static** {*mapped_obj* | **interface** [**ipv6**]} {*real_obj* | **any**}]
[**service** {*mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**]
[**description** *desc*]

no nat [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}]
source dynamic {*real_obj* | **any**}
{[*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]]]
[**interface** [**ipv6**]]}
[**destination static** {*mapped_obj* | **interface** [**ipv6**]} {*real_obj* | **any**}]
[**service** {*mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**]
[**description** *desc*]

또는

no nat {*line* | **after-auto** *line*}

구문 설명

(*real_ifc*,*mapped_ifc*)	(선택 사항) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 실제 및 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 중 하나 또는 둘 모두에 대해 **any** 키워드를 지정할 수도 있습니다. 투명 모드에서는 실제(real) 및 매핑된(mapped) 인터페이스를 지정해야 합니다. **any**는 사용할 수 없습니다. Twice NAT는 소스 주소와 수신 주소를 모두 변환할 수 있으므로, 소스 및 수신 인터페이스로서 더 잘 이해될 수 있습니다.
after-auto	NAT 테이블의 섹션 3 끝 부분, 네트워크 객체 NAT 규칙 뒤에 규칙을 삽입합니다. 기본적으로 Twice NAT 규칙은 섹션 1에 추가됩니다. *line* 인수를 사용하여 섹션 3의 어디에나 규칙을 삽입할 수 있습니다.
any	(선택 사항) 와일드카드 값을 지정합니다. **any**의 주요 사용 방식은 다음과 같습니다. • 인터페이스 - 하나 또는 두 인터페이스에 **any**를 사용할 수 있습니다(예: **(any,outside)**). 인터페이스를 지정하지 않으면 **any**가 기본값입니다. 투명 모드에서는 **any**를 사용할 수 없습니다. • 고정 NAT 소스 실제 및 매핑된 IP 주소 - 모든 주소에 대해 아이덴티티 NAT를 활성화하려면 **source static any any**를 지정할 수 있습니다. • 동적 NAT 또는 PAT 소스 실제 주소 - **source dynamic any** *mapped_obj*를 지정하여 소스 인터페이스의 모든 주소를 변환할 수 있습니다. 고정 NAT의 경우 실제 소스 포트/매핑된 목적지 포트 또는 소스/수신 실제 주소에도 **any**를 사용할 수 있지만(매핑된 주소에는 **any** 없이), 이렇게 할 경우 예기치 못한 상황이 발생할 수 있습니다. **참고** "any" 트래픽의 정의(IPv4 대 IPv6)는 규칙에 따라 다릅니다. ASA가 패킷에 대해 NAT를 수행하기 전에 패킷은 IPv6-to-IPv6 또는 IPv4-to-IPv4여야 합니다. 이 전제 조건하에 ASA는 NAT 규칙에서 **any**의 값을 결정할 수 있습니다. 예를 들어 "any"에서 IPv6 서버로 규칙을 구성하며 해당 서버가 IPv4 주소에서 매핑된 것이면 **any**는 "모든 IPv6 트래픽"을 의미합니다. "any"에서 "any"로 규칙을 구성하며 소스를 인터페이스 IPv4 주소로 매핑하면 **any**는 "모든 IPv4 트래픽"을 의미합니다. 매핑된 인터페이스 주소는 수신 주소도 IPv4임을 암시하기 때문입니다.
description *desc*	(선택 사항) 최대 200자로 설명을 제공합니다.
destination	(선택 사항) 수신 주소에 대한 변환을 구성합니다. Twice NAT의 주요 기능은 수신 IP 주소를 포함하는 것이지만, 수신 주소는 선택 사항입니다. 수신 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 아이덴티티 NAT를 사용할 수도 있습니다. 실제 주소에 네트워크 객체 그룹 사용, 수동으로 규칙 순서 지정 등을 비롯한 Twice NAT의 몇 가지 다른 기능을 활용하려면 수신 주소 없이 Twice NAT를 구성할 수 있습니다. 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.
dns	(선택 사항) DNS 회신을 변환합니다. DNS 검사를 활성화해야 합니다(**inspect dns**)(기본적으로 활성화됨). **destination** 주소를 구성하는 경우 **dns** 키워드를 구성할 수 없습니다. 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.
dynamic	소스 주소에 대해 동적 NAT 또는 PAT를 구성합니다. 수신 변환은 항상 고정입니다.

extended	(선택 사항) PAT 풀에 대해 확장 PAT를 활성화합니다. 확장 PAT는 변환 정보의 수신 주소 및 포트를 포함하여 *서비스*당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 목적지 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다.
flat [**include-reserve**]	(선택 사항) 포트 할당 시 1024~65535의 전체 포트 범위 사용을 활성화합니다. 변환용의 매핑된 포트 번호를 선택하면 ASA에서는 사용 가능한 경우 실제 소스 포트 번호를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 *없는*경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **include-reserve** 키워드도 지정합니다.
inactive	(선택 사항) 명령을 삭제하지 않은 채 이 규칙을 비활성화하려면 **inactive** 키워드를 사용합니다. 다시 활성화하려면 **inactive** 키워드 없이 명령 전체를 다시 입력합니다.
interface [**ipv6**]	(선택 사항) 인터페이스 IP 주소를 매핑된 주소로서 사용합니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. 동적 NAT 소스 매핑된 주소의 경우 **interface** 키워드 뒤에 매핑된 객체 또는 그룹을 지정하면, 다른 모든 매핑된 주소가 이미 할당된 경우에만 매핑된 인터페이스의 IP 주소가 사용됩니다. 동적 PAT의 경우 소스 매핑된 주소에는 **interface**만 지정할 수 있습니다. Static NAT with port translation(source 또는 destination)의 경우 **service** 키워드도 구성해야 합니다. 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 이 옵션은 투명 모드에서 사용할 수 없습니다.
line	(선택 사항) NAT 테이블의 섹션 1에서 아무 곳에나 규칙을 삽입합니다. 기본적으로 NAT 규칙이 섹션 1의 끝에 추가됩니다(자세한 내용은 CLI 컨피그레이션 가이드 참조). 대신 섹션 3에 규칙을 추가하려면(네트워크 객체 NAT 규칙 이후) **after-auto** *line* 옵션을 사용합니다.
mapped_dest_svc_obj	(선택 사항) 동적 NAT/PAT의 경우 매핑된 목적지 포트를 지정합니다(목적지 변환은 항상 고정임). 자세한 내용은 **service** 키워드를 참조하십시오.

mapped_object	매핑된 네트워크 객체 또는 객체 그룹(**object network** 또는 **object-group network**)을 식별합니다. 동적 NAT의 경우 일반적으로 더 큰 주소 그룹을 더 작은 그룹에 매핑하도록 구성합니다. **참고** 매핑된 객체 또는 그룹에는 서브넷을 포함할 수 없습니다. 원하는 경우 서로 다른 동적 NAT 규칙에서 이 매핑된 IP 주소를 공유할 수 있습니다. IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다. 동적 PAT의 경우 주소의 그룹을 단일 주소에 매핑하도록 구성합니다. 실제 주소를 자신이 선택한 단일 매핑된 주소로 변환할 수도 있고, 매핑된 인터페이스 주소로 변환할 수도 있습니다. 인터페이스 주소를 사용하려는 경우 매핑된 주소용 네트워크 객체를 구성하는 대신 **interface** 키워드를 사용하십시오. 고정 NAT에서 매핑은 일반적으로 1대1이므로, 실제 주소의 수가 매핑된 주소의 수와 같습니다. 그러나 원하는 경우 수량을 다르게 지정할 수 있습니다. 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.
mapped_src_real_dest_svc_obj	(선택 사항) 고정 NAT의 경우 매핑된 소스 포트, 실제 목적지 포트 또는 둘을 함께 지정합니다. 자세한 내용은 **service** 키워드를 참조하십시오.
net-to-net	(선택 사항) 고정 NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째를 두 번째로 등과 같이 변환하려면 **net-to-net**을 지정합니다. 이 옵션이 없으면 IPv4-embedded 메서드가 사용됩니다. 일대일 변환에는 이 키워드를 반드시 사용해야 합니다.
no-proxy-arp	(선택 사항) 고정 NAT의 경우 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP을 비활성화합니다.
pat-pool *mapped_obj*	(선택 사항) 주소의 PAT 풀을 활성화합니다. 객체의 모든 주소가 PAT 주소로 사용됩니다. IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
real_dest_svc_obj	(선택 사항) 동적 NAT/PAT의 경우 실제 목적지 포트를 지정합니다(목적지 변환은 항상 고정임). 자세한 내용은 **service** 키워드를 참조하십시오.
real_ifc	(선택 사항) 패킷이 시작되었을 수 있는 인터페이스의 이름을 지정합니다. source 옵션의 경우 origin_ifc는 실제 인터페이스이고, destination 옵션의 경우 real_ifc는 매핑된 인터페이스입니다.
real_object	실제 네트워크 객체 또는 객체 그룹(**object network** 또는 **object-group network**)을 식별합니다. IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
real_src_mapped_dest_svc_obj	(선택 사항) 고정 NAT의 경우 실제 소스 포트, 매핑된 목적지 포트 또는 둘을 함께 지정합니다. 자세한 내용은 **service** 키워드를 참조하십시오.
round-robin	(선택 사항) PAT 풀에 대해 라운드 로빈 주소 할당을 활성화합니다. 기본적으로 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.

route-lookup	(선택 사항) 라우팅된 모드의 아이덴티티 NAT의 경우, NAT 명령으로 지정한 인터페이스 대신 경로 조회를 사용하여 이그레스(egress) 인터페이스를 결정합니다. NAT 명령으로 인터페이스를 지정하지 않는 경우 기본적으로 경로 조회가 사용됩니다.
service	(선택 사항) 포트 변환을 지정합니다. • 동적 NAT 및 PAT - 동적 NAT 및 PAT는 추가 포트 변환을 지원하지 않습니다. 그러나 *대상* 변환은 항상 고정이므로 목적지 포트의 포트 변환을 수행할 수 있습니다. 서비스 객체(**object service**)는 소스 포트와 목적지 포트를 모두 포함할 수 있지만, 이 경우에는 목적지 포트만 사용됩니다. 소스 포트를 지정하면 무시됩니다. • Static NAT with port translation - 두 서비스 객체 모두에 대해 소스 포트 *또는* 목적지 포트 중 *하나*만 지정해야 합니다. 애플리케이션이 고정된 소스 포트(예: 일부 DNS 서버)를 사용하는 경우에만 소스 포트와 목적지 포트를 *모두* 지정해야 합니다. 그러나 고정된 소스 포트는 매우 드뭅니다. 소스 포트 변환의 경우 객체는 소스 서비스를 지정해야 합니다. 이 경우 명령에서 서비스 객체의 순서는 **service** *real_port mapped_port*입니다. 목적지 포트 변환의 경우 객체는 목적지 서비스를 지정해야 합니다. 이 경우 서비스 객체의 순서는 **service** *mapped_port real_port*입니다. 드문 경우이지만 객체에서 소스 포트와 목적지 포트를 모두 지정하는 경우, 첫 번째 서비스 객체는 실제 소스 포트/매핑된 목적지 포트를 포함하고, 두 번째 서비스 객체는 매핑된 소스 포트/실제 목적지 포트를 포함합니다. "소스(source)" 및 "목적지/수신(destination)" 용어에 대한 자세한 내용은 "사용 지침" 섹션을 참조하십시오9. 아이덴티티 포트 변환의 경우 실제 포트와 매핑된 포트에 동일한 서비스 객체를 사용합니다(컨피그레이션에 따라 소스 및/또는 목적지 포트). "not equal"(**neq**) 연산자는 지원되지 않습니다. NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 객체의 프로토콜과 매핑된 서비스 객체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP).
source	소스 주소에 대한 변환을 구성합니다.
static	고정 NAT 또는 Static NAT with port translation을 구성합니다.
unidirectional	(선택 사항) 고정 NAT의 경우 변환을 소스에서 수신의 단방향으로 만듭니다. 수신 주소는 소스 주소로 가는 트래픽을 시작할 수 없습니다. 이 옵션은 테스트용으로 유용할 수 있습니다.

기본값

- 기본적으로 규칙은 NAT 테이블의 섹션 1 끝에 추가됩니다.
- *real_ifc* 및 *mapped_ifc*의 기본값은 **any**입니다. 즉, 모든 인터페이스에 규칙을 적용합니다.
- (8.3(1), 8.3(2) 및 8.4(1)) 아이덴티티 NAT의 기본 동작은 프록시 ARP를 비활성화하는 것입니다. 이 설정은 구성할 수 없습니다. (8.4(2) 이상) 아이덴티티 NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다.

- 사용자가 선택적인 인터페이스를 지정하는 경우 ASA에서는 NAT 컨피그레이션을 사용하여 이그레스(egress) 인터페이스를 결정합니다. (8.3(1)~8.4(1)) 유일한 예외는 NAT 컨피그레이션과 상관없이 항상 경로 조회를 사용하는 아이덴티티 NAT에 대한 것입니다. (8.4(2) 이상) 아이덴티티 NAT의 기본 동작은 NAT 컨피그레이션을 사용하는 것이지만, 대신 항상 경로 조회를 사용할 수 있는 옵션이 사용자에게 제공됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.
8.3(2)	사전 8.3 NAT 예외 컨피그레이션에서 마이그레이션하면 고정 아이덴티티 NAT 규칙 결과에 **unidirectional** 키워드가 추가됩니다.
8.4(2)/8.5(1)	**no-proxy-arp**, **route-lookup**, **pat-pool** 및 **round-robin** 키워드가 추가되었습니다. 아이덴티티 NAT의 기본 동작이 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것으로 변경되었습니다. 8.3 이전 컨피그레이션의 경우 NAT 예외 규칙(**nat 0 access-list** 명령)을 8.4(2) 이상으로 마이그레이션하려면 **no-proxy-arp** 및 **route-lookup** 키워드를 포함하여 프록시 ARP를 비활성화하고 경로 조회를 사용해야 합니다. 8.3(2) 및 8.4(1)로 마이그레이션하는 데 사용된 **unidirectional** 키워드는 더 이상 마이그레이션에 사용되지 않습니다. 8.3(1), 8.3(2) 및 8.4(1)에서 8.4(2)로 업그레이드하면, 이제 기존 기능을 유지할 수 있도록 모든 아이덴티티 NAT 컨피그레이션에 **no-proxy-arp** 및 **route-lookup** 키워드가 포함됩니다. **unidirectional** 키워드는 제거됩니다.
8.4(3)	**extended**, **flat** 및 **include-reserve** 키워드가 추가되었습니다. 라운드 로빈 할당으로 PAT 풀을 사용할 때 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. *8.5(1)에서는 이 기능을 사용할 수 없습니다.*
9.0(1)	NAT는 이제 IPv6 트래픽은 물론 IPv4 및 IPv6 간 변환도 지원합니다. 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. **interface ipv6** 옵션 및 **net-to-net** 옵션이 추가되었습니다.

사용 지침

Twice NAT에서는 소스 주소와 수신 주소를 단일 규칙에서 식별할 수 있습니다. 소스 주소와 수신 주소를 모두 지정하면, 예를 들어 수신 X로 이동할 경우 소스 주소가 A로 변환되고 수신 Y로 이동할 경우 B로 변환되도록 지정할 수 있습니다.

참고 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "소스(source)"와 "수신(destination)"이 사용됩니다. 특정 연결이 "수신" 주소에서 시작되는 경우에도 마찬가지입니다. Static NAT with port translation을 구성하고, 소스 주소를 텔넷 서버로 지정하며, 텔넷 서버로 이동하는 모든 트래픽에 대해 포트를 2323에서 23으로 변환하려면 명령에서 *source* 포트가 변환되도록 지정해야 합니다(real: 23, mapped: 2323). 텔넷 서버 주소를 **source** 주소로 지정했기 때문에 소스 포트를 지정하는 것입니다.

수신 주소는 선택 사항입니다. 수신 주소를 지정하는 경우 이를 수신 주소 자신에게 매핑할 수도 있고(아이덴티티 NAT) 다른 주소에 매핑할 수도 있습니다. 수신 주소 매핑은 항상 고정 매핑입니다.

또한 Twice NAT를 사용하는 경우 static NAT with port translation에 대해 서비스 객체를 사용할 수 있습니다. 네트워크 객체 NAT는 인라인 정의만 수용합니다.

Twice NAT 및 네트워크 객체 NAT의 차이에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

Twice NAT 규칙은 NAT 규칙 테이블의 섹션 1(지정한 경우 섹션 3)에 추가됩니다. NAT 순서에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

매핑된 주소 지침

매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.

- 매핑된 인터페이스 IP 주소. 규칙에 대해 **any** 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅된 모드만)의 경우 IP 주소 대신 **interface** 키워드를 사용합니다.
- (투명 모드) 관리 IP 주소.
- (동적 NAT) VPN이 활성화된 경우의 대기 인터페이스 IP 주소.
- 기존의 VPN 풀 주소.

사전 요구 사항

- 실제 주소와 매핑된 주소 모두에 대해 네트워크 객체 또는 네트워크 객체 그룹을 구성합니다(**object network** 또는 **object-group network** 명령). 네트워크 객체 그룹은 비연속 IP 주소 범위 또는 다중 호스트나 서브넷을 이용해 매핑된 주소 풀을 만드는 데 특히 유용합니다. IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
- Static NAT with port translation에 대해 TCP 또는 UDP 서비스 객체를 구성합니다(**object service** 명령).

NAT의 객체 및 객체 그룹은 정의하지 않고 사용할 수 없으며, IP 주소를 반드시 포함해야 합니다.

변환 세션 지우기

NAT 컨피그레이션을 변경한 경우 새 NAT 정보가 사용되기 전 기존 변환이 시간 초과되기까지 기다리고 싶지 않다면 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 현재의 모든 연결이 해제됩니다.

PAT 풀 지침

- 각 A 레코드에 여러 PAT 규칙을 적용할 수 있으며 사용할 PAT 규칙이 애매하므로 DNS 재작성은 PAT에 적용되지 않습니다.

- 사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 *없는* 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다. (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 낮은 포트 범위를 사용하는 트래픽이 많은 경우 이제 크기가 서로 다른 세 가지 계층 대신 균일한 포트 범위(1024~65535 또는 1~65535)를 사용하도록 지정할 수 있습니다.
- (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 별개의 두 규칙에서 동일한 PAT 풀 객체를 사용하는 경우 각 규칙에 대해 동일한 옵션을 지정해야 합니다. 예를 들어, 한 규칙에서 확장 PAT와 균일한 범위를 지정하는 경우 다른 규칙에서도 확장 PAT와 균일한 범위를 지정해야 합니다.

PAT 풀용 확장 PAT 가이드라인

- 확장 PAT를 지원하지 않는 애플리케이션 검사가 많습니다. 지원되지 않는 검사 리스트는 컨피그레이션 가이드를 참조하십시오.
- 동적 PAT 규칙에 대해 확장 PAT를 활성화하면, PAT 풀의 주소를 별도의 static NAT-with-port-translation 규칙에서 PAT 주소로서 사용할 수 없습니다. 예를 들어 PAT 풀이 10.1.1.1을 포함하면, 10.1.1.1을 PAT 주소로 사용하는 static NAT-with-port-translation 규칙을 만들 수 없습니다.
- PAT 풀을 사용하고 대안용 인터페이스를 지정하는 경우 확장 PAT를 지정할 수 없습니다.
- ICE 또는 TURN을 사용하는 VoIP 배포에는 확장 PAT를 사용할 수 없습니다. ICE 및 TURN은 모든 목적지에 대해 PAT 바인딩이 동일할 것으로 신뢰합니다.

PAT 풀용 라운드 로빈 지침

- (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. **참고**: 장애 조치 이후에는 "동질성"이 해제됩니다. ASA에서 장애 조치를 수행하면 호스트의 후속 연결에는 초기 IP 주소가 사용되지 않을 수 있습니다.
- (8.4(2), 8.5(1) 및 8.6(1)) 호스트에 기존 연결이 있으면, 라운드 로빈 방식의 할당 때문에 해당 호스트의 후속 연결에서는 연결마다 *다른* PAT 주소가 사용될 수 있습니다. 이 경우 호스트에 대한 정보를 교환하는 두 웹사이트(예: 전자상거래 사이트 및 결제 사이트)에 액세스할 때 문제가 발생할 수 있습니다. 단일 호스트라고 예상했는데 두 개의 IP 주소가 존재하면 트랜잭션이 실패할 수 있습니다.

NAT 및 IPv6

IPv6 네트워크 간 변환 및 IPv4와 IPv6 네트워크 간 변환(라우팅된 모드 전용)을 위해 NAT를 사용할 수 있습니다. 다음의 모범 사례를 권장합니다.

- NAT66(IPv6-to-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(Twice NAT 전용).
- NAT46(IPv4-to-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. IPv6 주소 공간이 IPv4 주소 공간보다 훨씬 크기 때문에 고정 변환을 손쉽게 수용할 수 있습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(Twice NAT 전용). IPv6 서브넷(/96 이하)으로 변환하면 결과로 나타나는 매핑된 주소는 IPv4-embedded IPv6 주소입니다. 이 경우 IPv6 접두사 뒤에 IPv4 주소의 32비트가 포함됩니다. 예를 들어 IPv6 접두사가 /96 접두사이면, 주소의 마지막 32비트에 IPv4 주소가 첨부됩니다. 예를 들어 192.168.1.0/24를 201b::0/96에 매핑하면 192.168.1.4는 201b::0.192.168.1.4(혼합된 표기로 표시됨)에 매핑됩니다. 접두사가 더 작으면(예: /64) IPv4 주소가 접두사 뒤에 첨부되고, 접미사 0이 IPv4 주소 뒤에 첨부됩니다.
- NAT64(IPv6-to-IPv4) - IPv6 주소의 수를 수용할 만큼 IPv4 주소가 충분하지 않을 수 있습니다. 대량의 IPv4 변환을 제공하려면 동적 PAT 풀을 사용하는 것이 좋습니다.

예

다음 예에는 두 개의 서로 다른 서버에 액세스하는 10.1.2.0/24 네트워크의 호스트가 포함되어 있습니다. 호스트가 209.165.201.11의 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 209.165.200.225의 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0

ciscoasa(config)# object network DMZnetwork1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224

ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129

ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1

ciscoasa(config)# object network DMZnetwork2
ciscoasa(config-network-object)# subnet 209.165.200.224 255.255.255.224

ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130

ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

다음 예는 소스 포트와 목적지 포트의 사용법을 보여줍니다. 10.1.2.0/24 네트워크의 호스트가 웹 서비스와 텔넷 서비스를 모두 제공하는 단일 호스트에 액세스합니다. 호스트가 텔넷 서비스용 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 동일한 웹 서비스용 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0

ciscoasa(config)# object network TelnetWebServer
ciscoasa(config-network-object)# host 209.165.201.11

ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129

ciscoasa(config)# object service TelnetObj
ciscoasa(config-network-object)# service tcp destination eq telnet

ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj

ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130

ciscoasa(config)# object service HTTPObj
ciscoasa(config-network-object)# service tcp destination eq http

ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

다음 예는 Static interface NAT with port translation의 사용법을 보여줍니다. 외부의 호스트가 목적지 포트 65000~65004로 외부 인터페이스 IP 주소에 연결하여 내부의 FTP 서버에 액세스합니다. 192.168.10.100:6500~:65004에서는 트래픽이 내부 FTP 서버로 변환되지 않습니다. 소스 주소와 포트를 명령에 지정된 대로 변환하고자 하기 때문에 서비스 객체에서 소스 포트 범위를 지정하는 것입니다(목적지 포트는 지정하지 않음). 목적지 포트는 "any"입니다. 고정 NAT는 양방향이므로 "source" 및 "destination"은 기본적으로 명령 키워드를 가리킵니다. 패킷의 실제 소스 및 수신 주소

와 포트는 어떤 호스트가 패킷을 보냈는가에 따라 달라집니다. 이 예에서는 연결이 외부에서 시작되어 내부로 들어오므로 FTP 서버의 "source" 주소 및 포트는 실제로 원래 패킷의 수신 주소 및 포트입니다.

```
ciscoasa(config)# object service FTP_PASV_PORT_RANGE
ciscoasa(config-service-obvject)# service tcp source range 65000 65004

ciscoasa(config)# object network HOST_FTP_SERVER
ciscoasa(config-network-obvject)# host 192.168.10.100

ciscoasa(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

다음 예는 IPv4 209.165.201.1/27 네트워크의 서버 및 203.0.113.0/24 네트워크의 서버에 액세스할 때 IPv6 내부 네트워크 2001:DB8:AAAA::/96에 대해 동적 NAT를 구성합니다.

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96

ciscoasa(config)# object network MAPPED_1
ciscoasa(config-network-object)# range 209.165.200.225 209.165.200.254

ciscoasa(config)# object network MAPPED_2
ciscoasa(config-network-object)# range 209.165.202.129 209.165.200.158

ciscoasa(config)# object network SERVERS_1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224

ciscoasa(config)# object network SERVERS_2
ciscoasa(config-network-object)# subnet 203.0.113.0 255.255.255.0

ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

다음 예는 외부 IPv6 텔넷 서버 2001:DB8::23에 액세스할 때 내부 네트워크 192.168.1.0/24에 대해 인터페이스 PAT를 구성하고 2001:DB8:AAAA::/96 네트워크에 있는 서버에 액세스할 때 PAT 풀을 이용한 동적 PAT를 구성합니다.

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0

ciscoasa(config)# object network PAT_POOL
ciscoasa(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

ciscoasa(config)# object network TELNET_SVR
ciscoasa(config-network-object)# host 2001:DB8::23

ciscoasa(config)# object service TELNET
ciscoasa(config-service-object)# service tcp destination eq 23

ciscoasa(config)# object network SERVERS
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96

ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

관련 명령

명령	설명
clear configure nat	NAT 컨피그레이션(Twice NAT 및 네트워크 객체 NAT 모두)을 제거합니다.
show nat	NAT 정책 통계를 표시합니다.
show nat pool	NAT 풀에 대한 정보를 표시합니다.
show running-config nat	NAT 컨피그레이션을 표시합니다.
show xlate	NAT 세션(xlate) 정보를 표시합니다.

nat(object)

네트워크 객체용 NAT를 구성하려면 객체 네트워크 컨피그레이션 모드에서 **nat** 명령을 사용합니다. NAT 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

동적 NAT 및 PAT의 경우:

nat [(*real_ifc*,*mapped_ifc*)] **dynamic**
{*mapped_inline_host_ip* [**interface** [**ipv6**]] | [*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]]] [**interface** [**ipv6**]]} [**dns**]

no nat [(*real_ifc*,*mapped_ifc*)] **dynamic**
{*mapped_inline_host_ip* [**interface** [**ipv6**]] | [*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]]] [**interface** [**ipv6**]]} [**dns**]

고정 NAT 또는 Static NAT with port translation:

nat [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

no nat [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

구문 설명

(*real_ifc*,*mapped_ifc*)	(선택 사항) 고정 NAT의 경우 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 실제 및 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 중 하나 또는 둘 모두에 대해 **any** 키워드를 지정할 수도 있습니다. 명령에 괄호를 포함하십시오. 투명 모드에서는 실제(real) 및 매핑된(mapped) 인터페이스를 지정해야 합니다. **any**는 사용할 수 없습니다.
dns	(선택 사항) DNS 회신을 변환합니다. DNS 검사(**inspect dns**)를 활성화해야 합니다(기본적으로 활성화됨). **service** 키워드를 지정하면 이 옵션을 사용할 수 없습니다(고정 NAT의 경우). 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.
dynamic	동적 NAT 또는 PAT를 구성합니다.
extended	(선택 사항) PAT 풀에 대해 확장 PAT를 활성화합니다. 확장 PAT는 변환 정보의 수신 주소 및 포트를 포함하여 *서비스*당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 목적지 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다.
flat [**include-reserve**]	(선택 사항) 포트 할당 시 1024~65535의 전체 포트 범위 사용을 활성화합니다. 변환용의 매핑된 포트 번호를 선택하면 ASA에서는 사용 가능한 경우 실제 소스 포트 번호를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 *없는*경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **include-reserve** 키워드도 지정합니다.

interface [**ipv6**]	(선택 사항) 동적 NAT의 경우 **interface** 키워드 뒤에 매핑된 IP 주소, 객체 또는 그룹을 지정하면, 다른 모든 매핑된 주소가 이미 할당된 경우에만 매핑된 인터페이스의 IP 주소가 사용됩니다. 동적 PAT의 경우 매핑된 IP 주소, 객체 또는 그룹 대신 **interface** 키워드를 지정하면 매핑된 IP 주소에 대해 인터페이스 IP 주소를 사용하게 됩니다. 인터페이스 IP 주소를 사용하려면 이 키워드를 사용해야 하며, 인라인으로 또는 객체로서 입력할 수 없습니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. Static NAT with port translation의 경우 **service** 키워드도 함께 구성하는 경우에만 **interface** 키워드를 지정할 수 있습니다. 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 투명 모드에서는 **interface**를 지정할 수 없습니다.
mapped_inline_host_ip	인라인 값으로서 매핑된 주소를 지정합니다. **dynamic**을 지정하고 호스트 IP 주소를 사용하면 동적 PAT가 구성됩니다.
mapped_inline_ip	고정 NAT의 경우 인라인 값으로서 매핑된 IP 주소를 지정합니다. 매핑된 네트워크의 범위 또는 넷마스크가 실제 네트워크와 동일합니다. 예를 들어 실제 네트워크가 호스트이면 이 주소도 호스트 주소입니다. 범위의 경우 매핑된 주소에는 동일한 주소 번호가 실제 범위로서 포함됩니다. 예를 들어 실제 주소의 범위를 10.1.1.1~10.1.1.6으로 정의하고 매핑된 주소로 172.20.1.1을 지정하는 경우 매핑된 범위에는 172.20.1.1~172.20.1.6이 포함됩니다.
mapped_obj	매핑된 IP 주소를 네트워크 객체(**object network**) 또는 객체 그룹(**object-group network**)으로 지정합니다. IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다. 동적 NAT의 경우 객체 또는 그룹에는 서브넷을 포함할 수 없습니다. 원하는 경우 서로 다른 동적 NAT 규칙에서 이 매핑된 객체를 공유할 수 있습니다. 허용되지 않는 매핑된 IP 주소에 대한 자세한 내용은 "매핑된 주소 지침" 페이지의 섹션 13-34를 참조하십시오. 고정 NAT의 경우 일반적으로 일대일 매핑에서는 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다. 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.
mapped_port	(선택 사항) 매핑된 TCP 또는 UDP 포트를 지정합니다. 리터럴 이름 또는 0~65535 범위의 숫자로 포트를 지정할 수 있습니다.
net-to-net	(선택 사항) NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째를 두 번째로 등과 같이 변환하려면 **net-to-net**을 지정합니다. 이 옵션이 없으면 IPv4-embedded 메서드가 사용됩니다. 일대일 변환에는 이 키워드를 반드시 사용해야 합니다.
no-proxy-arp	(선택 사항) 고정 NAT의 경우 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP을 비활성화합니다.
pat-pool *mapped_obj*	(선택 사항) 주소의 PAT 풀을 활성화합니다. 객체의 모든 주소가 PAT 주소로 사용됩니다. IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
real_port	(선택 사항) 고정 NAT의 경우 실제 TCP 또는 UDP 포트를 지정합니다. 리터럴 이름 또는 0~65535 범위의 숫자로 포트를 지정할 수 있습니다.

round-robin	(선택 사항) PAT 풀에 대해 라운드 로빈 주소 할당을 활성화합니다. 기본적으로 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다.
route-lookup	(선택 사항) 라우팅된 모드의 아이덴티티 NAT의 경우, NAT 명령으로 지정한 인터페이스 대신 경로 조회를 사용하여 이그레스(egress) 인터페이스를 결정합니다. NAT 명령으로 인터페이스를 지정하지 않는 경우 기본적으로 경로 조회가 사용됩니다.
service {**tcp** | **udp**}	(선택 사항) Static NAT with port translation의 경우 포트 변환용 프로토콜을 지정합니다. TCP와 UDP만 지원됩니다.
static	고정 NAT 또는 Static NAT with port translation을 구성합니다.

기본값

- *real_ifc* 및 *mapped_ifc*의 기본값은 **any**입니다. 즉, 모든 인터페이스에 규칙을 적용합니다.
- (8.3(1), 8.3(2) 및 8.4(1)) 아이덴티티 NAT의 기본 동작은 프록시 ARP를 비활성화하는 것입니다. 이 설정은 구성할 수 없습니다. (8.4(2) 이상) 아이덴티티 NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다.
- 사용자가 선택적인 인터페이스를 지정하는 경우 ASA에서는 NAT 컨피그레이션을 사용하여 이그레스(egress) 인터페이스를 결정합니다. (8.3(1)~8.4(1)) 유일한 예외는 NAT 컨피그레이션과 상관없이 항상 경로 조회를 사용하는 아이덴티티 NAT에 대한 것입니다. (8.4(2) 이상) 아이덴티티 NAT의 기본 동작은 NAT 컨피그레이션을 사용하는 것이지만, 대신 항상 경로 조회를 사용할 수 있는 옵션이 사용자에게 제공됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
객체 네트워크 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.
8.4(2)/8.5(1)	**no-proxy-arp**, **route-lookup**, **pat-pool** 및 **round-robin** 키워드가 추가되었습니다. 아이덴티티 NAT의 기본 동작이 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것으로 변경되었습니다. 8.3(1), 8.3(2) 및 8.4(1)에서 8.4(2)로 업그레이드하면, 이제 기존 기능을 유지할 수 있도록 모든 아이덴티티 NAT 컨피그레이션에 **no-proxy-arp** 및 **route-lookup** 키워드가 포함됩니다.

릴리스	수정
8.4(3)	**extended**, **flat** 및 **include-reserve** 키워드가 추가되었습니다. 라운드 로빈 할당으로 PAT 풀을 사용할 때 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. *8.5(1)에서는 이 기능을 사용할 수 없습니다.*
9.0(1)	NAT는 이제 IPv6 트래픽은 물론 IPv4 및 IPv6 간 변환도 지원합니다. 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. **interface ipv6** 옵션 및 **net-to-net** 옵션이 추가되었습니다.

사용 지침

패킷이 ASA로 들어가면 소스 및 수신 IP 주소 모두에서 네트워크 객체 NAT 규칙의 점검이 수행됩니다. 별도의 일치를 만든 경우 별도의 규칙을 통해 패킷의 소스 및 수신 주소를 변환할 수 있습니다. 이러한 규칙은 서로 연결되어 있지 않습니다. 트래픽에 따라 규칙의 서로 다른 조합을 사용할 수 있습니다.

규칙은 쌍을 이루지 않으므로 소스 주소가 수신 주소 X로 이동할 때 A로 변환되도록, 수신 주소 Y로 이동할 때 B로 변환되도록 지정할 수 없습니다. 그런 종류의 기능이 필요한 경우 Twice NAT를 사용하십시오. Twice NAT를 사용하면 단일 규칙으로 소스 및 수신 주소를 식별할 수 있습니다.

Twice NAT 및 네트워크 객체 NAT의 차이에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

네트워크 객체 NAT 규칙은 NAT 규칙 테이블의 섹션 2에 추가됩니다. NAT 순서에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

컨피그레이션에 따라 원하는 경우 매핑된 주소를 인라인으로 구성할 수도 있고, 매핑된 주소에 대해 네트워크 객체 또는 네트워크 객체 그룹을 만들 수도 있습니다(**object network** 또는 **object-group network** 명령). 네트워크 객체 그룹은 비연속 IP 주소 범위 또는 다중 호스트나 서브넷을 이용해 매핑된 주소 풀을 만드는 데 특히 유용합니다. IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다.

NAT의 객체 및 객체 그룹은 정의하지 않고 사용할 수 없으며, IP 주소를 반드시 포함해야 합니다.

한 객체에는 단일 NAT 규칙만 정의할 수 있습니다. 여러 NAT 규칙을 구성하려면 동일한 IP 주소를 지정하는 여러 객체를 만들어야 합니다(예: **object network obj-10.10.10.1-01**, **object network obj-10.10.10.1-02** 등).

매핑된 주소 지침

매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.

- 매핑된 인터페이스 IP 주소. 규칙에 대해 **any** 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅된 모드만)의 경우 IP 주소 대신 **interface** 키워드를 사용합니다.
- (투명 모드) 관리 IP 주소.
- (동적 NAT) VPN이 활성화된 경우의 대기 인터페이스 IP 주소.
- 기존의 VPN 풀 주소.

변환 세션 지우기

NAT 컨피그레이션을 변경한 경우 새 NAT 정보가 사용되기 전 기존 변환이 시간 초과되기까지 기다리고 싶지 않다면 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 현재의 모든 연결이 해제됩니다.

PAT 풀 지침

- 각 A 레코드에 여러 PAT 규칙을 적용할 수 있으며 사용할 PAT 규칙이 애매하므로 DNS 재작성은 PAT에 적용되지 않습니다.
- 사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 *없는* 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다. (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 낮은 포트 범위를 사용하는 트래픽이 많은 경우 이제 크기가 서로 다른 세 가지 계층 대신 균일한 포트 범위(1024~65535 또는 1~65535)를 사용하도록 지정할 수 있습니다.
- (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 별개의 두 규칙에서 동일한 PAT 풀 객체를 사용하는 경우 각 규칙에 대해 동일한 옵션을 지정해야 합니다. 예를 들어, 한 규칙에서 확장 PAT와 균일한 범위를 지정하는 경우 다른 규칙에서도 확장 PAT와 균일한 범위를 지정해야 합니다.

PAT 풀용 확장 PAT 가이드라인

- 확장 PAT를 지원하지 않는 애플리케이션 검사가 많습니다. 지원되지 않는 검사 리스트는 컨피그레이션 가이드를 참조하십시오.
- 동적 PAT 규칙에 대해 확장 PAT를 활성화하면, PAT 풀의 주소를 별도의 static NAT-with-port-translation 규칙에서 PAT 주소로서 사용할 수 없습니다. 예를 들어 PAT 풀이 10.1.1.1을 포함하면, 10.1.1.1을 PAT 주소로 사용하는 static NAT-with-port-translation 규칙을 만들 수 없습니다.
- PAT 풀을 사용하고 대안용 인터페이스를 지정하는 경우 확장 PAT를 지정할 수 없습니다.
- ICE 또는 TURN을 사용하는 VoIP 배포에는 확장 PAT를 사용할 수 없습니다. ICE 및 TURN은 모든 목적지에 대해 PAT 바인딩이 동일할 것으로 신뢰합니다.

PAT 풀용 라운드 로빈 지침

- (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. **참고**: 장애 조치 이후에는 "동질성"이 해제됩니다. ASA에서 장애 조치를 수행하면 호스트의 후속 연결에는 초기 IP 주소가 사용되지 않을 수 있습니다.
- (8.4(2), 8.5(1) 및 8.6(1)) 호스트에 기존 연결이 있으면, 라운드 로빈 방식의 할당 때문에 해당 호스트의 후속 연결에서는 연결마다 *다른* PAT 주소가 사용될 수 있습니다. 이 경우 호스트에 대한 정보를 교환하는 두 웹사이트(예: 전자상거래 사이트 및 결제 사이트)에 액세스할 때 문제가 발생할 수 있습니다. 단일 호스트라고 예상했는데 두 개의 IP 주소가 존재하면 트랜잭션이 실패할 수 있습니다.
- 라운드 로빈은 특히 확장 PAT와 함께 사용할 경우 대량의 메모리를 소모할 수 있습니다.

NAT 및 IPv6

IPv6 네트워크 간 변환 및 IPv4와 IPv6 네트워크 간 변환(라우팅된 모드 전용)을 위해 NAT를 사용할 수 있습니다. 다음의 모범 사례를 권장합니다.

- NAT66(IPv6-to-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(Twice NAT 전용).
- NAT46(IPv4-to-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. IPv6 주소 공간이 IPv4 주소 공간보다 훨씬 크기 때문에 고정 변환을 손쉽게 수용할 수 있습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(Twice NAT 전용). IPv6 서브넷(/96 이하)으로 변환하면 결과로 나타나는 매핑된 주소는 IPv4-embedded IPv6 주소입니다. 이 경우 IPv6 접두사 뒤에 IPv4 주소의 32비트가 포함됩니다. 예를 들어 IPv6 접두사가 /96 접두사

이면, 주소의 마지막 32비트에 IPv4 주소가 첨부됩니다. 예를 들어 192.168.1.0/24를 201b::0/96에 매핑하면 192.168.1.4는 201b::0.192.168.1.4(혼합된 표기로 표시됨)에 매핑됩니다. 접두사가 더 작으면(예: /64) IPv4 주소가 접두사 뒤에 첨부되고, 접미사 0이 IPv4 주소 뒤에 첨부됩니다.

- NAT64(IPv6-to-IPv4) - IPv6 주소의 수를 수용할 만큼 IPv4 주소가 충분하지 않을 수 있습니다. 대량의 IPv4 변환을 제공하려면 동적 PAT 풀을 사용하는 것이 좋습니다.

예

동적 NAT 예

다음 예는 192.168.2.0 네트워크를 2.2.2.1~2.2.2.10의 외부 주소 범위 뒤에 숨기는 동적 NAT를 구성합니다.

```
ciscoasa(config)# object network my-range-obj
ciscoasa(config-network-object)# range 2.2.2.1 2.2.2.10
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

다음 예는 동적 PAT 백업으로 동적 NAT를 구성합니다. 내부 네트워크 10.76.11.0의 호스트는 먼저 nat-range1 풀(10.10.10.10~10.10.10.20)에 매핑됩니다. nat-range1 풀의 모든 주소가 할당된 후에는 pat-ip1 주소(10.10.10.21)를 사용해 동적 PAT가 수행됩니다. 잘 발생하지는 않지만, PAT 변환도 모두 사용되면 외부 인터페이스 주소를 사용해 동적 PAT가 수행됩니다.

```
ciscoasa(config)# object network nat-range1
ciscoasa(config-network-object)# range 10.10.10.10 10.10.10.20

ciscoasa(config-network-object)# object network pat-ip1
ciscoasa(config-network-object)# host 10.10.10.21

ciscoasa(config-network-object)# object-group network nat-pat-grp
ciscoasa(config-network-object)# network-object object nat-range1
ciscoasa(config-network-object)# network-object object pat-ip1

ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 10.76.11.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

다음 예는 IPv6 호스트를 IPv4로 변환하기 위해 동적 PAT 백업으로 동적 NAT를 구성합니다. 내부 네트워크 2001:DB8::/96의 호스트가 먼저 IPv4_NAT_RANGE 풀(209.165.201.1~209.165.201.30)에 매핑됩니다. IPv4_NAT_RANGE 풀의 모든 주소가 할당된 후에는 IPv4_PAT 주소(209.165.201.31)를 사용해 동적 PAT가 수행됩니다. PAT 변환도 모두 사용되면 외부 인터페이스 주소를 사용해 동적 PAT가 수행됩니다.

```
ciscoasa(config)# object network IPv4_NAT_RANGE
ciscoasa(config-network-object)# range 209.165.201.1 209.165.201.30

ciscoasa(config-network-object)# object network IPv4_PAT
ciscoasa(config-network-object)# host 209.165.201.31

ciscoasa(config-network-object)# object-group network IPv4_GROUP
ciscoasa(config-network-object)# network-object object IPv4_NAT_RANGE
ciscoasa(config-network-object)# network-object object IPv4_PAT

ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

동적 PAT 예

다음 예는 192.168.2.0 네트워크를 주소 2.2.2.2 뒤에 숨기는 동적 PAT를 구성합니다.

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic 2.2.2.2
```

다음 예는 192.168.2.0 네트워크를 외부 인터페이스 주소 뒤에 숨기는 동적 PAT를 구성합니다.

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

다음 예는 내부 IPv6 네트워크를 외부 IPv4 네트워크로 변환할 수 있도록 PAT 풀이 있는 동적 PAT를 구성합니다.

```
ciscoasa(config)# object network IPv4_POOL
ciscoasa(config-network-object)# range 203.0.113.1 203.0.113.254
ciscoasa(config)# object network IPv6_INSIDE
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

고정 NAT 예

다음 예는 DNS 재작성을 활성화하여 내부의 1.1.1.1에서 외부의 2.2.2.2로 실제 호스트에 대한 고정 NAT를 구성합니다.

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 2.2.2.2 dns
```

다음 예는 매핑된 객체를 사용하여 내부의 1.1.1.1에서 외부의 2.2.2.2로 실제 호스트에 대한 고정 NAT를 구성합니다.

```
ciscoasa(config)# object network my-mapped-obj
ciscoasa(config-network-object)# host 2.2.2.2

ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-mapped-obj
```

다음 예는 TCP 포트 21의 1.1.1.1에서 포트 2121의 외부 인터페이스로 Static NAT with port translation을 구성합니다.

```
ciscoasa(config)# object network my-ftp-server
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

다음 예는 내부 IPv4 네트워크를 외부 IPv6 네트워크로 매핑합니다.

```
ciscoasa(config)# object network inside_v4_v6
ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

다음 예는 내부 IPv6 네트워크를 외부 IPv6 네트워크로 매핑합니다.

```
ciscoasa(config)# object network inside_v6
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

아이덴티티 NAT 예

다음 예는 인라인 매핑된 주소를 사용하여 호스트 주소를 자체에 매핑합니다.

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 10.1.1.1
```

다음 예는 네트워크 객체를 사용하여 호스트 주소를 자체에 매핑합니다.

```
ciscoasa(config)# object network my-host-obj1-identity
ciscoasa(config-network-object)# host 10.1.1.1

ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

관련 명령

명령	설명
clear configure nat	NAT 컨피그레이션(Twice NAT 및 네트워크 객체 NAT 모두)을 제거합니다.
show nat	NAT 정책 통계를 표시합니다.
show nat pool	NAT 풀에 대한 정보를 표시합니다.
show running-config nat	NAT 컨피그레이션을 표시합니다.
show xlate	xlate 정보를 표시합니다.

nat(vpn load-balancing)

NAT가 이 디바이스의 IP 주소를 변환하는 IP 주소를 설정하려면 VPN load-balancing 컨피그레이션 모드에서 **nat** 명령을 사용합니다. NAT 변환을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

nat *ip-address*

no nat [*ip-adddress*]

구문 설명

ip-address	NAT가 이 디바이스의 IP 주소를 변환하도록 할 IP 주소입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
VPN 로드 밸런싱 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

먼저 **vpn load-balancing** 명령을 사용해야 VPN 로드 밸런싱 모드로 들어갈 수 있습니다.

이 명령의 **no nat** 형식에서 선택 사항인 *ip-address* 값을 지정하면, IP 주소가 실행 중인 컨피그레이션의 기존 NAT IP 주소와 일치해야 합니다.

예

다음은 NAT 변환 주소를 192.168.10.10으로 설정하는 **nat** 명령이 포함된 VPN 로드 밸런싱 명령 시퀀스의 예입니다.

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
vpn load-balancing	VPN 로드 밸런싱 모드로 들어갑니다.

nat-assigned-to-public-ip

VPN 피어의 로컬 IP 주소를 피어의 실제 IP 주소로 자동 변환하려면 tunnel-group general-attributes 컨피그레이션 모드에서 **nat-assigned-to-public-ip** 명령을 사용합니다. NAT 규칙을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

nat-assigned-to-public-ip *interface*

no nat-assigned-to-public-ip *interface*

구문 설명

interface	NAT를 적용할 인터페이스를 지정합니다.

명령 기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group general-attributes 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
8.4(3)	이 명령이 추가되었습니다.

사용 지침

드문 경우이지만 할당된 로컬 IP 주소 대신 내부 네트워크에 있는 VPN 피어의 실제 IP 주소를 사용하고자 할 수 있습니다. 일반적으로 VPN에서는 내부 네트워크에 액세스할 수 있도록, 할당된 로컬 IP 주소를 피어에 제공합니다. 그러나 예를 들어 내부 서버 및 네트워크 보안이 피어의 실제 IP 주소를 기반으로 하는 경우, 로컬 IP 주소를 피어의 실제 공개 IP 주소로 다시 변환할 수 있습니다.

터널 그룹당 한 인터페이스에서 이 기능을 활성화할 수 있습니다. VPN 세션이 설정되거나 연결이 해제되면 객체 NAT 규칙이 동적으로 추가 및 삭제됩니다. **show nat** 명령을 사용하여 규칙을 볼 수 있습니다.

데이터 흐름

다음 단계는 이 기능이 활성화되었을 때 ASA를 통과하는 패킷 흐름에 대해 설명합니다.

1. VPN 피어가 ASA에 패킷을 전송합니다.

   외부 소스/수신은 피어 공용 IP 주소/ASA IP 주소로 구성됩니다. 암호화된 내부 소스/수신은 VPN 할당 IP 주소/내부 서버 주소로 구성됩니다.
2. ASA가 패킷을 해독합니다(외부 소스/수신 제거).
3. ASA가 내부 서버에 대해 경로 조회를 수행하고 패킷을 내부 인터페이스로 전송합니다.
4. 자동으로 생성된 VPN NAT 정책은 VPN 할당 소스 IP 주소를 피어 공용 IP 주소로 변환합니다.

5. ASA가 변환된 패킷을 서버로 전송합니다.
6. 서버가 패킷에 응답하고, 패킷을 피어의 공용 IP 주소로 전송합니다.
7. ASA가 응답을 받고, 수신 IP 주소를 VPN 할당 IP 주소로 변환하지 않습니다.
8. ASA가 변환되지 않은 패킷을 외부 인터페이스로 전달하면 여기에서 패킷이 암호화되며, 외부 소스/대상이 추가되어 ASA IP 주소/피어 공용 IP 주소가 구성됩니다.
9. ASA가 패킷을 피어로 다시 전송합니다.
10. 피어가 데이터를 해독 및 처리합니다.

제한 사항

라우팅 문제 때문에, 반드시 필요한 경우가 아니면 이 기능을 사용하지 않는 것이 좋습니다. 네트워크와의 기능 호환성을 확인하려면 Cisco TAC에 문의하십시오. 다음 제한을 참조하십시오.

- Cisco IPsec 및 AnyConnect 클라이언트만 지원합니다.
- NAT 정책과 VPN 정책이 적용될 수 있도록, 공개 IP 주소로 반환되는 트래픽을 ASA로 다시 라우팅해야 합니다.
- 역 경로 삽입을 활성화하면(**set reverse-route** 명령 참조) VPN 할당 IP 주소만 광고됩니다.
- 로드 밸런싱을 지원하지 않습니다(라우팅 문제 때문).
- 로밍을 지원하지 않습니다(공개 IP 변경).

예

다음 예는 "vpnclient" 터널 그룹용 공용 IP에 대해 NAT를 활성화합니다.

```
ciscoasa# ip local pool client 10.1.226.4-10.1.226.254
ciscoasa# tunnel-group vpnclient type remote-access
ciscoasa# tunnel-group vpnclient general-attributes
ciscoasa(config-tunnel-general)# address-pool client
ciscoasa(config-tunnel-general)# nat-assigned-to-public-ip inside
```

다음은 IP 10.1.226.174가 할당된 피어 209.165.201.10의 자동 NAT 규칙을 보여주는 **show nat detail** 명령의 샘플 출력입니다.

```
ciscoasa# show nat detail

 Auto NAT Policies (Section 2)
 1 (outside) to (inside) source static _vpn_nat_10.1.226.174 209.165.201.10
     translate_hits = 0, untranslate_hits = 0
     Source - Origin: 10.1.226.174/32, Translated: 209.165.201.10/32
```

관련 명령

명령	설명
show nat	현지 xlate를 보여줍니다.
tunnel-group general-attributes	터널 그룹에 대한 일반 특성을 설정합니다.
debug menu webvpn 99	AnyConnect SSL 세션의 경우 VPN NAT 인터페이스는 세션에 저장됩니다.
debug menu ike 2 *peer_ip*	Cisco IPsec 클라이언트 세션의 경우 VPN NAT 인터페이스는 SA에 저장됩니다.
debug nat 3	NAT에 대한 디버그 메시지를 보여줍니다.

nat-rewrite

DNS 응답의 A 레코드에 포함된 IP 주소에 대해 NAT 재작성을 활성화하려면 매개변수 컨피그레이션 모드에서 **nat-rewrite** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

nat-rewrite

no nat-rewrite

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

NAT 재작성은 기본적으로 활성화되어 있습니다. **policy-map type inspect dns**가 정의되지 않았어도 **inspect dns**가 구성되어 있으면 이 기능을 활성화할 수 있습니다. 비활성화하려면 정책 맵 컨피그레이션에서 **no nat-rewrite**를 명시적으로 작성해야 합니다. **inspect dns**가 구성되어 있지 않으면 NAT 재작성이 수행되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 기능은 DNS 응답에서 A 유형 RR(리소스 레코드)의 NAT 변환을 수행합니다.

예

다음 예는 DNS 검사 정책 맵에서 NAT 재작성을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# nat-rewrite
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

nbns-server(tunnel-group webvpn attributes mode)

NBNS 서버를 구성하려면 tunnel-group webvpn 컨피그레이션 모드에서 **nbns-server** 명령을 사용합니다. 컨피그레이션에서 NBNS 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ASA는 NetBIOS 이름을 IP 주소에 매핑하기 위해 NBNS 서버에 쿼리합니다. WebVPN은 원격 시스템의 파일에 대한 액세스 또는 공유를 NetBIOS에 요청합니다.

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

구문 설명

hostname	NBNS 서버의 호스트 이름을 지정합니다.
ipaddr	NBNS 서버의 IP 주소를 지정합니다.
master	WINS 서버가 아니라 마스터 브라우저임을 나타냅니다.
retry	재시도 값이 이어짐을 나타냅니다.
retries	NBNS 서버에 대한 쿼리 재시도 횟수를 지정합니다. ASA는 오류 메시지를 전송하기 전에 여기에서 지정한 횟수만큼 서버 목록을 순환합니다. 기본값은 2, 허용 범위는 1~10입니다.
timeout	시간 제한 값이 이어짐을 나타냅니다.
timeout	여러 NBNS 서버가 하나뿐인 경우 동일한 서버에 또는 여러 개가 있는 경우 또 다른 서버에 ASA가 쿼리를 다시 전송하기까지 대기하는 시간을 지정합니다. 기본 시간 제한은 2초이고 범위는 1~30초입니다.

기본값

NBNS 서버는 기본적으로 구성되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.1(1)	webvpn 모드에서 tunnel-group webvpn 컨피그레이션 모드로 이동했습니다.

사용 지침

릴리스 7.1(1)의 webvpn 컨피그레이션 모드에서 이 명령을 입력하면 tunnel-group webvpn-attributes 컨피그레이션 모드의 동일한 명령으로 전환됩니다.

서버 엔트리는 최대 3개입니다. 구성하는 첫 번째 서버는 기본 서버이고 나머지 두 개는 이중화용 백업 서버입니다.

컨피그레이션에서 일치하는 엔트리를 제거하려면 **no** 옵션을 사용합니다.

예

다음 예는 IP 주소 10.10.10.19, 시간 제한 값 10초, 재시도 8회의 마스터 브라우저인 NBNS 서버로 터널 그룹 "test"를 구성하는 방법을 보여줍니다. 또한 IP 주소 10.10.10.24, 시간 제한 값 15초, 재시도 8회의 NBNS WINS 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

명령	설명
clear configure group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대한 컨피그레이션을 제거합니다.
show running-config group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대해 실행 중인 컨피그레이션을 표시합니다.
tunnel-group webvpn-attributes	명명된 터널 그룹에 대한 WebVPN 특성을 지정합니다.

nbns-server(webvpn mode)

NBNS 서버를 구성하려면 tunnel-group webvpn 컨피그레이션 모드에서 **nbns-server** 명령을 사용합니다. 컨피그레이션에서 NBNS 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ASA는 NetBIOS 이름을 IP 주소에 매핑하기 위해 NBNS 서버에 쿼리합니다. WebVPN은 원격 시스템의 파일에 대한 액세스 또는 공유를 NetBIOS에 요청합니다.

nbns-server {*ipaddr* | *hostname*} [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

구문 설명

hostname	NBNS 서버의 호스트 이름을 지정합니다.
ipaddr	NBNS 서버의 IP 주소를 지정합니다.
master	WINS 서버가 아니라 마스터 브라우저임을 나타냅니다.
retry	재시도 값이 이어짐을 나타냅니다.
retries	NBNS 서버에 대한 쿼리 재시도 횟수를 지정합니다. ASA는 오류 메시지를 전송하기 전에 여기에서 지정한 횟수만큼 서버 목록을 순환합니다. 기본값은 2, 허용 범위는 1~10입니다.
timeout	시간 제한 값이 이어짐을 나타냅니다.
timeout	여러 NBNS 서버가 하나뿐인 경우 동일한 서버에 또는 여러 개가 있는 경우 또 다른 서버에 ASA가 쿼리를 다시 전송하기까지 대기하는 시간을 지정합니다. 기본 시간 제한은 2초이고 범위는 1~30초입니다.

기본값

NBNS 서버는 기본적으로 구성되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.1(1)	webvpn 모드에서 tunnel-group webvpn 컨피그레이션 모드로 이동했습니다.

사용 지침

이 명령은 webvpn 컨피그레이션 모드에서 사용되지 않습니다. 대신 tunnel-group webvpn-attributes 컨피그레이션 모드의 nbns-server 명령이 사용됩니다. 릴리스 7.1(1)의 webvpn 컨피그레이션 모드에서 이 명령을 입력하면 tunnel-group webvpn-attributes 모드의 동일한 명령으로 전환됩니다.

서버 엔트리는 최대 3개입니다. 구성하는 첫 번째 서버는 기본 서버이고 나머지 두 개는 이중화용 백업 서버입니다.

컨피그레이션에서 일치하는 엔트리를 제거하려면 **no** 옵션을 사용합니다.

예

다음 예는 IP 주소 10.10.10.19, 시간 제한 값 10초, 재시도 8회의 마스터 브라우저인 NBNS 서버를 구성하는 방법을 보여줍니다. 또한 IP 주소 10.10.10.24, 시간 제한 값 15초, 재시도 8회의 NBNS WINS 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

포인트-투-포인트 비 브로드캐스트 네트워크에서 고정 인접 디바이스를 정의하려면 라우터 컨피그레이션 모드에서 **neighbor** 명령을 사용합니다. 정의된 인접 디바이스를 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor *ip_address* [**interface** *name*]

no neighbor *ip_address* [**interface** *name*]

구문 설명

interface *name*	(선택 사항) 인접 디바이스에 도달할 수 있는 인터페이스 이름(**nameif** 명령으로 지정)을 지정합니다.
ip_address	인접 라우터의 IP 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

neighbor 명령은 VPN 터널을 통해 OSPF 경로를 광고하는 데 사용됩니다. 각각의 알려진 비 브로드캐스트 네트워크 인접 디바이스에 하나의 인접 디바이스 엔트리를 포함해야 합니다. 인접 디바이스 주소는 인터페이스의 기본 주소에 있어야 합니다.

인접 디바이스가 시스템에 직접 연결된 인터페이스 중 하나와 동일한 네트워크에 있지 않은 경우 **interface** 옵션을 지정해야 합니다. 또한 인접 디바이스에 도달하려면 고정 경로를 만들어야 합니다.

예

다음 예는 192.168.1.1 주소로 인접 라우터를 정의합니다.

```
ciscoasa(config-router)# neighbor 192.168.1.1
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드로 들어갑니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

neighbor(EIGRP)

라우팅 정보를 교환할 EIGRP 인접 라우터를 정의하려면 라우터 컨피그레이션 모드에서 **neighbor** 명령을 사용합니다. 인접 디바이스 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor *ip_address* **interface** *name*

no neighbor *ip_address* **interface** *name*

구문 설명

interface *name*	인접 디바이스에 도달할 수 있는 인터페이스 이름입니다(**nameif** 명령으로 지정).
ip_address	인접 라우터의 IP 주소입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

특정 EIGRP 인접 디바이스로 피어링을 설정하려면 여러 neighbor 명령문을 사용할 수 있습니다. EIGRP가 라우팅 업데이트를 교환하는 인터페이스는 neighbor 명령문으로 지정해야 합니다. 두 개의 EIGRP 인접 디바이스가 라우팅 업데이트를 교환하는 인터페이스는 동일한 네트워크의 IP 주소로 구성해야 합니다.

참고 인터페이스에 대해 **passive-interface** 명령을 구성하면 해당 인터페이스에서 들어오고 나가는 모든 라우팅 업데이트 및 hello 메시지가 억제됩니다. 패시브로 구성된 인터페이스를 통해서는 EIGRP 인접 디바이스 인접성을 설정하거나 유지 관리할 수 없습니다.

EIGRP hello 메시지는 **neighbor** 명령으로 정의한 인접 디바이스에 유니캐스트 메시지로서 전송됩니다.

예

다음 예는 192.168.1.1 및 192.168.2.2 인접 디바이스로 EIGRP 피어링 세션을 구성합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.0.0
ciscoasa(config-router)# neighbor 192.168.1.1 interface outside
ciscoasa(config-router)# neighbor 192.168.2.2 interface branch_office
```

관련 명령

명령	설명
debug eigrp neighbors	EIGRP 인접 디바이스 메시지에 대한 디버그 정보를 표시합니다.
show eigrp neighbors	EIGRP 인접 디바이스 테이블을 표시합니다.

neighbor activate

BGP(Border Gateway Protocol) 인접 디바이스와의 정보 교환을 활성화하려면 주소군 컨피그레이션 모드에서 **neighbor activate** 명령을 사용합니다. BGP 인접 디바이스와의 주소 교환을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **activate**

no neighbor{*ip_address*} **activate**

구문 설명

ip_address	BGP 라우터의 IP 주소

기본값

BGP 인접 디바이스와의 주소 교환은 IPv4 주소군에 대해 기본적으로 활성화되어 있습니다. 다른 주소군에 대해서는 주소 교환을 활성화할 수 없습니다.

참고 **neighbor remote-as** 명령으로 정의한 각 BGP 라우팅 세션에 대해서는 IPv4 주소군과의 주소 교환이 기본적으로 활성화됩니다. 단, **neighbor remote-as** 명령을 구성하기 전에 **no bgp default ipv4-activate** 명령을 구성하지 않는 경우 또는 **no neighbor activate** 명령을 사용하여 특정 인접 디바이스와의 주소 교환을 비활성화하지 않은 경우에 한합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

IP 접두사 형식으로 주소 정보를 광고하려면 이 명령을 사용할 수 있습니다. 주소 접두사 정보는 BGP에서 NLRI(Network Layer Reachability Information)로 알려져 있습니다.

예

다음 예는 BGP 인접 디바이스 172.16.1.1에 대한 IPv4 주소군 유니캐스트의 주소 교환을 활성화합니다.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 4
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

다음 예는 group2라는 이름의 BGP 피어 그룹에 있는 모든 인접 디바이스 및 BGP 인접 디바이스 7000::2에 대한 주소군 IPv6의 주소 교환을 활성화하는 방법을 보여줍니다.

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

관련 명령

명령	설명
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.

neighbor advertise-map

구성된 경로 맵과 일치하는 BGP 테이블에서 경로를 광고하려면 라우터 컨피그레이션 모드에서 **neighbor advertise-map** 명령을 사용합니다. 경로 광고를 비활성화하려면 이 명령의 no 형식을 사용합니다.

neighbor {*ipv4-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}[**check-all-paths**]

no neighbor {*ipv4-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}[**check-all-paths**]

구문 설명

ipv4_address	조건부 광고를 수신해야 하는 라우터의 IPv4 주소를 지정합니다.
ipv6_address	조건부 광고를 수신해야 하는 라우터의 IPv6 주소를 지정합니다.
advertise-map *map-name*	exist 맵 또는 non-exist 맵의 조건이 충족될 경우 알릴 경로 맵의 이름입니다.
exist-map *map-name*	exist-map의 이름을 BGP 테이블의 경로와 비교하여 advertise-map 경로의 광고 여부를 결정합니다.
non-exist-map *map-name*	non-exist-map의 이름을 BGP 테이블의 경로와 비교하여 advertise-map 경로의 광고 여부를 결정합니다.
check-all-paths	(선택 사항) BGP 테이블의 접두사를 통해 모든 경로를 exist-map으로 확인할 수 있도록 허용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

선택한 경로를 조건부로 광고하려면 neighbor advertise-map 명령을 사용합니다. 조건부로 광고할 경로(접두사)는 두 개의 경로 맵(advertise map 및 exist map 또는 non-exist map)에서 정의됩니다.

exist map 또는 non-exist map과 연결된 경로 맵은 BGP 스피커가 추적하는 접두사를 지정합니다.

advertise map과 연결된 경로 맵은 조건이 충족될 때 지정된 인접 디바이스로 광고할 접두사를 지정합니다.

exist map을 구성하면, advertise map과 exist map에 모두 접두사가 존재하는 경우 조건이 충족됩니다.

non-exist map을 구성하면, advertise map에는 접두사가 존재하지만 non-exist map에는 존재하지 않는 경우 조건이 충족됩니다.

조건이 충족되지 않으면 경로가 취소되고 조건부 광고가 발생하지 않습니다. 조건부 광고가 발생하려면 동적으로 광고 여부를 결정할 수 있는 모든 경로가 BGP 라우팅 테이블에 존재해야 합니다.

예

다음 라우터 컨피그레이션 예는 모두를 확인하는 BGP를 구성합니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

다음 주소군 컨피그레이션 예는 non-exist map을 사용하여 접두사를 10.1.1.1 인접 디바이스에 조건부로 광고하도록 BGP를 구성합니다. 접두사가 MAP3에는 있지만 MAP4에는 없는 경우 조건이 충족되어 접두사가 광고됩니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

다음의 피어 그룹 컨피그레이션 예는 모든 경로에서 BGP 인접 디바이스에 대한 접두사를 확인하도록 BGP를 구성합니다.

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute static
ciscoasa(config-router-af)# neighbor route1 send-community both
ciscoasa(config-router-af)# neighbor route1 advertise-map MAP1 exist-map MAP2
check-all-paths
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.

neighbor advertisement-interval

BGP 라우팅 업데이트 전송 간 MRAI(Minimum Route Advertisement Interval)를 설정하려면 주소군 컨피그레이션 모드에서 **neighbor advertisement-interval** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **advertisement-interval** *seconds*

no neighbor {*ip_address*} **advertisement-interval** *seconds*

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
seconds	BGP 라우팅 업데이트 전송 간 최소 시간 간격입니다. 유효한 값은 0~600입니다.

기본값

VRF에 있지 않은 eBGP 세션: 30초

VRF에 있는 eBGP 세션: 0초

iBGP 세션: 0초

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

MRAI가 0초이면 BGP 라우팅 테이블이 변경되자마자 BGP 라우팅 업데이트가 전송됩니다.

예

다음 예는 BGP 라우팅 업데이트 전송 간 최소 시간을 10초로 설정합니다.

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 advertisement-interval 10
```

관련 명령

명령	설명
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

neighbor default-originate

BGP 스피커(로컬 라우터)에서 인접 디바이스로 기본 경로 0.0.0.0을 전송하도록 허용하려면 주소군 컨피그레이션 모드에서 **neighbor default-originate** 명령을 사용합니다. 기본값으로 경로를 전송하지 않으려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **default-originate** [**route-map** *route-map name*]

no neighbor {*ip_address*} **default-originate** [**route-map** *route-map name*]

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
route-map *route-map name*	(선택 사항) 경로 맵의 이름입니다. 경로 맵을 사용하면 경로 0.0.0.0을 조건부로 삽입할 수 있습니다.

기본값

인접 디바이스로 기본 경로가 전송되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하기 위해 로컬 라우터에 0.0.0.0이 있어야 할 필요는 없습니다. 경로 맵과 함께 사용할 경우, 경로 맵에 **match ip address** 구문이 포함되어 있고 IP 액세스 목록과 정확히 일치하는 경로가 있으면 기본 경로 0.0.0.0이 삽입됩니다. 경로 맵에는 다른 일치 구문도 포함할 수 있습니다.

표준 또는 확장 액세스 목록을 **neighbor default-originate** 명령과 함께 사용할 수 있습니다.

예

다음 예에서 로컬 라우터는 경로 0.0.0.0을 인접 디바이스 72.16.2.3에 조건 없이 삽입합니다.

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 default-originate
```

다음 예에서 로컬 라우터는 경로 0.0.0.0을 인접 디바이스 2001::1에 삽입합니다.

```
asa(config-router-af)#neighbor 2001::1 default-originate route-map default-map
```

관련 명령

명령	설명
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

neighbor description

설명을 인접 디바이스와 연결하려면 주소군 컨피그레이션 모드에서 **neighbor description** 명령을 사용합니다. 설명을 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **description** *text*

no neighbor {*ip_address*} **description** *text*

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
text	인접 디바이스를 설명하는 텍스트(길이 최대 80자).

기본값

인접 디바이스의 설명이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

예

다음 예에서 인접 디바이스의 설명은 "peer with example.com"입니다.

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 description peer with example.com
```

관련 명령

명령	설명
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

neighbor disable-connected-check

루프백 인터페이스를 사용하는 single-hop 피어와의 eBGP 피어링 세션을 설정하기 위해 연결 확인을 비활성화하려면 주소군 컨피그레이션 모드에서 **neighbor disable-connected-check** 명령을 사용합니다. eBGP 피어링 세션에 대한 연결 확인을 활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **disable-connected-check**

no neighbor {*ip_address*} **disable-connected-check**

구문 설명

ip_address	인접 라우터의 IP 주소입니다.

기본값

eBGP 피어가 기본적으로 동일한 네트워크 세그먼트에 직접 연결되어 있는지 확인하기 위해 BGP 라우팅 프로세스는 single-hop eBGP 피어링 세션(TTL=254)의 연결을 확인합니다. 피어가 동일한 네트워크에 직접 연결되어 있지 않은 경우 연결 확인을 수행하면 피어링 세션의 연결이 차단됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

neighbor disable-connected-check 명령은 single hop으로 도달 가능하지만 루프백 인터페이스에 구성되어 있거나 직접 연결되지 않은 IP 주소로 구성된 eBGP 피어링 세션에 대한 연결 확인 프로세스를 비활성화하는 데 사용됩니다.

neighbor ebgp-multihop 명령이 TTL 값 1로 구성된 경우에만 이 명령이 필요합니다. single-hop eBGP 피어의 주소는 도달 가능해야 합니다. BGP 라우팅 프로세스에서 피어링 세션에 대해 루프백 인터페이스를 사용하도록 허용하려면 **neighbor update-source** 명령을 구성해야 합니다.

예

다음 예에서는 각 라우터의 로컬 루프백 인터페이스를 통해 동일한 네트워크 세그먼트에서 도달할 수 있는 두 개의 BGP 피어 간에 single-hop eBGP 피어링 세션이 구성됩니다.

BGP 피어 1

```
ciscoasa(config)# interface loopback1
ciscoasa(config-if)# ip address 10.0.0.100 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 64512
ciscoasa(config-router)# neighbor 192.168.0.200 remote-as 65534
ciscoasa(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
```

```
ciscoasa(config-router)# neighbor 192.168.0.200 update-source loopback2
ciscoasa(config-router)# neighbor 192.168.0.200 disable-connected-check
```

BGP 피어 2

```
ciscoasa(config)# interface loopback2
ciscoasa(config-if)# ip address 192.168.0.200 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 65534
ciscoasa(config-router)# neighbor 10.0.0.100 remote-as 64512
ciscoasa(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
ciscoasa(config-router)# neighbor 10.0.0.100 update-source loopback1
ciscoasa(config-router)# neighbor 10.0.0.100 disable-connected-check
```

관련 명령

명령	설명
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.
neighbor ebgp-multihop	직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시작합니다.

neighbor distribute-list

액세스 목록에 지정된 대로 BGP 인접 디바이스 정보를 배포하려면 주소군 컨피그레이션 모드에서 **neighbor distribute-list** 명령을 사용합니다. 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor *ip_address* **distribute-list** {*access-list-name*} {**in** | **out**}

no neighbor *ip_address* **distribute-list** {*access-list-name*} {**in** | **out**}

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
access-list-name	표준 액세스 목록의 이름입니다.
in	액세스 목록이 해당 인접 디바이스의 들어오는 광고에 적용됩니다.
out	액세스 목록이 해당 인접 디바이스의 나가는 광고에 적용됩니다.

기본값

BGP 인접 디바이스가 지정되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

배포 목록 사용은 광고를 필터링하는 여러 방법 중 하나입니다. 다음 방법을 사용하여 광고를 필터링할 수도 있습니다.

- **ip as-path access-list** 및 **neighbor filter-list** 명령으로 자동 시스템 경로 필터를 구성할 수 있습니다.
- 광고 필터링을 위한 표준 액세스 목록을 구성하는 데 **access-list (IP standard)** 명령을 사용할 수 있습니다.
- 광고를 필터링하는 데 **route-map (IP)** 명령을 사용할 수 있습니다. 경로 맵은 자동 시스템 필터, 접두사 필터, 액세스 목록 및 배포 목록으로 구성할 수 있습니다.

라우팅 업데이트를 필터링하는 데 표준 액세스 목록을 사용할 수 있습니다. 그러나 CIDR(Classless Inter-Domain Routing)을 사용하여 경로를 필터링하는 경우, 표준 액세스 목록은 네트워크 주소 및 마스크의 고급 필터링 구성에 필요한 세분화 수준을 제공하지 못합니다.

예

다음의 예에서는 표준 액세스 목록 distribute-list-acl의 BGP 인접 디바이스 정보가 172.16.4.1 인접 디바이스에 대한 들어오는 광고에 적용됩니다.

```
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af) neighbor 172.16.4.1 distribute-list distribute-list-acl in
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
network	BGP에서 광고할 네트워크를 지정합니다.
access-list permit	전달할 패킷을 지정합니다.
access-list deny	거부할 패킷을 지정합니다.

neighbor ebgp-multihop

직접 연결되지 않은 네트워크에 상주하는 외부 피어에 대한 BGP 연결을 허용 및 시도하려면 주소군 컨피그레이션 모드에서 **neighbor ebgp-multihop** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **ebgp-multihop [ttl]**

no neighbor{*ip_address*} **ebgp-multihop**

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
ttl	(선택 사항) TTL(Time to live). 유효한 값은 홉(hop) 1~255입니다.

기본값

직접 연결된 인접 디바이스만 허용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 기능은 Cisco 기술 지원 직원의 감독하에서만 사용해야 합니다. 멀티 홉 피어에 대한 유일한 경로가 기본 경로 (0.0.0.0)인 경우, 진동 경로를 통해 루프가 생성되는 것을 방지하기 위해 멀티 홉이 설정되지 않습니다.

예

다음 예는 직접 연결되지 않은 네트워크에 상주하는 인접 디바이스 10.108.1.1과의 연결을 허용합니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af) neighbor 10.108.1.1 ebgp-multihop
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

neighbor filter-list

BGP 필터를 설정하려면 주소군 컨피그레이션 모드에서 **neighbor filter-list** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **filter-list** *access-list-name* {**in** | **out**}

no neighbor {*ip_address*} **filter-list** *access*-list-name {**in** | **out**}

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
access-list-name	자동 시스템 경로 액세스 목록의 이름입니다. **as-path access-list** 명령으로 이 액세스 목록을 정의합니다.
in	액세스 목록이 들어오는 경로에 적용됩니다.
out	액세스 목록이 나가는 경로에 적용됩니다.

명령 기본값

BGP 필터가 사용되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 인바운드 및 아웃바운드 BGP 경로에서 모두 필터를 설정합니다.

참고 어느 한 방향에서(인바운드 또는 아웃바운드) 인접 디바이스에 **neighbor distribute-list** 및 **neighbor prefix-list** 명령을 모두 적용해서는 안 됩니다. 이 두 명령은 상호 배타적이므로 인바운드와 아웃바운드 방향에 각각 하나의 명령(**neighbor distribute-list** 또는 **neighbor prefix-list**)만 적용할 수 있습니다.

예

다음 주소군 컨피그레이션 모드 예에서, 인접한 자동 시스템 123을 통과하는 어떤 경로에 대한 광고도 IP 주소 172.16.1.1의 BGP 인접 디바이스에 전송되지 않습니다.

```
ciscoasa(config)# as-path access-list as-path-acl deny _123_
ciscoasa(config)# as-path access-list as-path-acl deny ^123$
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# neighbor 172.16.1.1 filter-list as-path-acl out
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.
network	BGP 라우팅 프로세스가 광고할 네트워크를 지정합니다.

neighbor ha-mode graceful-restart

BGP(Border Gateway Protocol) 인접 디바이스에 대한 BGP Graceful Restart 기능을 활성화 또는 비활성화하려면 주소군 컨피그레이션 모드에서 neighbor ha-mode graceful-restart 명령을 사용합니다. 컨피그레이션에서 인접 디바이스에 대한 BGP Graceful Restart 기능을 제거하려면 이 명령의 no 형식을 사용합니다.

neighbor *ip_address* **ha-mode graceful-restart** [**disable**]

no neighbor *ip_address* **ha-mode graceful-restart**

구문 설명

ip_address	인접 디바이스의 IP 주소.
disable	(선택 사항) 인접 디바이스에 대한 BGP Graceful Restart 기능을 비활성화합니다.

명령 기본값

BGP Graceful Restart 기능이 비활성화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

neighbor ha-mode graceful-restart 명령은 개별 BGP 인접 디바이스에 대한 Graceful Restart 기능을 활성화 또는 비활성화하는 데 사용됩니다. Graceful Restart가 전에 BGP 피어에 대해 활성화된 경우 Graceful Restart 기능을 비활성화하려면 disable 키워드를 사용합니다.

Graceful Restart 기능은 세션 설정 중에 OPEN 메시지에서 NSF(Nonstop Forwarding) 지원 피어 및 NSF 인식 피어 간에 협상됩니다. BGP 세션이 설정된 후 Graceful Restart 기능이 활성화되면 소프트 또는 하드 리셋으로 세션을 다시 시작해야 합니다.

Graceful Restart 기능은 NSF 지원 및 NSF 인식 ASA에서 지원됩니다. NSF 지원 ASA는 SSO(Stateful Switchover) 작업(Graceful Restart)을 수행할 수 있으며, SSO 작업 중 라우팅 테이블 정보를 유지하여 피어 다시 시작을 지원할 수 있습니다. NSF 인식 ASA는 NSF 지원 라우터처럼 작동하지만 SSO 작업을 수행할 수 없습니다.

참고 모든 BGP 인접 디바이스에서 BGP Graceful Restart 기능을 전체적으로 활성화하려면 **bgp graceful-restart** 명령을 사용합니다. 개별 인접 디바이스에 대해 BGP Graceful Restart 기능을 구성하는 경우, 각 Graceful Restart 구성 방법은 동일한 우선순위를 갖게 되며 마지막 컨피그레이션 인스턴스가 인접 디바이스에 적용됩니다.

BGP 인접 디바이스에 대한 BGP Graceful Restart 컨피그레이션을 확인하려면 show bgp neighbors 명령을 사용합니다.

예

다음 예는 BGP 인접 디바이스 172.21.1.2에 대한 BGP Graceful Restart 기능을 활성화합니다.

```
Ciscoasa(config)# router bgp 45000
Ciscoasa(config-router)# bgp log-neighbor-changes
Ciscoasa(config-router)# address-family ipv4 unicast
Ciscoasa(config-router-af)# neighbor 172.21.1.2 remote-as 45000
Ciscoasa(config-router-af)# neighbor 172.21.1.2 activate
Ciscoasa(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart
```

관련 명령

명령	설명
bgp graceful-restart	모든 BGP 인접 디바이스에 대한 BGP Graceful Restart 기능을 전체적으로 활성화 또는 비활성화합니다.
show bgp neighbors	인접 디바이스에 대한 TCP 및 BGP 연결에 관한 정보를 표시합니다.

neighbor local-as

eBGP(external Border Gateway Protocol) 인접 디바이스에서 수신한 경로의 AS_PATH 특성을 사용자 지정하려면 주소군 컨피그레이션 모드에서 **neighbor local-as** 명령을 사용합니다. AS_PATH 특성 사용자 지정을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]

no neighbor {*ip_address*} **local-as**

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
autonomous-system-number	(선택 사항) AS_PATH 특성에 접두사로 추가할 자동 시스템의 번호입니다. 이 인수의 값 범위는 1~65535의 유효한 자동 시스템 번호입니다. **참고** 이 인수를 사용하면 로컬 BGP 라우팅 프로세스 또는 원격 피어의 네트워크에서 자동 시스템 번호를 지정할 수 없습니다. 자동 시스템 번호 형식에 대한 자세한 내용은 **router bgp** 명령을 참조하십시오.
no-prepend	(선택 사항) 로컬 자동 시스템 번호를 eBGP 인접 디바이스에서 수신한 경로에 접두사로 추가하지 않습니다.
replace-as	(선택 사항) 실제 자동 시스템 번호를 eBGP 업데이트의 로컬 자동 시스템 번호로 교체합니다. 로컬 BGP 라우팅 프로세스에서의 자동 시스템 번호는 접두사로 추가되지 않습니다.
dual-as	(선택 사항) 실제 자동 시스템 번호(로컬 BGP 라우팅 프로세스에서)를 사용하거나 *autonomous-system-number* 인수(local-as)로 구성된 자동 시스템 번호를 사용하여 피어링 세션을 설정하도록 eBGP 인접 디바이스를 구성합니다.

명령 기본값

기본적으로 로컬 BGP 라우팅 프로세스에서의 자동 시스템 번호가 모든 외부 경로에 접두사로 추가됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

neighbor local-as 명령은 eBGP 인접 디바이스에서 수신하는 경로에 대한 자동 시스템 번호를 추가 및 제거하여 AS_PATH 특성을 사용자 지정하는 데 사용됩니다. 이 명령의 컨피그레이션은 라우터가 자동 시스템 번호 마이그레이션을 위해 외부 피어에 또 다른 자동 시스템의 멤버로서 표시되도록 허용합니다. 이 기능은 기존 피어링 정돈 작업을 방해하지 않은 채 네트워크 운영자가 고객을 새로운 컨피그레이션으로 마이그레이션하도록 허용함으로써 BGP 네트워크에서 자동 시스템 번호를 변경하는 프로세스를 간소화합니다.

주의 BGP는 네트워크 도달 정보를 유지하고 라우팅 루프를 예방하기 위해 경로가 이동하는 각 BGP 네트워크에서 자동 시스템을 접두사로 추가합니다. 이 명령은 자동 시스템 마이그레이션에 대해 구성해야 하고 이전이 완료된 후에 제거해야 합니다. 이 절차는 숙련된 네트워크 운영자만 시도해야 합니다. 라우팅 루프가 부적절한 컨피그레이션을 통해 생성될 수 있습니다.

이 명령은 실제 eBGP 피어링 세션에만 사용할 수 있습니다. 이 명령은 연합의 서로 다른 하위 자동 시스템에 있는 두 개의 피어에 대해 작동하지 않습니다.

원활한 전환을 보장하려면, 4바이트 자동 시스템 번호로 식별되는 자동 시스템 내에 있는 모든 BGP 스피커를 4바이트 자동 시스템 번호를 지원하도록 업그레이드하는 것이 좋습니다.

예

Local-AS 예

다음 예는 local-as 기능을 사용하여 자동 시스템 300을 통해 라우터 1과 라우터 2 사이에 피어링을 설정합니다.

라우터 1(로컬 라우터)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.1.1 local-as 300
```

라우터 2(원격 라우터)

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.0.0.1 remote-as 300
```

No-prepend 키워드 컨피그레이션 예

다음 예는 192.168.1.1 인접 디바이스에서 수신하는 경로에 자동 시스템 500을 접두사로 추가하지 않도록 BGP를 구성합니다.

```
ciscoasa(config)# router bgp 400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.0.0
ciscoasa(config-router-af)# neighbor 192.168.1.1 local-as 500 no-prepend
```

Replace-as 키워드 컨피그레이션 예

다음 예는 172.20.1.1 인접 디바이스에 대한 아웃바운드 라우팅 업데이트에서 비공개 자동 시스템 64512를 제거하고 이를 자동 시스템 600으로 교체합니다.

```
ciscoasa(config)# router bgp 64512
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.20.1.1 local-as 600 no-prepend replace-as
ciscoasa(config-router-af)# neighbor 172.20.1.1 remove-private-as
```

Dual-as 키워드 컨피그레이션 예

다음 예는 두 개의 공급자 네트워크 및 하나의 고객 네트워크에 대한 컨피그레이션을 보여줍니다. 라우터 1은 자동 시스템 100에 속하고 라우터 2는 자동 시스템 200에 속합니다. 자동 시스템 200은 자동 시스템 100으로 병합됩니다. 이 변환은 자동 시스템 300(고객 네트워크)에서 라우터 3에 대한 서비스를 중단하지 않은 채 발생해야 합니다. **neighbor local-as** 명령은 이 변환 중에 라우터 3이 자동 시스템 200과의 피어링을 유지할 수 있도록 라우터 1에서 구성됩니다. 변환이 완료되면 정상적인 유지 관리 기간 중에 또는 기타 예약된 다운타임 중에 자동 시스템 100과 피어링되도록 라우터 3의 컨피그레이션이 업데이트됩니다.

라우터 1 컨피그레이션(로컬 공급자 네트워크)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
ciscoasa(config-router-af)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

라우터 2 컨피그레이션(원격 공급자 네트워크)

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
```

라우터 3 컨피그레이션(원격 고객 네트워크)

```
ciscoasa(config)# router bgp 300
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.3
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 200
```

두 개의 자동 시스템이 병합된 후 마이그레이션을 완료하기 위해 라우터 3에서 피어링 세션이 업데이트됩니다.

```
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 100
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
bgp router-id	로컬 BGP(Border Gateway Protocol) 라우팅 프로세스에 대한 고정 라우터 ID를 구성합니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.
network	BGP 라우팅 프로세스가 광고할 네트워크를 지정합니다.
synchronization	BGP와 IGP(Interior Gateway Protocol) 시스템 간 동기화를 활성화합니다.

neighbor maximum-prefix

인접 디바이스에서 수신할 수 있는 접두사 수를 제어하려면 주소군 컨피그레이션 모드에서 **neighbor maximum-prefix** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]

no neighbor {*ip_address*} **maximum-prefix** *maximum*

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
maximum	이 인접 디바이스에서 허용되는 접두사의 최대 수.
threshold	(선택 사항) 라우터가 경고 메시지 생성을 시작할 *maximum* 비율을 지정하는 정수. 범위는 1~100이고, 기본값은 75(퍼센트)입니다.
restart	(선택 사항) 접두사 최대 수 제한을 초과하여 비활성화된 피어링 세션을 자동으로 다시 설정할 수 있도록 BGP를 실행하는 라우터를 구성합니다. restart 타이머는 *restart-interval* 인수로 구성됩니다.
restart-interval	(선택 사항) 피어링 세션이 다시 설정되는 시간 간격 (분). 범위는 1~65535 분입니다 .
warning-only	(선택 사항) *maximum*을 초과하면 피어링을 종료하는 대신 라우터가 로그 메시지를 생성하도록 허용합니다.

명령 기본값

이 명령은 기본적으로 비활성화되어 있습니다. 접두사 수에는 제한이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 BGP 라우터가 피어에서 수신할 수 있는 접두사의 최대 수를 구성할 수 있습니다. 또한 배포 목록, 필터 목록, 경로 맵 외에도 피어에서 수신하는 접두사를 제어하기 위한 또 다른 메커니즘을 추가합니다.

수신한 접두사의 수가 구성된 최대 수를 초과하면 라우터가 피어링을 종료합니다(기본값). 그러나 **warning-only** 키워드를 구성하면, 라우터가 대신 로그 메시지를 전송하되 발신자와의 피어링을 계속 진행합니다. 피어가 종료되면 **clear bgp** 명령을 실행할 때까지 종료 상태가 유지됩니다.

예

다음 예는 192.168.6.6의 인접 디바이스에서 허용되는 접두사의 최대 수를 1000으로 설정합니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 maximum-prefix 1000
```

다음 예는 2001::1의 인접 디바이스에서 허용되는 접두사의 최대 수를 1000으로 설정합니다.

```
ciscoasa(config-router-af)# neighbor 2001::1 maximum-prefix 1000
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
network	BGP 라우팅 프로세스가 광고할 네트워크를 지정합니다.

neighbor next-hop-self

라우터를 BGP-speaking 인접 디바이스에 대한 next hop으로 구성하려면 주소군 컨피그레이션 모드에서 **neighbor next-hop-self** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **next-hop-self**

no neighbor {*ip_address*} **next-hop-self**

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
warning-only	(선택 사항) *maximum*을 초과하면 피어링을 종료하는 대신 라우터가 로그 메시지를 생성하도록 허용합니다.

명령 기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 BGP 인접 디바이스가 동일한 IP 서브넷의 다른 모든 인접 디바이스에 직접 액세스하지 못할 수 있는 unmeshed 네트워크(예: Frame Relay 또는 X.25)에서 유용합니다.

예

다음 예는 10.108.1.1에 대한 모든 업데이트가 이 라우터를 next hop으로 광고하도록 지정합니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 next-hop-self
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

neighbor password

TCP 연결에서 두 BGP 피어 간 MD5(Message Digest5) 인증을 활성화하려면 주소군 컨피그레이션 모드에서 **neighbor password** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **password** [**0-7**] *string*

no neighbor {*ip_address*} **password**

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
string	대/소문자를 구분하는 최대 25자의 비밀번호. 첫 번째 문자는 숫자가 될 수 없습니다. 문자열은 공백을 포함하여 모든 영숫자 문자를 포함할 수 있습니다. *number-space-anything* 형식의 비밀번호는 지정할 수 없습니다. 숫자 뒤에 공백이 오면 인증이 실패할 수 있습니다.
0-7	(선택 사항) 암호화 유형. 0~6은 암호화가 없고, 7은 암호화에 사용됩니다.

명령 기본값

MD5는 TCP 연결에서 두 BGP 피어 간에 인증되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

두 BGP 피어 간 MD5 인증을 구성할 수 있습니다. 이렇게 하면 피어 간 TCP 연결에서 전송되는 각 세그먼트가 확인됩니다. 두 BGP 피어에서 동일한 비밀번호로 MD5 인증을 구성해야 합니다. 그렇게 하지 않으면 두 BGP 피어 간에 연결이 설정되지 않습니다. MD5 인증을 구성하면 Cisco ASA 소프트웨어는 TCP 연결에서 전송되는 모든 세그먼트의 MD5 digest를 생성 및 확인합니다.

구성 시 **service password-encryption** 명령의 활성화 여부와 상관없이 최대 25자의 대/소문자를 구분하는 비밀번호를 제공할 수 있습니다. 비밀번호의 길이가 25자를 넘으면 오류 메시지가 표시되고 비밀번호가 허용되지 않습니다. 문자열은 공백을 포함하여 모든 영숫자 문자를 포함할 수 있습니다. 비밀번호는 숫자-공백-문자 형식으로 구성할 수 없습니다. 숫자 뒤에 공백이 오면 인증이 실패할 수 있습니다. 또한 다음의 기호 문자를 영숫자와 함께 사용할 수 있습니다.

` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > < . , ?

주의 인증 문자열을 잘못 구성하면 BGP 피어링 세션이 설정되지 않습니다. 인증 문자열을 신중하게 입력할 것과 인증이 구성된 후 피어링 세션이 설정되는지 확인할 것을 권장합니다.

한 라우터에는 인접 라우터에 대해 구성된 비밀번호가 있지만 인접 라우터에는 없는 경우, 두 라우터 간에 BGP 세션을 설정하려고 시도할 때 콘솔에 다음과 같은 메시지가 나타납니다.

%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179

마찬가지로, 두 라우터에 서로 다른 비밀번호가 구성되어 있으면 화면에 다음과 같은 메시지가 나타납니다.

%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179

설정된 BGP 세션에서 MD5 비밀번호 구성

두 BGP 피어 간의 MD5 인증에 사용되는 비밀번호 또는 키를 구성하거나 변경하면, 비밀번호가 구성된 후 로컬 라우터에서 기존 세션을 종료하지 않습니다. 로컬 라우터는 BGP 보류 타이머가 만료될 때까지 새 비밀번호를 사용하여 피어링 세션을 유지하려고 시도합니다. 기본 시간은 180초입니다. 보류 타이머가 만료되기 전에 원격 라우터에서 비밀번호를 입력하거나 변경하지 않으면 세션이 시간 초과됩니다.

참고 보류 타이머에 대해 새 타이머 값을 구성하면 세션이 재설정된 후에 적용됩니다. 따라서 BGP 세션을 재설정하지 않은 채 보류 타이머의 컨피그레이션을 변경하는 것은 불가능합니다.

예 다음 예는 10.108.1.1 인접 디바이스와의 피어링 세션에 대해 MD5 인증을 구성합니다. 보류 타이머가 만료되기 전에 원격 피어에서 동일한 비밀번호를 구성해야 합니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 password bla4u00=2nkq
```

다음 예는 **service password-encryption** 명령이 비활성화될 때 25자가 넘는 비밀번호를 구성합니다.

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 2.2.2.2
ciscoasa(config-router-af)# neighbor remote-as 3
ciscoasa(config-router-af)# neighbor 209.165.200.225 password 12345678912345678912345678901
% BGP: Password length must be less than or equal to 25.
ciscoasa(config-router-af)# do show run | i password
no service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

다음 예에서는 **service password-encryption** 명령이 활성화될 때 25자가 넘는 비밀번호를 구성하는 경우 오류 메시지가 표시됩니다.

```
Router(config)# service password-encryption
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901
% BGP: Password length must be less than or equal to 25.
Router(config-router)# do show run | i password service password-encryption
 neighbor 209.165.200.225 password 123456789123456789123456
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
bgp router-id	로컬 BGP(Border Gateway Protocol) 라우팅 프로세스에 대한 고정 라우터 ID를 구성합니다.
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가합니다.

neighbor prefix-list

접두사 목록에 지정된 대로 BGP(Border Gateway Protocol) 인접 디바이스 정보의 배포를 차단하려면 주소군 컨피그레이션 모드에서 **neighbor prefix-list** 명령을 사용합니다. 필터 목록을 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **prefix-list** *prefix-list-name* {**in** | **out**}

no neighbor {*ip_address*} **p prefix-list** *prefix-list-name* {**in** | **out**}

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
prefix-list-name	접두사 목록의 이름입니다.
in	필터 목록이 해당 인접 디바이스에서 들어오는 광고에 적용됩니다.
out	필터 목록이 해당 인접 디바이스로 나가는 광고에 적용됩니다.

명령 기본값

모든 외부 및 광고된 주소 접두사는 BGP 인접 디바이스에 배포됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

접두사 목록 사용은 BGP 광고를 필터링하는 세 가지 방법 중 하나입니다. 또한 **ip as-path access-list** 글로벌 컨피그레이션 명령으로 정의되고 **neighbor filter-list** 명령에서 사용되는 AS-path 필터를 사용하여 BGP 광고를 필터링할 수도 있습니다. BGP 광고를 필터링하는 세 번째 방법은 액세스 또는 접두사 목록을 **neighbor distribute-list** 명령과 함께 사용하는 것입니다.

참고 어느 한 방향에서(인바운드 또는 아웃바운드) 인접 디바이스에 **neighbor distribute-list** 및 **neighbor prefix-list** 명령을 모두 적용해서는 안 됩니다. 이 두 명령은 상호 배타적이므로 인바운드와 아웃바운드 방향에 각각 하나의 명령(**neighbor distribute-list** 또는 **neighbor prefix-list**)만 적용할 수 있습니다.

예

다음의 주소군 컨피그레이션 모드 예에서는 인접 디바이스 10.23.4.1에서 들어오는 광고에 *abc*라는 접두사 목록을 적용합니다.

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.1.2
ciscoasa(config-router-af)# neighbor 10.23.4.1 prefix-list abc in
```

다음의 주소군 라우터 컨피그레이션 모드 예에서는 인접 디바이스 10.23.4.3으로 나가는 광고에 CustomerA라는 접두사 목록을 적용합니다.

```
ciscoasa(config)# router bgp 64800
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.3.6
ciscoasa(config-router-af)# neighbor 10.23.4.3 prefix-list CustomerA out
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
network	BGP 라우팅 프로세스가 광고할 네트워크를 지정합니다.

neighbor remote-as

BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 테이블에 엔트리를 추가하려면 주소군 컨피그레이션 모드에서 **neighbor remote-as** 명령을 사용합니다. 테이블에서 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **remote-as** *autonomous-system-number*

no neighbor {*ip_address*} **remote-as** *autonomous-system-number*

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
autonomous-system-number	인접 디바이스가 속한 자동 시스템의 번호(범위 1~65535). 자동 시스템 번호 형식에 대한 자세한 내용은 **router bgp** 명령을 참조하십시오. **alternate-as** 키워드와 함께 사용하면 최대 5개의 자동 시스템 번호를 입력할 수 있습니다.

명령 기본값

BGP 또는 MBGP(Multiprotocol BGP) 인접 디바이스 피어가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

router bgp 글로벌 컨피그레이션 명령으로 지정한 자동 시스템 번호와 일치하는 자동 시스템 번호로 인접 디바이스를 지정하면 해당 인접 디바이스는 로컬 자동 시스템에 대해 internal로 식별됩니다. 그러지 않은 경우 해당 인접 디바이스는 external로 식별됩니다.

기본적으로 라우터 컨피그레이션 모드에서 **neighbor remote-as** 명령을 사용하여 정의한 인접 디바이스는 유니캐스트 주소 접두사만 교환합니다.

alternate-as 키워드를 사용하면 동적 BGP 인접 디바이스를 식별할 수 있는 최대 5개의 대체 자동 시스템을 지정할 수 있습니다. BGP 동적 인접 디바이스 지원에 따라 IP 주소 범위로 정의한 원격 인접 디바이스 그룹에 대한 BGP 피어링이 허용됩니다. BGP 동적 인접 디바이스는 IP 주소 범위 및 BGP 피어 그룹을 사용하여 구성됩니다. **bgp listen** 명령을 사용하여 서브넷 범위를 구성하고 BGP 피어 그룹과 연결한 다음 서브넷 범위의 IP 주소에 대해 TCP 세션을 시작하면 새로운 BGP 인접 디바이스가 해당 그룹의 멤버로서 동적으로 생성됩니다. 새로운 BGP 인접 디바이스는 그룹에 대한 컨피그레이션 또는 템플릿을 상속합니다.

Cisco의 4바이트 자동 시스템 번호 구현에서는 자동 시스템 번호에 대한 기본 정규식 일치 및 출력 표시 형식으로서 asplain(예: 65538)을 사용합니다. 그러나 RFC 5396에 설명된 대로 asplain 형식 및 asdot 형식 모두로 4바이트 자동 시스템 번호를 구성할 수 있습니다. 4바이트 자동 시스템 번호의 기본 정규식 일치 및 출력 표시를 asdot 형식으로 변경하려면 **bgp asnotation dot** 명령과 **clear bgp *** 명령을 차례로 사용하여 현재의 모든 BGP 세션에 대해 하드 리셋을 수행합니다.

예

다음 예는 주소 10.108.1.2의 라우터가 자동 시스템 번호 65200의 iBGP(internal BGP) 인접 디바이스임을 지정합니다.

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 10.108.1.2 remote-as 65200
```

다음 예는 BGP 라우터를 자동 시스템 65400에 할당합니다. 두 개의 네트워크가 자동 시스템에서 나오는 것으로 나열되고, 그 다음에는 세 개의 원격 라우터 주소(및 해당 자동 시스템)가 나열됩니다. 구성 중인 라우터는 네트워크 10.108.0.0 및 192.168.7.0에 대한 정보를 인접 라우터와 공유합니다. 첫 번째 라우터는 이 컨피그레이션이 입력된 라우터에서 오는 다른 자동 시스템의 원격 라우터입니다. 두 번째 **neighbor remote-as** 명령은 주소 10.108.234.2의 internal BGP 인접 디바이스(동일한 자동 시스템 번호와 함께)를 표시합니다. 마지막 **neighbor remote-as** 명령은 이 컨피그레이션이 입력된 라우터에서 오는 다른 네트워크의 인접 디바이스(및 eBGP 인접 디바이스)를 지정합니다.

```
ciscoasa(config)# router bgp 65400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# network 192.168.7.0
ciscoasa(config-router-af)# neighbor 10.108.200.1 remote-as 65200
ciscoasa(config-router-af)# neighbor 10.108.234.2 remote-as 65400
ciscoasa(config-router-af)# neighbor 172.29.64.19 remote-as 65300
```

다음 예는 유니캐스트 경로만 교환할 수 있도록 자동 시스템 65001의 인접 디바이스 10.108.1.1을 구성합니다.

```
ciscoasa(config)# router bgp 65001
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.31 1.2 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.2 remote-as 65002
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
network	BGP 라우팅 프로세스가 광고할 네트워크를 지정합니다.
neighbor remove private-as	eBGP 아웃바운드 라우팅 업데이트에서 비공개 자동 시스템 번호를 제거합니다.

neighbor remove-private-as

eBGP 아웃바운드 라우팅 업데이트에서 비공개 자동 시스템 번호를 제거하려면 주소군 컨피그레이션 모드에서 **neighbor remove-private-as** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **remove-private-as** [**all** [**replace-as**]]

no neighbor {*ip_address*} **remove-private-as** [**all** [**replace-as**]]

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
all	(선택 사항) 나가는 업데이트의 AS 경로에서 모든 비공개 AS 번호를 제거합니다.
replace-as	(선택 사항) **all** 키워드를 지정하고 **replace-as** 키워드를 지정하면 AS 경로의 모든 비공개 AS 번호가 라우터의 로컬 AS 번호로 교체됩니다.

명령 기본값

비공개 AS 번호가 AS 경로에서 제거되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 eBGP(external BGP) 인접 디바이스에만 이용할 수 있습니다. 비공개 AS 값의 범위는 64512~65535입니다. 외부 인접 디바이스로 업데이트를 전달할 때 AS 경로에 비공개 AS 번호가 포함되어 있으면, 소프트웨어에서는 비공개 AS 번호를 삭제합니다.

- 경로에 공개 및 비공개 ASN이 모두 포함되어 있더라도 **neighbor remove-private-as** 명령은 AS 경로에서 비공개 AS 번호를 제거합니다.
- 경로에 비공개 AS 번호만 포함되어 있더라도 **neighbor remove-private-as** 명령은 비공개 AS 번호를 제거합니다. 길이가 0인 AS 경로는 존재할 가능성이 없습니다. 이 명령은 eBGP 피어에만 적용되며, 이 경우 로컬 라우터의 AS 번호가 AS 경로에 첨부되기 때문입니다. AS 경로의 Confederation 세그먼트 전에 비공개 ASN이 나타나더라도 **neighbor remove-private-as** 명령은 비공개 AS 번호를 제거합니다.
- AS 경로에서 비공개 AS 번호를 제거하면 전송 중인 접두사의 경로 길이가 줄어듭니다. AS 경로 길이는 BGP 최적 경로 선택의 핵심 요소이기 때문에 경로 길이를 유지해야 할 수 있습니다. **replace-as** 키워드는 제거된 모든 AS 번호를 로컬 라우터의 AS 번호로 교체함으로써 경로 길이가 유지되도록 합니다.

- 이 기능은 주소군 단위로 인접 디바이스에 적용할 수 있습니다. 따라서 이 기능을 한 주소군의 인접 디바이스에는 적용하고 다른 주소군의 인접 디바이스에는 적용하지 않을 수 있습니다. 그러면 이 기능이 구성된 주소군에 대해서만 아웃바운드 측의 업데이트 메시지가 영향을 받습니다.

예

다음 예는 172.16.2.33으로 전송된 업데이트에서 비공개 AS 번호를 제거하는 컨피그레이션을 보여줍니다. 결과적으로, 10.108.1.1에서 AS 100을 통해 광고되는 경로에 대한 AS 경로는 "100"(자동 시스템 2051에 의해 표시되는 것처럼)만 포함하게 됩니다.

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 description peer with private-as
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.33 description eBGP peer
ciscoasa(config-router-af)# neighbor 172.16.2.33 remote-as 2051
ciscoasa(config-router-af)# neighbor 172.16.2.33 remove-private-as

Router-in-AS100# show bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
 Advertised to non peer-group peers:
   172.16.2.33
 65001
    10.108.1.1 from 10.108.1.1
     Origin IGP, metric 0, localpref 100, valid, external, best

Router-in-AS2501# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
    172.16.2.32 from 172.16.2.32
     Origin IGP, metric 0, localpref 100, valid, external, best
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor description	설명을 인접 디바이스와 연결합니다.
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 라우팅 엔트리를 라우팅 테이블에 추가합니다.

neighbor route-map

들어오는 경로 또는 나가는 경로에 경로 맵을 적용하려면 주소군 컨피그레이션 모드에서 **neighbor route-map** 명령을 사용합니다. 경로 맵을 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip_address*} **route-map** *map-name* {**in** | **out**}

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
map-name	경로 맵의 이름입니다.
in	들어오는 경로에 경로 맵을 적용합니다.
out	나가는 경로에 경로 맵을 적용합니다.

명령 기본값

피어에 경로 맵을 적용하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

주소군 컨피그레이션 모드에서 지정하는 경우 이 명령은 특정 주소군에만 경로 맵을 적용합니다. 라우터 컨피그레이션 모드에서 지정하는 경우 이 명령은 IPv4 유니캐스트 경로에만 경로 맵을 적용합니다.

아웃바운드 경로 맵이 지정된 경우, 경로 맵에서 적어도 한 섹션과 일치하는 경로만을 광고하는 것이 정상적인 동작입니다.

예

다음 예는 internal-map이라는 경로 맵을 172.16.70.24로부터의 BGP 들어오는 경로에 적용합니다.

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.24 route-map internal-map in
ciscoasa(config-router-af)# route-map internal-map
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
match as-path	액세스 목록에 지정된 BGP 자동 시스템 경로를 확인합니다.
route-map	하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의합니다.
match as-path	액세스 목록에 지정된 BGP 자동 시스템 경로를 확인합니다.
set local-preference	자동 시스템 경로의 기본 설정 값을 지정합니다.

neighbor send-community

BGP 인접 디바이스로 커뮤니티 특성을 전송하도록 지정하려면 주소군 컨피그레이션 모드에서 **neighbor send-community** 명령을 사용합니다. 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **send-community** [**both | standard**]

no neighbor{*ip_address*} **send-community** [**both | standard**]

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
both	(선택 사항) 표준 및 확장 커뮤니티를 모두 전송하도록 지정합니다.
standard	(선택 사항) 표준 커뮤니티만 전송하도록 지정합니다.

명령 기본값

인접 디바이스로 커뮤니티 특성이 전송되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

예

다음의 주소군 컨피그레이션 모드 예에서 라우터는 자동 시스템 109에 속하며 IP 주소 172.16.70.23의 인접 디바이스에 커뮤니티 특성을 전송하도록 구성됩니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.23 send-community
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.

neighbor shutdown

인접 디바이스를 비활성화하려면 주소군 컨피그레이션 모드에서 **neighbor shutdown** 명령을 사용합니다. 인접 디바이스를 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor *ip_address* **shutdown**

no neighbor *ip_address* **shutdown**

구문 설명

ip_address	인접 라우터의 IP 주소입니다.

명령 기본값

BGP 인접 디바이스의 상태를 변경하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

neighbor shutdown 명령은 지정한 인접 디바이스의 활성 세션을 종료하고 관련된 모든 라우팅 정보를 제거합니다.

BGP 인접 디바이스의 요약 정보를 표시하려면 **show bgp summary** 명령을 사용합니다. Idle 상태 및 Admin 엔트리의 인접 디바이스는 **neighbor shutdown** 명령으로 비활성화된 것입니다.

'State/PfxRcd'는 라우터가 인접 디바이스에서 수신한 접두사 수 또는 BGP 세션의 현재 상태를 보여줍니다. 최대 수(**neighbor maximum-prefix** 명령으로 설정)에 도달하면 'PfxRcd' 문자열이 엔트리에 나타나고, 인접 디바이스가 종료되고, 연결이 유휴 상태가 됩니다.

예

다음 예는 인접 디바이스 172.16.70.23의 활성 세션을 비활성화합니다.

```
ciscoasa(config-router-af)# neighbor 172.16.70.23 shutdown
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
show bgp summary	BGP 인접 디바이스 상태의 요약 정보를 표시합니다.

neighbor timers

특정 BGP 피어에 대한 타이머를 설정하려면 주소군 컨피그레이션 모드에서 **neighbor timers** 명령을 사용합니다. 특정 BGP 피어에 대한 타이머를 지우려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **timers** *keepalive* holdtime [*min- holdtime*]

no neighbor {*ip_address*} **timers**

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
keepalive	Cisco ASA 소프트웨어가 피어로 *keepalive* 메시지를 보내는 빈도(초)입니다. 기본값은 60초, 허용 범위는 0~65535입니다.
holdtime	소프트웨어가 데드 피어를 선언하는 *keepalive* 메시지를 수신하지 않은 이후의 간격(초)입니다. 기본값은 180초입니다. 범위는 0~65535입니다.
min-holdtime	(선택 사항) BGP 인접 디바이스로부터 허용 가능한 최소 보류 시간을 지정하는 간격(초). 허용 가능한 최소 보류 시간은 *holdtime* 인수로 지정한 간격보다 작거나 같아야 합니다. 범위는 0~65535입니다.

명령 기본값

Keepalive time: 60초

Holdtime: 180초

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

- 특정 인접 디바이스에 대해 구성된 타이머는 **timers bgp** 명령을 사용하여 모든 BGP 인접 디바이스에 대해 구성된 타이머를 재지정합니다.
- 20초 미만의 값으로 *holdtime* 인수를 구성하면 "A hold time of less than 20 seconds increases the chances of peer flapping."이라는 경고가 표시됩니다.
- 허용 가능한 최소 보류 시간 간격이 지정된 값보다 크면 "Minimum acceptable hold time should be less than or equal to the configured hold time."이라는 알림이 표시됩니다.

참고 허용 가능한 최소 보류 시간이 BGP 라우터에 구성되어 있으면, 원격 피어가 허용 가능한 최소 보류 시간보다 크거나 같은 보류 시간을 광고하는 경우에만 원격 BGP 피어 세션이 설정됩니다. 허용 가능한 최소 보류 시간 간격이 지정된 값보다 크면, 다음에 원격 세션이 연결을 시도할 때 실패하게 되며 로컬 라우터에서 "unacceptable hold time"이라는 알림을 전송합니다.

예

다음 예는 BGP 피어 192.168.47.0에 대해 keepalive 타이머를 70초, 보류 시간 타이머를 210초로 변경합니다.

```
ciscoasa(config-router-af)# neighbor 192.168.47.0 timers 70 210
```

다음 예는 BGP 피어 192.168.1.2에 대해 keepalive 타이머를 70초, 보류 시간 타이머를 130초, 최소 보류 시간 간격을 100초로 변경합니다.

```
ciscoasa(config-router-af)# neighbor 192.168.1.2 timers 70 130 100
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

neighbor transport

BGP(Border Gateway Protocol) 세션에 대해 TCP 전송 세션 옵션을 활성화하려면 주소군 컨피그레이션 모드에서 **neighbor transport** 명령을 사용합니다. BGP 세션에 대해 TCP 전송 세션 옵션을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** [**disable**]}

no neighbor {*ip_address*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** [**disable**]}

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
connection-mode	연결의 유형(active 또는 passive)을 지정합니다.
active	active 연결을 지정합니다.
passive	passive 연결을 지정합니다.
path-mtu-discovery	TCP 전송 경로 MTU(Maximum Transmission Unit) 검색을 활성화합니다. TCP 경로 MTU 검색은 기본적으로 활성화되어 있습니다.
disable	TCP 경로 MTU 검색을 비활성화합니다.

명령 기본값

이 명령을 구성하지 않으면, TCP 경로 MTU 검색은 기본적으로 활성화되지만 다른 TCP 전송 세션 옵션은 활성화되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 다양한 전송 옵션을 지정하는 데 사용됩니다. BGP 세션에 대해 active 또는 passive 전송 연결을 지정할 수 있습니다. BGP 세션이 더 큰 MTU 링크를 활용하도록 하려면 TCP 전송 경로 MTU 검색을 활성화할 수 있습니다. TCP 경로 MTU 검색의 활성화 여부를 확인하려면 **show bgp neighbors** 명령을 사용합니다. 검색을 비활성화하기 위해 **disable** 키워드를 사용하면 검색을 비활성화한 템플릿을 상속하는 피어에서도 검색이 비활성화됩니다.

예

다음 예는 단일 iBGP(internal BGP) 인접 디바이스에 대해 TCP 전송 연결을 active 상태로 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# neighbor 172.16.1.2 transport connection-mode active
```

다음 예는 단일 eBGP(external BGP) 인접 디바이스에 대해 TCP 전송 연결을 passive 상태로 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 192.168.1.2 activate
ciscoasa(config-router-af)# neighbor 192.168.1.2 transport connection-mode passive
```

다음 예는 단일 BGP 인접 디바이스에 대해 TCP 경로 MTU 검색을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# no neighbor 172.16.1.2 transport path-mtu-discovery
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
neighbor remote-as	BGP 또는 MBGP(Multiprotocol BGP) 라우팅 테이블에 엔트리를 추가합니다.
show bgp neighbor	BGP 인접 디바이스에 대한 정보를 표시합니다.

neighbor ttl-security

BGP(Border Gateway Protocol) 피어링 세션을 보호하고 두 개의 eBGP(external BGP) 피어를 분리하는 홉(hop)의 최대 수를 구성하려면 주소군 컨피그레이션 모드에서 **neighbor ttl-security** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **ttl-security hops** *hop-count*

no neighbor {*ip_address*} **ttl-security hops** *hop-count*

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
hop-count	eBGP 피어를 구분하는 홉(hop)의 수. TTL 값은 구성된 *hop-count* 인수로부터 라우터에 의해 계산됩니다. 유효한 값은 1~254 사이의 숫자입니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

neighbor ttl-security 명령은 CPU 사용률 기반 공격으로부터 BGP 피어링 세션을 보호하기 위해 경량 보안 메커니즘을 제공합니다. 이러한 유형의 공격은 일반적으로 패킷 헤더에 위조된 소스 및 수신 IP 주소가 포함된 IP 패킷을 네트워크에 집중적으로 보내 네트워크를 무력화하려는 DoS(Denial of Service) 무차별 대입(brute force) 공격입니다.

이 기능은 TTL 수가 로컬에서 구성한 값보다 크거나 같은 IP 패킷만 허용하는 IP 패킷의 기본 동작을 활용합니다. IP 패킷에서 TTL 수를 정확하게 위조하는 것은 일반적으로 불가능한 것으로 간주됩니다. 소스 또는 대상 네트워크에 내부적으로 액세스하지 않고는, 신뢰 피어의 TTL 수와 일치하도록 패킷을 정확히 위조하는 것이 불가능합니다.

이 기능은 각각의 참여 라우터에서 구성해야 합니다. 들어오는 방향의 BGP 세션만 보호하며 나가는 IP 패킷 또는 원격 라우터에는 영향을 미치지 않습니다. 이 기능이 활성화되면 BGP는 IP 패킷 헤더의 TTL 값이 피어링 세션에 대해 구성된 TTL 값보다 크거나 같은 경우에만 세션을 설정 또는 유지합니다. 이 기능은 BGP 피어링 세션에 영향을 미치지 않으며, keepalive 패킷을 수신하지 않는 경우에도 피어링 세션이 만료될 수 있습니다. 수신한 패킷의 TTL 값이 로컬에서 구성한 값보다 작으면 패킷이 자동으로 무시되고 ICMP(Internet Control Message Protocol) 메시지가 생성되지 않습니다. 이것은 기본 동작이며, 위조된 패킷에 대한 반응은 필요하지 않습니다.

이 기능의 효과를 최대화하려면 로컬 네트워크와 외부 네트워크 간 홉(hop) 수가 일치하도록 *hop-count* 값을 엄격하게 구성해야 합니다. 그러나 멀티 홉(multihop) 피어링 세션에 대해 이 기능을 구성할 경우 경로 변경 가능성을 고려해야 합니다.

이 명령의 컨피그레이션에는 다음과 같은 제한이 적용됩니다.

- iBGP(internal BGP) 피어에서는 이 기능이 지원되지 않습니다.
- **neighbor ebgp-multihop** 명령으로 이미 구성된 피어에 대해서는 **neighbor ttl-security** 명령을 구성할 수 없습니다. 이 두 명령의 컨피그레이션은 상호 배타적이므로 멀티 홉 eBGP 피어링 세션을 활성화하는 데에는 두 명령 중 하나만 필요합니다. 두 명령을 동일한 피어링 세션에 대해 구성하려고 시도하면 오류 메시지가 콘솔에 표시됩니다.
- 광범위한 멀티 홉 피어링에서는 이 기능의 효과가 줄어듭니다. 광범위한 피어링에 대해 구성된 BGP 라우터에서 CPU 사용률 기반 공격이 발생하는 경우 공격을 처리하려면 영향을 받는 피어링 세션을 닫아야 할 수 있습니다.
- 네트워크 내부에서 손상된 피어로부터의 공격에는 이 기능이 아무런 효과가 없습니다. 소스 및 대상 네트워크 간 네트워크 세그먼트에 있는 피어에도 이 제한이 적용됩니다.

예

다음 예는 직접 연결된 인접 디바이스에 대해 홉(hop) 수를 2로 설정합니다. *hop-count* 인수가 2로 설정되므로, BGP는 헤더에 253보다 크거나 같은 TTL 수가 있는 IP 패킷만 허용합니다. IP 패킷 헤더에 다른 TTL 값이 있는 패킷이 수신되면 해당 패킷은 자동으로 무시됩니다.

```
ciscoasa(config-router-af)# neighbor 10.0.0.1 ttl-security hops 2
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.
neighbor ebgp-multihop	직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시도합니다.

neighbor version

특별한 BGP 버전만 허용하도록 ASA 소프트웨어를 구성하려면 주소군 컨피그레이션 모드에서 **neighbor version** 명령을 사용합니다. 인접 디바이스의 기본 버전 수준을 사용하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **version** *number*

no neighbor{*ip_address*} **version** *number*

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
number	BGP 버전 번호. 버전을 2로 설정하여 소프트웨어가 지정된 인접 디바이스에서 버전 2만 사용하도록 강제할 수 있습니다. 기본값은 버전 4를 사용하고 요청 시 동적으로 버전 2까지 사용할 수 있도록 하는 것입니다.

명령 기본값

BGP 버전 4

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 입력하면 동적 버전 협상이 비활성화됩니다.

예

다음 예는 BGP 프로토콜의 버전 4로 고정합니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.27.2 version 4
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

neighbor weight

인접 디바이스 연결에 가중치를 할당하려면 주소군 컨피그레이션 모드에서 **neighbor weight** 명령을 사용합니다. 가중치 할당을 제거하려면 이 명령의 **no** 형식을 사용합니다.

neighbor {*ip_address*} **weight** *number*

no neighbor {*ip_address*} **weight** *number*

구문 설명

ip_address	인접 라우터의 IP 주소입니다.
number	할당할 가중치. 유효한 값은 0~65535입니다.

명령 기본값

또 다른 BGP 피어를 통해 학습된 경로의 기본 가중치는 0이고, 로컬 라우터에서 소싱된 경로의 기본 가중치는 32768입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 인접 디바이스에서 학습된 모든 경로에는 처음부터 가중치가 할당됩니다. 특정 네트워크에 대해 여러 경로를 사용할 수 있을 때 최고 가중치의 경로가 기본 경로로 선택됩니다.

set weight route-map 명령으로 할당된 가중치는 **neighbor weight** 명령으로 할당된 가중치를 재지정합니다.

예

다음 주소군 컨피그레이션 모드 예는 172.16.12.1을 통해 학습된 모든 경로의 가중치를 50으로 설정합니다.

```
ciscoasa(config-router-af)# neighbor 172.16.12.1 weight 50
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드로 들어갑니다.
neighbor activate	BGP 인접 디바이스와의 정보 교환을 활성화합니다.

nem

하드웨어 클라이언트에 대해 NEM(Network Extension Mode)을 활성화하려면 그룹 정책 컨피그레이션 모드에서 **nem enable** 명령을 사용합니다. NEM을 비활성화하려면 **nem disable** 명령을 사용합니다. 실행 중인 컨피그레이션에서 NEM 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션은 다른 그룹 정책으로부터 값을 상속하도록 허용합니다.

nem {**enable** | **disable**}

no nem

구문 설명

disable	NEM(Network Extension Mode)을 비활성화합니다.
enable	NEM(Network Extension Mode)을 활성화합니다.

기본값

NEM(Network Extension Mode)이 비활성화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

사용 지침

NEM(Network Extension Mode)에서는 하드웨어 클라이언트가 VPN 터널을 통해 원격 사설 네트워크에 라우팅 가능한 단일 네트워크를 표시할 수 있습니다. IPsec은 하드웨어 클라이언트 뒤에 있는 사설 네트워크의 모든 트래픽을 ASA 뒤에 있는 네트워크로 캡슐화합니다. PAT는 적용되지 않습니다. 따라서 ASA 뒤에 있는 디바이스는 하드웨어 클라이언트 뒤에 있는 사설 네트워크의 디바이스에 터널을 통해서만(또는 그 반대로) 직접 액세스합니다. 하드웨어 클라이언트는 터널을 시작해야 하지만, 터널이 설정된 후에는 양쪽 어디서나 데이터 교환을 시작할 수 있습니다.

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 그룹 정책 FirstGroup에 대해 NEM을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# nem enable
```

network

RIP 라우팅 프로세스를 위한 네트워크 목록을 지정하려면 라우터 컨피그레이션 모드에서 **network** 명령을 사용합니다. 네트워크 정의를 제거하려면 이 명령의 **no** 형식을 사용합니다.

network {*ip_addr*}

no network {*ip_addr*}

구문 설명

ip_addr	직접 연결된 네트워크의 IP 주소입니다. 지정된 네트워크에 연결된 인터페이스는 RIP 라우팅 프로세스에 참여합니다.

기본값

네트워크가 지정되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션,	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

지정된 네트워크 번호에는 서브넷 정보를 포함해서는 안 됩니다. 라우터에서 사용할 수 있는 network 명령의 수에는 제한이 없습니다. RIP 라우팅 업데이트는 지정된 네트워크의 인터페이스를 통해서만 송수신됩니다. 또한, 인터페이스의 네트워크를 지정하지 않으면 RIP 업데이트가 인터페이스로 광고되지 않습니다.

예

다음 예는 RIP를 10.0.0.0~192.168.7.0 네트워크에 연결된 모든 인터페이스에서 사용할 라우팅 프로토콜로 정의합니다.

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 192.168.7.0
```

관련 명령

명령	설명
router rip	라우터 컨피그레이션 모드로 들어갑니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

network(EIGRP)

EIGRP 라우팅 프로세스를 위한 네트워크 목록을 지정하려면 라우터 컨피그레이션 모드에서 **network** 명령을 사용합니다. 네트워크 정의를 제거하려면 이 명령의 **no** 형식을 사용합니다.

network *ip_addr* [*mask*]

no network *ip_addr* [*mask*]

구문 설명

ip_addr	직접 연결된 네트워크의 IP 주소입니다. 지정된 네트워크에 연결된 인터페이스는 EIGRP 라우팅 프로세스에 참여합니다.
mask	(선택 사항) IP 주소의 네트워크 마스크입니다.

기본값

네트워크가 지정되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

network 명령은 지정된 네트워크에 IP 주소가 하나 이상 있는 모든 인터페이스에서 EIGRP를 시작합니다. EIGRP 토폴로지 테이블에서 지정된 네트워크로부터 연결된 서브넷을 삽입합니다.

그러면 ASA에서는 일치하는 인터페이스를 통해 인접 디바이스를 설정합니다. ASA에서 구성할 수 있는 **network** 명령의 수에는 제한이 없습니다.

예

다음 예는 EIGRP를 10.0.0.0~192.168.7.0 네트워크에 연결된 모든 인터페이스에서 사용할 라우팅 프로토콜로 정의합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# network 192.168.7.0 255.255.255.0
```

관련 명령

명령	설명
show eigrp interfaces	EIGRP에 대해 구성된 인터페이스에 관한 정보를 표시합니다.
show eigrp topology	EIGRP 토폴로지 테이블을 표시합니다.

network BGP

BGP(Border Gateway Protocol) 라우팅 프로세스로 광고할 네트워크를 지정하려면 주소군 컨피그레이션 모드에서 **network** 명령을 사용합니다. 라우팅 테이블에서 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

network {*network-number* [**mask** *network-mask*]} [**route-map** *map-tag*]

no network {*network-number* [**mask** *network-mask*]} [**route-map** *map-tag*]

구문 설명

network-number	BGP 또는 MBGP(Multiprotocol BGP)에서 광고할 네트워크.
mask *network-mask*	(선택 사항) 마스크 주소가 있는 네트워크 또는 하위 네트워크 마스크.
route-map *map-tag*	(선택 사항) 구성된 경로 맵의 식별자. 알릴 네트워크를 필터링하려면 경로 맵을 검사해야 합니다. 지정하지 않으면 모든 네트워크를 광고합니다. 키워드를 지정했지만 경로 맵 태그가 나열되지 않으면 네트워크가 광고되지 않습니다.

기본값

네트워크가 지정되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

연결된 경로, 동적 라우팅 및 고정 경로 소스로부터 BGP 및 MBGP(Multiprotocol BGP) 네트워크를 학습할 수 있습니다.

사용 가능한 **network** 명령의 최대 수는 구성된 NVRAM 또는 RAM과 같은 라우터의 리소스에 의해 결정됩니다.

예

다음 예는 BGP 업데이트에 10.108.0.0 네트워크를 포함하도록 설정합니다.

```
ciscoasa(config)# router bgp 65100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
```

관련 명령

명령	설명
show bgp interfaces	BGP 라우팅 테이블의 엔트리를 표시합니다.

network-acl

전에 **access-list** 명령을 사용하여 구성한 방화벽 ACL 이름을 지정하려면 dynamic-access-policy-record 컨피그레이션 모드에서 **network-acl** 명령을 사용합니다. 기존의 네트워크 ACL을 제거하려면 이 명령의 **no** 형식을 사용합니다. 모든 네트워크 ACL을 제거하려면 명령을 인수 없이 사용합니다.

network-acl *name*

no network-acl [*name***]**

구문 설명

name	네트워크 ACL의 이름을 지정합니다. 이름의 최대 길이는 240자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Dynamic-access-policy-record 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

DAP 레코드에 방화벽 ACL을 여러 번 할당하려면 이 명령을 여러 번 사용합니다.

ASA에서는 사용자가 지정하는 각 ACL을 확인하여, 액세스 목록 엔트리에 대해 허용 규칙만 또는 거부 규칙만을 포함하고 있는지 검토합니다. 지정된 ACL 중 허용 규칙과 거부 규칙이 혼합되어 있는 ACL에 대해서는 ASA에서 명령을 거부합니다.

다음 예는 Finance Restrictions라는 네트워크 ACL을 Finance라는 DAP 레코드에 적용하는 방법을 보여줍니다.

```
ciscoasa(config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# network-acl Finance Restrictions
ciscoasa(config-dynamic-access-policy-record)#
```

관련 명령

명령	설명
access-policy	방화벽 액세스 정책을 구성합니다.
dynamic-access-policy-record	DAP 레코드를 만듭니다.
show running-config dynamic-access-policy-record [*name*]	모든 DAP 레코드 또는 명명된 DAP 레코드에 대해 실행 중인 컨피그레이션을 표시합니다.

network area

OSPF가 실행되는 인터페이스를 정의하고 해당 인터페이스의 영역 ID를 정의하려면 라우터 컨피그레이션 모드에서 **network area** 명령을 사용합니다. 주소/넷마스크 쌍으로 정의한 인터페이스에 대해 OSPF 라우팅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

network *addr mask* **area** *area_id*

no network *addr mask* **area** *area_id*

구문 설명

addr	IP 주소.
area *area_id*	OSPF 주소 범위와 연결할 영역을 지정합니다. *area_id*는 IP 주소 형식 또는 십진수 형식으로 지정할 수 있습니다. 십진수 형식으로 지정하는 경우 유효한 값의 범위는 0~4294967295입니다.
mask	네트워크 마스크입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 OSPF가 작동하려면 인터페이스의 주소를 **network area** 명령으로 처리해야 합니다. **network area** 명령으로 인터페이스의 IP 주소를 처리하지 못하면 해당 인터페이스에서 OSPF를 활성화할 수 없습니다.

ASA에서 사용할 수 있는 **network area** 명령의 수에는 제한이 없습니다.

예

다음 예는 192.168.1.1 인터페이스에서 OSPF를 활성화하고 2를 할당합니다.

```
ciscoasa(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드로 들어갑니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

network-object

네트워크 객체 그룹에 호스트 객체, 네트워크 객체 또는 서브넷 객체를 추가하려면 object-group network 컨피그레이션 모드에서 **network-object** 명령을 사용합니다. 네트워크 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

network-object {host *address* **|** *IPv4_address mask* **|** *IPv6_address/IPv6_prefix* **| object** *name*}

no network-object {host *ip_address* **|** *ip_address mask* **| object** *name*}

구문 설명

host *ip_address*	호스트 IPv4 또는 IPv6 주소를 지정합니다.
IPv4_address mask	IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다.
IPv6_address/IPv6_prefix	IPv6 네트워크 주소 및 접두사 길이를 지정합니다.
object *name*	네트워크 객체(**object network** 명령으로 생성)를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Object-group network 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.3(1)	지원되는 네트워크 객체에 **object** 인수가 추가되었습니다(**object network** 명령).
9.0(1)	이전에는 네트워크 객체 그룹이 IPv4 주소만 또는 IPv6 주소만 포함할 수 있었습니다. 이제 네트워크 객체 그룹에서 IPv4 주소와 IPv6 주소를 혼합하여 사용할 수 있습니다(NAT에서는 혼합된 그룹을 사용할 수 없음).

사용 지침

호스트 객체, 네트워크 객체 또는 서브넷 객체를 정의하려면 **network-object** 명령을 **object-group** 명령과 함께 사용합니다.

예

다음 예는 **network-object** 명령을 사용하여 네트워크 객체 그룹에서 새 호스트 객체를 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group network sjj_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjj.eng.ftp
ciscoasa(config-network-object-group)# network-object host 172.16.56.195
ciscoasa(config-network-object-group)# network-object 192.168.1.0 255.255.255.224
ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure object-group	컨피그레이션에서 모든 **object-group** 명령을 제거합니다.
group-object	네트워크 객체 그룹을 추가합니다.
object network	네트워크 객체를 추가합니다.
object-group network	네트워크 객체 그룹을 정의합니다.
show running-config object-group	현재 객체 그룹을 표시합니다.

nop

IP Options 검사의 패킷에 No Operation IP 옵션이 있는 경우 수행할 작업을 정의하려면 매개변수 컨피그레이션 모드에서 **nop** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

nop action {allow | clear}

no nop action {allow | clear}

구문 설명

allow	No Operation IP 옵션이 포함된 패킷의 통과를 허용하도록 ASA에 지시합니다.
clear	패킷에서 No Operation IP 옵션을 지우고 패킷의 통과를 허용하도록 ASA에 지시합니다.

기본값

기본적으로 IP Options 검사는 No Operation IP 옵션이 포함된 패킷을 삭제합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IP Options 검사 정책 맵에서 구성할 수 있습니다.

ASA를 통과하도록 허용할 특정 IP 옵션의 IP 패킷을 제어하려면 IP Options 검사를 구성할 수 있습니다. 이 검사를 구성하면 ASA는 패킷이 통과하도록 허용하거나, 지정된 IP 옵션을 지운 다음 패킷이 통과하도록 허용합니다.

IP 헤더의 Options 필드는 0개, 1개 또는 그 이상의 옵션을 포함할 수 있으며, 이에 따라 필드의 총 길이가 달라집니다. 그러나 IP 헤더는 32비트의 배수여야 합니다. 모든 옵션의 비트 수가 32비트의 배수가 아니면 32비트 경계에 옵션을 맞추기 위해 No Operation(NOP) 또는 IP Option 1이 "internal padding"으로 사용됩니다.

예

다음 예는 정책 맵에서 IP Options 검사에 대한 작업을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

nsf cisco

OSPF(Open Shortest Path First)를 실행하는 ASA에서 Cisco NSF(Nonstop Forwarding) 작업을 활성화하려면 라우터 컨피그레이션 모드에서 **nsf cisco** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 no 형식을 사용합니다.

nsf cisco [enforce global]

no nsf cisco [enforce global]

구문 설명

enforce global	(선택 사항) 다시 시작 프로세스 중 어느 한 인터페이스에서 NSF를 인식하지 못하는 인접한 네트워킹 디바이스가 검색되면 모든 인터페이스에서 NSF 다시 시작을 취소합니다.

기본값

Cisco NSF Graceful Restart는 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션 모드	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 OSPF 라우터에서 Cisco NSF를 활성화합니다. 라우터에서 NSF가 활성화되면, 해당 라우터는 NSF를 지원하게 되며 다시 시작 모드에서 작동하게 됩니다.

라우터가 NSF Graceful Restart를 수행하는 인접 라우터와만 함께 작동하도록 구성된 경우, 인접 라우터에는 NSF를 지원하는 Cisco 소프트웨어 릴리스가 실행되고 있어야 합니다. 그러나 해당 라우터에 NSF가 구성되어 있어야 할 필요는 없습니다. 라우터에 NSF를 지원하는 Cisco 소프트웨어 릴리스가 실행되고 있는 경우 해당 라우터는 NSF 인식 라우터입니다.

기본적으로 인접한 NSF 인식 라우터는 Graceful Restart 중에 NSF 헬퍼 모드에서 작동됩니다.

NSF Graceful Restart 중에 네트워크 인터페이스에서 NSF를 인식하지 못하는 인접 디바이스가 감지되면, 해당 인터페이스에서만 다시 시작이 취소되고 다른 인터페이스에서는 Graceful Restart가 계속 진행됩니다. 다시 시작 중에 NSF를 인식하지 못하는 인접 디바이스가 감지될 경우 전체 OSPF 프로세스의 다시 시작을 취소하려면 **enforce global** 키워드와 함께 이 명령을 구성합니다.

참고 어느 한 인터페이스에서 인접 디바이스 인접성 재설정이 감지된 경우 또는 OSPF 인터페이스가 다운된 경우에도 전체 프로세스에 대해 NSF Graceful Restart가 취소됩니다.

예

다음 예는 enforce global 옵션과 함께 Cisco NSF Graceful Restart를 활성화합니다.

```
ciscoasa(config)# router ospf 24
ciscoasa(config-router)# cisco nsf enforce global
```

관련 명령

명령	설명
nsf cisco helper	ASA에서 Cisco NSF 헬퍼 모드를 활성화합니다.
nsf ietf	IETF NSF를 활성화합니다.

nsf cisco helper

OSPF(Open Shortest Path First)를 실행하는 ASA에서 Cisco NSF(Nonstop Forwarding) 헬퍼 모드를 활성화하려면 라우터 컨피그레이션 모드에서 **nsf cisco helper** 명령을 사용합니다. Cisco NSF 헬퍼 모드는 기본적으로 활성화되어 있으며 라우터 컨피그레이션 모드에서 **no nsf cisco helper** 명령을 실행하여 비활성화할 수 있습니다.

nsf cisco helper

no nsf cisco helper

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

Cisco NSF 헬퍼 모드는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션 모드	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

NSF가 활성화된 ASA는 NSF 지원 상태이며 Graceful Restart 모드에서 운영됩니다. OSPF 라우터 프로세스는 RP(Route Processor) 전환 때문에 무중단 전달 복구를 수행합니다. 기본적으로 NSF 지원 ASA와 인접한 ASA는 NSF 인식 상태가 되며 NSF 헬퍼 모드에서 운영됩니다. NSF 지원 ASA가 Graceful Restart를 수행하면 헬퍼 ASA는 무중단 전달 복구 프로세스를 지원합니다. ASA가 다시 시작하는 인접 디바이스에 대해 무중단 전달 복구를 지원하지 않도록 하려면 **no nsf cisco helper** 명령을 입력합니다.

예

다음 예는 NSF 헬퍼 모드를 비활성화합니다.

```
ciscoasa(config)# router ospf 24
ciscoasa(config-router)# no nsf cisco helper
```

관련 명령

명령	설명
nsf cisco	ASA에서 Cisco NSF를 활성화합니다.
nsf ietf	IETF NSF를 활성화합니다.

nsf ietf

OSPF를 실행하는 ASA에서 IETF(Internet Engineering Task Force) NSF 작업을 구성하려면 라우터 컨피그레이션 모드에서 **nsf ietf** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 no 형식을 사용합니다.

nsf ietf [restart-interval *seconds***]**

no nsf ietf

구문 설명

restart-interval *seconds*	(선택 사항) Graceful Restart 간격을 초 단위로 지정합니다. 범위는 1~1800입니다. 기본값은 120입니다. **참고** 재시작 간격이 30초 미만일 경우 Graceful Restart가 종료됩니다.

기본값

IETF NSF Graceful Restart 모드는 비활성화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션 모드	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 ASA에서 IETF NSF를 활성화합니다. ASA에서 NSF가 활성화되면, ASA는 NSF를 지원하게 되며 다시 시작 모드에서 작동하게 됩니다.

ASA가 NSF Graceful Restart를 수행하는 인접 ASA와만 함께 작동하도록 구성된 경우, 인접 ASA는 NSF를 지원해야 합니다. 그러나 해당 ASA에 NSF가 구성되어 있어야 할 필요는 없습니다. NSF를 지원하는 애플리케이션이 실행되고 있는 ASA는 NSF 인식 ASA입니다.

예

다음 예는 NSF 헬퍼 모드를 비활성화합니다.

```
ciscoasa(config)# router ospf 24
ciscoasa(config-router)# nsf ietf restart-interval 240
```

관련 명령

명령	설명
nsf cisco	ASA에서 Cisco NSF를 활성화합니다.
nsf cisco helper	ASA에서 Cisco NSF 헬퍼 모드를 활성화합니다.
nsf ietf helper	ASA에서 IETF NSF 헬퍼 모드를 활성화합니다.

nsf ietf helper

IETF NSF 헬퍼 모드는 기본적으로 활성화되어 있습니다. IETF NSF 헬퍼 모드를 명시적으로 활성화하려면 라우터 컨피그레이션 모드에서 **nsf ietf helper** 명령을 사용합니다. 비활성화하려면 **command** 명령의 no 형식을 사용합니다.

선택적으로 **nsf ietf helper strict-lsa-checking** 명령을 사용하여 엄격한 LSA(Link-state Advertisement) 점검을 활성화할 수 있습니다.

nsf ietf helper [strict-lsa-checking]

no nsf ietf helper

구문 설명

strict-lsa-checking	(선택 사항) 헬퍼 모드에 대해 엄격한 LSA(Link-state Advertisement) 점검을 활성화합니다.

기본값

IETF NSF 헬퍼 모드는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션 모드	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

NSF가 활성화된 ASA는 NSF 지원 상태이며 Graceful Restart 모드에서 운영됩니다. OSPF 라우터 프로세스는 RP(Route Processor) 전환 때문에 무중단 전달 복구를 수행합니다. 기본적으로 NSF 지원 ASA와 인접한 ASA는 NSF 인식 상태가 되며 NSF 헬퍼 모드에서 운영됩니다. NSF 지원 ASA가 Graceful Restart를 수행하면 헬퍼 ASA는 무중단 전달 복구 프로세스를 지원합니다. ASA가 다시 시작하는 인접 디바이스에 대해 무중단 전달 복구를 지원하지 않도록 하려면 **no nsf ietf helper** 명령을 입력합니다.

NSF 인식 ASA와 NSF 지원 ASA에서 모두 엄격한 LSA 점검을 활성화하려면 **nsf ietf helper strict-lsa-checking** 명령을 입력합니다. 그러나 IETF Graceful Restart 프로세스 중에 ASA가 헬퍼 ASA로 전환할 때까지는 엄격한 LSA 점검이 적용되지 않습니다. 엄격한 LSA 점검이 활성화된 상태에서, 다시 시작 ASA로 플러딩되는 LSA에서 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 다시 시작 ASA의 재전송 목록에 변경된 LSA가 있는 경우 헬퍼 ASA는 다시 시작 ASA의 지원 프로세스를 중단합니다.

예

다음 예는 엄격한 LSA 점검과 함께 IETF NSF 헬퍼를 활성화합니다.

```
ciscoasa(config)# router ospf 24
ciscoasa(config-router)# nsf ietf helper strict-lsa-checking
```

관련 명령

명령	설명
nsf cisco	ASA에서 Cisco NSF를 활성화합니다.
nsf cisco helper	ASA에서 Cisco NSF 헬퍼 모드를 활성화합니다.
nsf ietf	ASA에서 IETF NSF를 활성화합니다.

nt-auth-domain-controller

이 서버에 대한 NT Primary Domain Controller의 이름을 지정하려면 aaa-server host 컨피그레이션 모드에서 **nt-auth-domain-controller** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

nt-auth-domain-controller *string*

no nt-auth-domain-controller

구문 설명

string	이 서버에 대한 Primary Domain Controller의 이름을 최대 16자로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server host 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 NT Authentication AAA 서버에 대해서만 유효합니다. 호스트 컨피그레이션 모드로 들어가려면 먼저 **aaa-server host** 명령을 사용해야 합니다. *string* 변수의 이름은 서버 자체의 NT 엔트리와 일치해야 합니다.

예

다음 예는 이 서버에 대한 NT Primary Domain Controller의 이름을 "primary1"로 지정합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol nt
ciscoasa(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
aaa server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa server host 컨피그레이션 모드로 들어갑니다.
clear configure aaa-server	컨피그레이션에서 모든 AAA 명령문을 제거합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

ntp authenticate

NTP 서버에 대해 인증하려면 글로벌 컨피그레이션 모드에서 **ntp authenticate** 명령을 사용합니다. NTP 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ntp authenticate

no ntp authenticate

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

인증을 활성화하면 ASA는 패킷에서 올바른 신뢰 키를 사용하는 NTP 서버와만 통신합니다(**ntp trusted-key** 명령 참조). ASA는 또한 NTP 서버와의 동기화를 위해 인증 키를 사용합니다(**ntp authentication-key** 명령 참조).

예

다음 예는 NTP 패킷에서 인증 키 42를 제공하는 시스템에만 동기화하도록 ASA를 구성합니다.

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp authentication-key 42 md5 aNiceKey
ciscoasa(config)# ntp trusted-key 42
```

관련 명령

명령	설명
ntp authentication-key	NTP 서버와 동기화하도록 암호화된 인증 키를 설정합니다.
ntp server	NTP 서버를 지정합니다.
ntp trusted-key	ASA가 NTP 서버와의 인증을 위해 패킷에서 사용할 키 ID를 제공합니다.
show ntp associations	ASA와 연결되어 있는 NTP 서버를 보여줍니다.
show ntp status	NTP 연결 상태를 보여줍니다.

ntp authentication-key

NTP 서버에 대해 인증하기 위한 키를 설정하려면 글로벌 컨피그레이션 모드에서 **ntp authentication-key** 명령을 사용합니다. 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ntp authentication-key *key_id* **md5** *key*

no ntp authentication-key *key_id* [**md5** [0 | 8] *key*]

구문 설명

0	(선택 사항) <key_value>가 일반 텍스트임을 나타냅니다. 0 또는 8이 없으면 일반 형식입니다.
8	(선택 사항) <key_value>가 암호화된 텍스트임을 나타냅니다. 0 또는 8이 없으면 일반 형식입니다.
key	키 값을 최대 32자의 문자열로 설정합니다.
key_id	키 ID를 1~4294967295 범위로 지정합니다. 이 ID는 **ntp trusted-key** 명령을 사용하여 신뢰 키로 지정해야 합니다.
md5	인증 알고리즘을 지원되는 유일한 알고리즘인 MD5로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

NTP 인증을 사용하려면 **ntp authenticate** 명령도 구성해야 합니다.

예

다음 예는 인증을 활성화하고, 신뢰 키 ID 1과 2를 식별하고, 각 신뢰 키 ID에 대해 인증 키를 설정합니다.

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

관련 명령

명령	설명
ntp authenticate	NTP 인증을 활성화합니다.
ntp server	NTP 서버를 지정합니다.
ntp trusted-key	ASA가 NTP 서버와의 인증을 위해 패킷에서 사용할 키 ID를 제공합니다.
show ntp associations	ASA와 연결되어 있는 NTP 서버를 보여줍니다.
show ntp status	NTP 연결 상태를 보여줍니다.

ntp server

NTP 서버를 식별하여 ASA에서 시간을 설정하려면 글로벌 컨피그레이션 모드에서 **ntp server** 명령을 사용합니다. 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

no ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

구문 설명

ip_address	NTP 서버의 IP 주소 또는 호스트 이름을 설정합니다.
key *key_id*	**ntp authenticate** 명령을 사용하여 인증을 활성화한 경우 이 서버에 대한 신뢰 키 ID를 설정합니다. **ntp trusted-key** 명령도 참조하십시오.
source *interface_name*	라우팅 테이블의 기본 인터페이스를 사용하지 않을 경우 NTP 패킷의 나가는 인터페이스를 지정합니다. 다중 컨텍스트 모드에서는 어떤 인터페이스도 포함하지 않으므로 관리 상황에 정의된 인터페이스 이름을 지정합니다.
prefer	여러 서버의 정확도가 비슷할 경우 이 NTP 서버를 기본 서버로 설정합니다. NTP는 알고리즘을 사용하여 어떤 서버가 가장 정확한지 알아내고 그 서버와 동기화합니다. 서버의 정확도가 비슷할 경우 **prefer** 키워드로 그 중에서 사용할 서버를 지정합니다. 그러나 어떤 서버가 기본 서버보다 훨씬 더 정확할 경우 ASA는 더 정확한 쪽을 사용합니다. 예를 들어, ASA는 기본 서버인 stratum 3 서버 대신 stratum 2 서버를 사용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	소스 인터페이스가 선택 사항이 되도록 이 명령이 수정되었습니다.

사용 지침

여러 서버를 지정할 수 있습니다. ASA는 가장 정확한 서버를 사용합니다. 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서만 NTP 서버를 설정할 수 있습니다.

예

다음 예는 두 개의 NTP 서버를 식별하고 키 ID 1과 2에 대해 인증을 활성화합니다.

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

관련 명령

명령	설명
ntp authenticate	NTP 인증을 활성화합니다.
ntp authentication-key	NTP 서버와 동기화하도록 암호화된 인증 키를 설정합니다.
ntp trusted-key	ASA가 NTP 서버와의 인증을 위해 패킷에서 사용할 키 ID를 제공합니다.
show ntp associations	ASA와 연결되어 있는 NTP 서버를 보여줍니다.
show ntp status	NTP 연결 상태를 보여줍니다.

ntp trusted-key

신뢰 키가 될 인증 키 ID를 지정하려면(NTP 서버와의 인증에 필요) 글로벌 컨피그레이션 모드에서 **ntp trusted-key** 명령을 사용합니다. 신뢰 키를 제거하려면 이 명령의 **no** 형식을 사용합니다. 여러 서버에서 사용할 수 있도록 여러 신뢰 키를 입력할 수 있습니다.

ntp trusted-key *key_id*

no ntp trusted-key *key_id*

구문 설명

key_id	키 ID를 1~4294967295 범위로 설정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

NTP 인증을 사용하려면 **ntp authenticate** 명령도 구성해야 합니다. 서버와 동기화하려면 **ntp authentication-key** 명령을 사용하여 키 ID에 대해 인증 키를 설정합니다.

예

다음 예는 인증을 활성화하고, 신뢰 키 ID 1과 2를 식별하고, 각 신뢰 키 ID에 대해 인증 키를 설정합니다.

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
```

관련 명령

명령	설명
ntp authenticate	NTP 인증을 활성화합니다.
ntp authentication-key	NTP 서버와 동기화하도록 암호화된 인증 키를 설정합니다.
ntp server	NTP 서버를 지정합니다.
show ntp associations	ASA와 연결되어 있는 NTP 서버를 보여줍니다.
show ntp status	NTP 연결 상태를 보여줍니다.

num-packets

SLA 작업 중에 전송할 요청 패킷의 수를 지정하려면 sla monitor protocol 컨피그레이션 모드에서 **num-packets** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

num-packets *number*

no num-packets *number*

구문 설명

number	SLA 작업 중에 전송할 패킷의 수. 유효한 값은 1~100입니다. **참고** 이 명령에서 number 인수로 지정된 모든 패킷이 손실되면 추적 경로가 실패합니다.

기본값

에코 유형에 대해 전송되는 기본값은 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Sla 모니터 프로토콜 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

패킷 손실로 인해 잘못된 도달 정보가 생성되는 것을 막으려면 전송할 기본 패킷 수를 늘리면 됩니다.

예

다음 예는 ICMP 에코 요청/응답 시간 프로브 작업을 사용하는 ID 123으로 SLA 작업을 구성합니다. 에코 요청 패킷의 페이로드 크기를 48바이트로 설정하고 SLA 작업 중 전송되는 에코 요청의 수를 5로 설정합니다. 5개 패킷이 모두 손실되면 추적 경로가 제거됩니다.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

명령	설명
request-data-size	요청 패킷 페이로드의 크기를 지정합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.
type echo	SLA 작업을 에코 응답 시간 프로브 작업으로서 구성합니다.

14 장

object network through override-svc-download 명령

object network

명명된 네트워크 객체를 구성하려면 글로벌 컨피그레이션 모드에서 **object network** 명령을 사용합니다. 컨피그레이션에서 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

object network *name* [**rename** *new_obj_name*]

no object network *name*

구문 설명

name	네트워크 객체의 이름을 지정합니다. 이름은 1~64자 길이로 지정할 수 있으며 문자, 숫자 외에도 밑줄, 하이픈, 쉼표, 슬래시, 마침표 등의 특수 문자를 사용할 수 있습니다. 객체와 객체 그룹은 동일한 네임스페이스를 공유합니다.
rename *new_obj_name*	(선택 사항) 객체 이름을 새 이름으로 변경합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.
8.4(2)	FQDN(정규화된 도메인 이름)에 대한 지원이 추가되었습니다. **fqdn** 명령을 참조하십시오.

사용 지침

네트워크 객체에는 호스트, 네트워크, IP 주소 범위(IPv4 또는 IPv6) 또는 FQDN을 포함할 수 있습니다. 명령을 입력한 다음 **host**, **fqdn**, **subnet** 또는 **range** 명령을 사용하여 객체에 주소 하나를 추가합니다.

nat 명령을 사용하면 이 네트워크 객체에서 NAT 규칙을 활성화할 수 있습니다. 한 객체에는 단일 NAT 규칙만 정의할 수 있습니다. 여러 NAT 규칙을 구성하려면 동일한 IP 주소를 지정하는 여러 객체를 만들어야 합니다(예: **object network obj-10.10.10.1-01**, **object network obj-10.10.10.1-02** 등).

기존 네트워크 객체를 다른 IP 주소로 구성하면 새 컨피그레이션이 기존 컨피그레이션을 교체합니다.

예

다음 예는 네트워크 객체를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

관련 명령

명령	설명
clear configure object	생성된 모든 객체를 지웁니다.
description	네트워크 객체에 설명을 추가합니다.
fqdn	정규화된 도메인 이름 네트워크 객체를 지정합니다.
host	호스트 네트워크 객체를 지정합니다.
nat	네트워크 객체에 대해 NAT를 활성화합니다.
object-group network	네트워크 객체 그룹을 만듭니다.
range	네트워크 객체에 대해 주소 범위를 지정합니다.
show running-config object network	네트워크 객체 컨피그레이션을 보여줍니다.
subnet	서브넷 네트워크 객체를 지정합니다.

object service

객체가 사용되는 모든 컨피그레이션에 자동으로 반영되는 서비스 객체를 구성하려면 글로벌 컨피그레이션 모드에서 **object service** 명령을 사용합니다. 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

object service *name* [**rename** *new_obj_name*]

no object service *object name* [**rename** *new_obj_name*]

구문 설명

name	서비스 객체의 이름을 지정합니다. 이름은 1~64자 길이로 지정할 수 있으며 문자, 숫자 외에도 밑줄, 하이픈, 쉼표, 마침표 등의 특수 문자를 사용할 수 있습니다. 객체 이름은 문자로 시작해야 합니다.
rename *new_obj_name*	(선택 사항) 객체 이름을 새 이름으로 변경합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

서비스 객체는 프로토콜, ICMP, ICMPv6, TCP, UDP 포트 또는 포트 범위를 포함할 수 있습니다. 명령을 입력한 다음 **service** 명령을 사용하여 객체에 서비스 사양 하나를 추가합니다.

다른 프로토콜 및 포트로 기존 서비스 객체를 구성하면 새 컨피그레이션이 기존 프로토콜 및 포트를 새로운 것과 교체합니다.

예

다음 예는 서비스 객체를 생성하는 방법을 보여줍니다.

```
ciscoasa(config)# object service SERVOBJECT1
ciscoasa(config-service-object)# service tcp source eq www destination eq ssh
```

관련 명령

명령	설명
clear configure object	생성된 모든 객체를 지웁니다.
service	서비스 객체에 대한 프로토콜과 포트를 구성합니다.

object-group

컨피그레이션 최적화를 위해 사용할 수 있는 객체 그룹을 정의하려면 글로벌 컨피그레이션 모드에서 **object-group** 명령을 사용합니다. 컨피그레이션에서 객체 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

object-group {**protocol** | **network** | **icmp-type** | **security** | **user**} *grp_name*

object-group service *grp_name* [**tcp** | **udp** | **tcp-udp**]

구문 설명

grp_name	문자, 숫자 "_", "-", "." 문자를 사용하여 객체 그룹(1~64문자)을 지정합니다.
icmp-type	(권장하지 않음, 대신 **service** 사용) echo 및 echo-reply 같은 ICMP 유형의 그룹을 정의합니다. **object-group icmp-type** 명령을 입력한 다음 **icmp-object** 및 **group-object** 명령을 사용하여 ICMP 객체를 추가합니다.
network	호스트 또는 서브넷 IP 주소의 그룹을 정의합니다. **object-group network** 명령을 입력한 다음 **network-object** 및 **group-object** 명령을 사용하여 네트워크 객체를 추가합니다. IPv4 및 IPv6 주소를 함께 사용하여 그룹을 생성할 수 있습니다. **참고** NAT에는 혼합 객체 그룹을 사용할 수 없습니다.
protocol	(권장하지 않음, 대신 **service** 사용) TCP 및 UDP 같은 프로토콜의 그룹을 정의합니다. **object-group protocol** 명령을 입력한 다음 **protocol-object** 및 **group-object** 명령을 사용하여 프로토콜 객체를 추가합니다.
security	Cisco TrustSec과 함께 사용할 보안 그룹 객체를 정의합니다. **object-group protocol** 명령을 입력한 다음 **security-object** 및 **group-object** 명령을 사용하여 보안 그룹 객체를 추가합니다.
service [**tcp** | **udp** | **tcp-udp**]	프로토콜, ICMP 유형 및 TCP/UDP 포트를 기반으로 서비스를 정의합니다. 혼합된 서비스 그룹을 정의하려면 object-group에 대해 프로토콜 유형을 지정하지 마십시오. **object-group service** 명령을 입력한 다음 **service-object** 및 **group-object** 명령을 사용하여 서비스 객체를 서비스 그룹에 추가합니다. TCP 또는 UDP(또는 둘 다) 포트의 목록만 포함하려는 객체인 경우에도 이 방법을 사용하는 것이 좋습니다. object-group service 명령에서 직접 **tcp**, **udp** 및 **tcp-udp** 키워드를 사용하는 것은 권장하지 않습니다. 대신 이러한 키워드를 명령과 분리하고, **service-object** 명령에서 TCP 및 UDP 포트를 구성합니다. 이러한 키워드 중 하나를 포함하는 경우 **port-object** 및 **group-object** 명령을 사용하여 포트 그룹을 추가합니다.
user	ID 방화벽으로 액세스를 제어할 수 있는 사용자 및 사용자 그룹을 정의합니다. **object-group protocol** 명령을 입력한 다음 **user, user-group** 및 **group-object** 명령을 사용하여 사용자 및 사용자 그룹 객체를 추가합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

명령 모드	방화벽 모드		보안 컨텍스트		
	라우팅	투명성	단일	다중	
				컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.4(2)	ID 방화벽을 지원하도록 **user** 키워드에 대한 지원을 추가했습니다.
9.0(1)	이제는 네IPv4 주소와 IPv6 주소의 혼합을 지원하는 네트워크 객체 그룹을 만들 수 있습니다. Cisco TrustSec을 지원하도록 **security** 키워드에 대한 지원을 추가했습니다.

사용 지침

호스트나 서비스 같은 객체는 그룹화할 수 있습니다. 그런 다음 ACL(**access-list**) 및 NAT(**nat**) 같은 기능에서 객체 그룹을 사용할 수 있습니다. 다음은 ACL에서 네트워크 객체 그룹을 사용하는 예입니다.

```
ciscoasa(config)# access-list access_list_name extended permit tcp any object-group
NWgroup1
```

명령을 계층적으로 그룹화할 수 있습니다. 객체 그룹은 또 다른 객체 그룹의 멤버가 될 수 있습니다.

예

다음 예는 **object-group network** 명령을 사용하여 네트워크 객체 그룹을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group network sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.eng.ftp.servcers
ciscoasa(config-network-object-group)# network-object host 172.23.56.194
ciscoasa(config-network-object-group)# network-object 192.1.1.0 255.255.255.224
ciscoasa(config-network-object-group)# exit
```

다음 예는 **object-group network** 명령을 사용하여 기존 객체 그룹을 포함하는 네트워크 객체 그룹을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group network sjc_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.ftp.servers
ciscoasa(config-network-object-group)# network-object host 172.23.56.195
ciscoasa(config-network-object-group)# network-object 193.1.1.0 255.255.255.224
ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# exit
```

다음 예는 **group-object** 모드를 사용하여, 전에 정의한 객체로 구성된 새로운 객체 그룹을 만들고 이러한 객체를 ACL에서 사용하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network-object-group)# network-object host 192.168.1.1
ciscoasa(config-network-object-group)# network-object host 192.168.1.2
ciscoasa(config-network-object-group)# exit

ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network-object-group)# network-object host 172.23.56.1
ciscoasa(config-network-object-group)# network-object host 172.23.56.2
```

```
ciscoasa(config-network-object-group)# exit

ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network-object-group)# group-object host_grp_1
ciscoasa(config-network-object-group)# group-object host_grp_2
ciscoasa(config-network-object-group)# exit

ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)#access-list all permit tcp object-group all_hosts any eq www
```

group-object 명령을 사용하지 않는 경우, *host_grp_1* 및 *host_grp_2*에 이미 정의된 모든 IP 주소를 포함하기 위해 *all_hosts* 그룹을 정의해야 합니다. **group-object** 명령을 사용하는 경우, 호스트의 중복된 정의가 제거됩니다.

다음 예는 서비스 객체 그룹에 TCP 및 UDP 서비스를 모두 추가하는 방법을 보여줍니다.

```
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 예는 서비스 객체 그룹에 여러 서비스 객체를 추가하는 방법을 보여줍니다.

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

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

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

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

다음 예는 서비스 객체 그룹에 프로토콜, 포트 및 ICMP 사양을 혼합하여 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group service mixed
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 ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
```

다음 예는 TCP 및 UDP 서비스의 그룹화에 유용한 **service-object** 하위 명령을 사용하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host kqk.suu.dri.ixx
ciscoasa(config-network-object-group)# network-object host kqk.suu.pyl.gnl

ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
```

```
ciscoasa(config)# object-group service usr_svc
ciscoasa(config-service-object-group)# service-object tcp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object tcp destination eq pop3
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
ciscoasa(config-service-object-group)# service-object udp destination eq domain

ciscoasa(config)# access-list acl extended permit object-group usr_svc object-group locals
object-group remote
```

다음 예는 **object-group user** 명령을 사용하여 사용자 그룹 객체를 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

(권장하지 않음, 대신 service objects 사용) 다음 예는 **object-group icmp-type** 모드를 사용하여 ICMP 객체 그룹을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group icmp-type icmp-allowed
ciscoasa(config-icmp-object-group)# icmp-object echo
ciscoasa(config-icmp-object-group)# icmp-object time-exceeded
ciscoasa(config-icmp-object-group)# exit
```

(권장하지 않음, 대신 service objects 사용) 다음 예는 **object-group protocol** 모드를 사용하여 프로토콜 객체 그룹을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol-object-group)# protocol-object udp
ciscoasa(config-protocol-object-group)# protocol-object ipsec
ciscoasa(config-protocol-object-group)# exit

ciscoasa(config)# object-group protocol proto_grp_2
ciscoasa(config-protocol-object-group)# protocol-object tcp
ciscoasa(config-protocol-object-group)# group-object proto_grp_1
ciscoasa(config-protocol-object-group)# exit
```

(권장하지 않음, 대신 **tcp** 키워드를 없애고 포트를 **service-object** 명령으로 정의) 다음 예는 **object-group service** 모드를 사용하여 TCP 포트 객체 그룹을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service-object-group)# group-object eng_www_service
ciscoasa(config-service-object-group)# port-object eq ftp
ciscoasa(config-service-object-group)# port-object range 2000 2005
ciscoasa(config-service-object-group)# exit
```

다음 예는 객체 그룹을 사용하여 액세스 목록 컨피그레이션을 간소화하는 방법을 보여줍니다. 이렇게 그룹화하면 액세스 목록이 24줄 대신 1줄에서 구성되며, 이 방식은 그룹화가 사용되지 않는 경우 필요합니다.

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host 10.1.1.15
ciscoasa(config-network-object-group)# network-object host 10.1.1.16

ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
```

```
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240

ciscoasa(config)# object-group service eng_svc tcp
ciscoasa(config-service-object-group)# port-object eq www
ciscoasa(config-service-object-group)# port-object eq smtp
ciscoasa(config-service-object-group)# port-object range 25000 25100

ciscoasa(config)# access-list acl extended permit tcp object-group remote object-group
locals object-group eng_svc
```

참고 **show running-config access-list** 명령은 객체 그룹 이름으로 구성된 대로 액세스 목록을 표시합니다. **show access-list** 명령은 이 정보 외에도, 객체 그룹화 없이 개별 엔트리로 확장된 그룹을 사용하는 액세스 목록 엔트리를 표시합니다.

관련 명령

명령	설명
clear configure object-group	컨피그레이션에서 모든 **object group** 명령을 제거합니다.
group-object	네트워크 객체 그룹을 추가합니다.
network-object	네트워크 객체를 네트워크 객체 그룹에 추가합니다.
port-object	포트 객체를 서비스 객체 그룹에 추가합니다.
security-group	보안 그룹을 보안 그룹 객체 그룹에 추가합니다.
show running-config object-group	현재 객체 그룹을 표시합니다.
user	사용자 이름을 사용자 그룹 객체에 추가합니다.
user-group	사용자 그룹 이름을 사용자 그룹 객체에 추가합니다.

object-group-search

ACL 최적화를 활성화하려면 글로벌 컨피그레이션 모드에서 **object-group-search** 명령을 사용합니다. ACL 최적화를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

object-group-search access-control

no object-group-search access-control

구문 설명

access-control	액세스 제어 도메인을 검색합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

object-group-search 명령은 인바운드 방향의 모든 ACL을 최적화합니다.

객체 그룹 검색을 활성화하여 액세스 규칙을 검색하는 데 필요한 메모리를 줄일 수 있지만, 이 경우 조회 성능이 저하됩니다. 객체 그룹 검색을 활성화할 경우 ASP 테이블의 네트워크 객체를 사용하는 ACL로 검색이 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. 이 내용은 **show access-list** 출력에 표시됩니다.

ASA에서 **object-group-search access-control** 명령이 활성화되고 이와 더불어 상당히 많은 기능이 활성화되며 대규모 ACL과 함께 다수의 활성 연결이 로드되면, 운영 중에 연결이 감소되고 새 연결 설정 중에 성능이 감소될 수 있습니다.

예

다음 예는 **object-group-search** 명령을 사용하여 ACL 최적화를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group-search access-control
```

다음은 **object-group-search**가 활성화되지 않은 상태에서 **show access-list** 명령을 사용하는 경우의 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**가 활성화된 상태에서 **show access-list** 명령을 사용하는 경우의 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
```

관련 명령

명령	설명
clear config object-group search	object-group-search 컨피그레이션을 지웁니다.
show object-group	객체 그룹이 네트워크 객체 그룹 유형인 경우 히트 수를 보여줍니다.
show running-config object-group	현재 객체 그룹을 표시합니다.
show running-config object-group-search	실행 중인 컨피그레이션에서 object-group-search 컨피그레이션을 보여줍니다.

ocsp disable-nonce

nonce 확장을 비활성화하려면 crypto ca trustpoint 컨피그레이션 모드에서 **ocsp disable-nonce** 명령을 사용합니다. nonce 확장을 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

ocsp disable-nonce

no ocsp disable-nonce

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 OCSP 요청에는 nonce 확장이 포함됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 OCSP 요청에 OCSP nonce 확장이 포함되지 않으며, ASA에서 이를 확인하지 않습니다. 기본적으로 OCSP 요청에는 nonce 확장이 포함됩니다. 이 확장은 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지합니다. 그러나 일부 OCSP 서버에서는 이러한 매칭 nonce 확장이 포함되지 않은 미리 생성된 응답을 사용합니다. 이러한 서버에서 OCSP를 사용하려면 nonce 확장을 비활성화해야 합니다.

예

다음 예는 newtrust라는 신뢰 지점에 대해 nonce 확장을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# ocsp disable-nonce
ciscoasa(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다. 글로벌 컨피그레이션 모드에서 이 명령을 사용합니다.
match certificate	OCSP 재지정 규칙을 구성합니다.
ocsp url	신뢰 지점과 연결된 모든 인증서를 검사하는 데 사용할 OCSP 서버를 지정합니다.
revocation-check	폐기 검사에 사용할 방법 및 시도할 순서를 지정합니다.

ocsp url

신뢰 지점과 연결된 모든 인증서의 검사에 사용할 서버로서, 클라이언트 인증서의 AIA 확장에서 지정한 서버가 아니라 OCSP 서버를 ASA에 대해 구성하려면 crypto ca trustpoint 컨피그레이션 모드에서 **ocsp url** 명령을 사용합니다. 컨피그레이션에서 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ocsp url *URL*

no ocsp url

구문 설명

URL	OCSP 서버의 HTTP URL을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ASA는 HTTP URL만 지원하며, 신뢰 지점당 URL을 하나만 지정할 수 있습니다.

ASA는 OCSP 서버 URL을 정의하기 위한 세 가지 방법을 제공하며, 사용자가 정의한 방법에 따라 다음 순서로 OCSP 서버의 사용을 시도합니다.

- **match certificate** 명령을 사용하여 설정한 OCSP 서버
- **ocsp url** 명령을 사용하여 설정한 OCSP 서버
- 클라이언트 인증서 AIA 필드의 OCSP 서버

사용자가 **match certificate** 명령 또는 **ocsp url** 명령을 통해 OCSP URL을 구성하지 않는 경우, ASA는 클라이언트 인증서의 AIA 확장에서 OCSP 서버를 사용합니다. 인증서에 AIA 확장이 없으면 폐기 상태 검사가 실패합니다.

예

다음 예는 URL http://10.1.124.22로 OCSP 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# ocsp url http://10.1.124.22
ciscoasa(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca trustpoint 컨피그레이션 모드로 들어갑니다. 글로벌 컨피그레이션 모드에서 이 명령을 사용합니다.
match certificate	OCSP 재지정 규칙을 구성합니다.
ocsp disable-nonce	OCSP 요청의 nonce 확장을 비활성화합니다.
revocation-check	폐기 검사에 사용할 방법 및 시도할 순서를 지정합니다.

onscreen-keyboard

로그온 창 또는 로그인/비밀번호가 필요한 모든 창에 화면 키보드를 삽입하려면 webvpn 모드에서 **onscreen-keyboard** 명령을 사용합니다. 전에 구성한 화면 키보드를 제거하려면 이 명령의 **no** 형식을 사용합니다.

onscreen-keyboard {logon | all}

no onscreen-keyboard [logon | all]

구문 설명

logon	로그온 창에 화면 키보드를 삽입합니다.
all	로그온 창 및 로그인/비밀번호가 필요한 모든 창에 화면 키보드를 삽입합니다.

기본값

화면 키보드가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

화면 키보드를 사용하면 키스트로크 없이 사용자 자격 증명을 입력할 수 있습니다.

예

다음 예는 로그온 페이지에서 화면 키보드를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# onscreen-keyboard logon
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
webvpn	클라이언트리스 SSLVPN 연결을 위해 특성을 구성할 수 있는 webvpn 모드로 들어갑니다.

ospf authentication

OSPF 인증 사용을 활성화하려면 인터페이스 컨피그레이션 모드에서 **ospf authentication** 명령을 사용합니다. 기본 인증 상태를 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf authentication [**message-digest** | **null**]

no ospf authentication

구문 설명

message-digest	(선택 사항) OSPF 메시지 다이제스트 인증을 사용하도록 지정합니다.
null	(선택 사항) OSPF 인증을 사용하지 않도록 지정합니다.

기본값

기본적으로 OSPF 인증이 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

ospf authentication 명령을 사용하기 전에 **ospf authentication-key** 명령을 사용하여 인터페이스에 대한 비밀번호를 구성합니다. **message-digest** 키워드를 사용하는 경우 **ospf message-digest-key** 명령을 통해 인터페이스에 대한 message-digest 키를 구성합니다.

이전 버전과의 호환성을 위해 영역에 대한 인증 유형이 여전히 지원됩니다. 인터페이스에 대해 인증 유형을 지정하지 않으면 영역에 대한 인증 유형이 사용됩니다(영역 기본값은 null 인증).

옵션 없이 이 명령을 사용하면 단순 비밀번호 인증이 활성화됩니다.

예

다음 예는 선택한 인터페이스의 OSPF에 대해 단순 비밀번호 인증을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf authentication
ciscoasa(config-if)#
```

관련 명령

명령	설명
ospf authentication-key	인접한 라우팅 디바이스에서 사용할 비밀번호를 지정합니다.
ospf message-digest-key	MD5 인증을 활성화하고 MD5 키를 지정합니다.

ospf authentication-key

인접한 라우팅 디바이스에서 사용할 비밀번호를 지정하려면 인터페이스 컨피그레이션 모드에서 **ospf authentication-key** 명령을 사용합니다. 비밀번호를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ospf authentication-key [**0** | **8**] *password*

no ospf authentication-key

구문 설명

0	암호화되지 않은 비밀번호가 이어짐을 지정합니다.
8	암호화된 비밀번호가 이어짐을 지정합니다.
password	인접한 라우팅 디바이스에서 사용할 OSPF 인증 비밀번호를 할당합니다. 비밀번호는 9자 미만이어야 합니다. 두 문자 사이에 공백을 포함할 수 있습니다. 맨 앞이나 맨 뒤의 공백은 무시됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

이 명령으로 생성된 비밀번호는 라우팅 프로토콜 패킷이 시작될 때 OSPF 헤더에 직접 삽입되는 키로 사용됩니다. 인터페이스 하나당 각 네트워크에 별도의 비밀번호를 할당할 수 있습니다. 동일한 네트워크의 모든 인접한 라우터에는 OSPF 정보를 교환할 수 있는 동일한 비밀번호가 있어야 합니다.

예참고

다음 예는 OSPF 인증을 위한 비밀번호를 지정하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf authentication-key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

관련 명령

명령	설명
area authentication	지정된 영역에 대해 OSPF 인증을 활성화합니다.
ospf authentication	OSPF 인증의 사용을 활성화합니다.

ospf cost

인터페이스를 통해 패킷을 전송하는 비용을 지정하려면 인터페이스 컨피그레이션 모드에서 **ospf cost** 명령을 사용합니다. 인터페이스 비용을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf cost *interface_cost*

no ospf cost

구문 설명

interface_cost	인터페이스를 통해 패킷을 전송하는 비용(link-state 메트릭). 이 매개변수는 범위 0~65535의 무부호 정수 값입니다. 0은 인터페이스에 직접 연결된 네트워크를 나타냅니다. 인터페이스 대역폭이 클수록 해당 인터페이스에 패킷을 전송하기 위한 관련 비용이 낮아집니다. 다시 말해, 큰 비용 값은 낮은 대역폭 인터페이스를 나타내고 작은 비용 값은 높은 대역폭 인터페이스를 나타냅니다. ASA의 OSPF 인터페이스 기본 비용은 10입니다. 이 기본값은 Cisco IOS 소프트웨어와 다릅니다. Cisco IOS 소프트웨어의 경우 고속 이더넷의 기본 비용은 1이고 10BaseT의 기본 비용은 10입니다. 네트워크에서 ECMP를 사용 중인 경우 이 차이를 고려해야 합니다.

기본값

기본 *interface_cost*는 10입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

ospf cost 명령을 사용하면 인터페이스에서 패킷을 전송하는 비용을 명시적으로 지정할 수 있습니다. *interface_cost* 매개변수는 범위 0~65535의 무부호 정수 값입니다.

no ospf cost 명령을 사용하면 경로 비용을 기본값으로 재설정할 수 있습니다.

예

다음 예는 선택한 인터페이스에서 패킷을 전송하는 비용을 지정하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf cost 4
```

관련 명령

명령	설명
show running-config interface	지정된 인터페이스의 컨피그레이션을 표시합니다.

ospf database-filter

동기화 및 플러딩 중 OSPF 인터페이스에 대한 모든 나가는 LSA를 필터링하려면 인터페이스 컨피그레이션 모드에서 **ospf database-filter** 명령을 사용합니다. LSA를 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf database-filter all out

no ospf database-filter all out

구문 설명

all out	OSPF 인터페이스에 대한 모든 나가는 LSA를 필터링합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ospf database-filter 명령은 OSPF 인터페이스에 대한 나가는 LSA를 필터링합니다. **no ospf database-filter all out** 명령은 인터페이스에 대한 LSA의 전달을 복원합니다.

예

다음 예는 **ospf database-filter** 명령을 사용하여 나가는 LSA를 필터링하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf database-filter all out
```

관련 명령

명령	설명
show interface	인터페이스 상태 정보를 표시합니다.

ospf dead-interval

인접 디바이스에서 라우터가 다운되었음을 선언하기까지의 간격을 지정하려면 인터페이스 컨피그레이션 모드에서 **ospf dead-interval** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf dead-interval {*seconds*| **minimal hello-multiplier** *multiplier*}

no ospf dead-interval

구문 설명

seconds	Hello 패킷이 보이지 않는 기간. *seconds*의 기본값은 **ospf hello-interval** 명령으로 설정된 간격의 4배입니다(범위 1~65535).
minimal	Dead 간격을 1초로 설정합니다. 이 키워드를 사용하려면 hello-multiplier 키워드 및 multiplier 인수도 구성해야 합니다.
hello-multiplier *multiplier*	1초 동안 전송되는 hello 패킷의 수를 나타내는 범위 3~20의 정수 값.

기본값

*seconds*의 기본값은 **ospf hello-interval** 명령으로 설정된 간격의 4배입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.
9.2(1)	Fast Hello Packets에 대한 지원이 추가되었습니다.

사용 지침

ospf dead-interval 명령을 사용하면 인접 디바이스에서 라우터가 다운되었음을 선언하기까지의 dead 간격(hello 패킷이 보이지 않는 기간)을 설정할 수 있습니다. *seconds* 인수는 dead 간격을 지정하며, 네트워크의 모든 노드에서 동일해야 합니다. *seconds*의 기본값은 **ospf hello-interval** 명령으로 설정된 간격의 4배입니다(범위 1~65535).

no ospf dead-interval 명령은 기본 간격 값을 복원합니다.

Dead 간격은 OSPF hello 패킷에서 광고됩니다. 이 값은 특정 네트워크의 모든 네트워킹 디바이스에서 동일해야 합니다.

더 작은 dead 간격(초)을 지정하면 인접 디바이스의 다운을 더 빠르게 감지하여 컨버전스를 개선할 수 있지만, 라우팅이 더 불안정해질 수 있습니다.

OSPF Support for Fast Hello Packets

Minimal 및 hello-multiplier 키워드를 multiplier 인수와 함께 지정하면 OSPF Fast Hello Packets를 활성화할 수 있습니다. Minimal 키워드는 dead 간격을 1초로 설정하고, hello-multiplier 값은 1초 동안 전송되는 hello 패킷의 수를 설정하므로 1초 미만의 또는 "빠른" hello 패킷이 제공됩니다.

Fast Hello Packets가 인터페이스에서 구성되면, 이 인터페이스로 전송되는 Hello 패킷에서 광고되는 Hello 간격은 0으로 설정됩니다. 이 인터페이스를 통해 수신되는 Hello 패킷의 Hello 간격은 무시됩니다.

1초로 설정하든(Fast Hello Packets의 경우) 다른 값으로 설정하든, Dead 간격은 세그먼트에서 일정해야 합니다. Hello multiplier의 경우에는 Dead 간격 내에 최소 하나 이상의 Hello 패킷이 전송된다면 전체 세그먼트에서 동일하지 않아도 됩니다.

Dead 간격 및 Fast Hello 간격을 확인하려면 **show ospf interface** 명령을 사용합니다.

예

다음 예에서는 minimal 키워드 및 hello-multiplier 키워드와 값을 지정하여 OSPF Support for Fast Hello Packets를 활성화합니다. Multiplier가 5로 설정되어 있으므로 1초마다 5개의 Hello 패킷이 전송됩니다.

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
```

관련 명령

명령	설명
ospf hello-interval	인터페이스에서 전송되는 hello 패킷 간의 간격을 지정합니다.
show ospf interface	OSPF 관련 인터페이스 정보를 표시합니다.

ospf hello-interval

인터페이스에서 전송되는 hello 패킷 간의 간격을 지정하려면 인터페이스 컨피그레이션 모드에서 **ospf hello-interval** 명령을 사용합니다. Hello 간격을 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

ospf hello-interval *seconds*

no ospf hello-interval

구문 설명

seconds	인터페이스에서 전송되는 hello 패킷 간의 간격을 지정합니다. 유효한 값의 범위는 1~65535초입니다.

기본값

hello-interval *seconds*의 기본값은 10초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

이 값은 hello 패킷에서 광고됩니다. Hello 간격의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 라우팅 트래픽이 더 많이 발생합니다. 이 값은 특정 네트워크의 모든 라우터 및 액세스 서버에서 동일해야 합니다.

예

다음 예는 OSPF hello 간격을 5초로 변경합니다.

```
ciscoasa(config-if)# ospf hello-interval 5
```

관련 명령

명령	설명
ospf dead-interval	인접 디바이스에서 라우터가 다운되었음을 선언하기까지의 간격을 지정합니다.
show ospf interface	OSPF 관련 인터페이스 정보를 표시합니다.

ospf message-digest-key

OSPF MD5 인증을 활성화하려면 인터페이스 컨피그레이션 모드에서 **ospf message-digest-key** 명령을 사용합니다. MD5 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ospf message-digest-key *key-id* **md5** [**0** | **8**] *key*

no ospf message-digest-key

구문 설명

key-id	MD5 인증을 활성화하고 숫자 인증 키 ID 번호를 지정합니다. 유효한 값의 범위는 1~255입니다.
md5 *key*	최대 16바이트의 영숫자 비밀번호입니다. 키 문자 사이에 공백을 포함할 수 있습니다. 맨 앞이나 맨 뒤의 공백은 무시됩니다. MD5 인증은 통신의 무결성을 확인하고, 발신지를 인증하며, 적시성을 점검합니다.
0	암호화되지 않은 비밀번호가 이어짐을 지정합니다.
8	암호화된 비밀번호가 이어짐을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

ospf message-digest-key 명령은 MD5 인증을 활성화합니다. 명령의 **no** 형식을 사용하면 이전 MD5 키가 제거됩니다. *key_id*는 인증 키에 대한 숫자 식별자이며 범위는 1~255입니다. *key*는 최대 16바이트의 영숫자 비밀번호입니다. MD5는 통신의 무결성을 확인하고, 발신지를 인증하며, 적시성을 점검합니다.

예

다음 예는 OSPF 인증을 위한 MD5 키를 지정하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf message-digest-key 3 md5 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

관련 명령

명령	설명
area authentication	OSPF 영역 인증을 활성화합니다.
ospf authentication	OSPF 인증의 사용을 활성화합니다.

ospf mtu-ignore

수신 데이터베이스 패킷에서 OSPF MTU(Maximum Transmission Unit) 불일치 감지를 비활성화하려면 인터페이스 컨피그레이션 모드에서 **ospf mtu-ignore** 명령을 사용합니다. MTU 불일치 감지를 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf mtu-ignore

no ospf mtu-ignore

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 **ospf mtu-ignore**가 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

OSPF에서는 인접 디바이스가 공통 인터페이스의 동일한 MTU를 사용하고 있는지 여부를 확인합니다. 인접 디바이스가 DBD(Database Descriptor) 패킷을 교환할 때 이러한 확인이 이루어집니다. DBD 패킷의 수신 MTU가 들어오는 인터페이스에 구성된 IP MTU보다 클 경우 OSPF 인접성이 설정되지 않습니다. **ospf mtu-ignore** 명령은 수신 DBD 패킷에서 OSPF MTU 불일치 감지를 비활성화합니다. 이 명령은 기본적으로 활성화되어 있습니다.

예

다음 예는 **ospf mtu-ignore** 명령을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf mtu-ignore
```

관련 명령

명령	설명
show interface	인터페이스 상태 정보를 표시합니다.

ospf network point-to-point non-broadcast

OSPF 인터페이스를 point-to-point, non-broadcast 네트워크로 구성하려면 인터페이스 컨피그레이션 모드에서 **ospf network point-to-point non-broadcast** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ospf network point-to-point non-broadcast

no ospf network point-to-point non-broadcast

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

ospf network point-to-point non-broadcast 명령을 사용하면 VPN 터널을 통해 OSPF 경로를 전송할 수 있습니다.

인터페이스를 point-to-point로 지정하는 경우 OSPF 인접 디바이스를 수동으로 구성해야 합니다. 동적 검색이 불가능하기 때문입니다. OSPF 인접 디바이스를 수동으로 구성하려면 라우터 컨피그레이션 모드에서 **neighbor** 명령을 사용합니다.

인터페이스가 point-to-point non-broadcast로 구성된 경우 다음과 같은 제한이 적용됩니다.

- 인터페이스에 대해 하나의 인접 디바이스만 정의할 수 있습니다.
- 암호화 엔드포인트를 가리키는 고정 경로를 정의해야 합니다.
- 인접 디바이스가 명시적으로 구성되어 있지 않은 한 인터페이스에서 인접성을 형성할 수 없습니다.
- 인터페이스에서 터널을 통해 OSPF가 실행 중일 경우, 업스트림 라우터가 있는 일반 OSPF를 동일한 인터페이스에서 실행할 수 없습니다.
- OSPF 인접 디바이스를 지정하기 전에 crypto-map을 인터페이스에 바인딩하여 OSPF 업데이트가 VPN 터널을 통해 전달되도록 해야 합니다. OSPF 인접 디바이스를 지정한 후에 crypto-map을 인터페이스에 바인딩한 경우, **clear local-host all** 명령을 사용하여 OSPF 연결을 지워 OSPF 인접성이 VPN 터널을 통해 설정될 수 있도록 합니다.

예

다음 예는 선택한 인터페이스를 point-to-point, non-broadcast 인터페이스로 구성하는 방법을 보여 줍니다.

```
ciscoasa(config-if)# ospf network point-to-point non-broadcast
ciscoasa(config-if)#
```

관련 명령

명령	설명
neighbor	수동으로 구성된 OSPF 인접 디바이스를 지정합니다.
show interface	인터페이스 상태 정보를 표시합니다.

ospf priority

OSPF 라우터 우선순위를 변경하려면 인터페이스 컨피그레이션 모드에서 **ospf priority** 명령을 사용합니다. 기본 우선순위를 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf priority *number*

no ospf priority [*number*]

구문 설명

number	라우터의 우선순위를 지정합니다. 유효한 값의 범위는 0~255입니다.

기본값

*number*의 기본값은 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

네트워크에 연결된 두 라우터가 모두 전용 라우터가 되려고 시도하는 경우 라우터 우선순위가 더 높은 라우터가 전용 라우터가 됩니다. 연관성이 있을 경우, 라우터 ID가 더 높은 라우터가 전용 라우터가 됩니다. 라우터 우선순위가 0으로 설정된 라우터는 전용 라우터 또는 백업 전용 라우터가 될 수 없습니다. 라우터 우선순위는 멀티액세스 네트워크의 인터페이스에 대해서만 구성됩니다(다시 말해, 포인트-투-포인트 네트워크에 대해서는 구성되지 않음).

예

다음 예는 선택한 인터페이스에서 OSPF 우선순위를 변경하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf priority 4
ciscoasa(config-if)#
```

관련 명령

명령	설명
show ospf interface	OSPF 관련 인터페이스 정보를 표시합니다.

ospf retransmit-interval

인터페이스에 속하는 인접성에 대해 LSA 재전송 간의 시간을 지정하려면 인터페이스 컨피그레이션 모드에서 **ospf retransmit-interval** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf retransmit-interval [*seconds*]

no ospf retransmit-interval [*seconds*]

구문 설명

seconds	인터페이스에 속하는 인접성에 대해 LSA 재전송 간의 시간을 지정합니다. 유효한 값의 범위는 1~65535초입니다.

기본값

retransmit-interval *seconds*의 기본값은 5초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

라우터에서는 LSA를 인접 디바이스로 전송하면 승인 메시지가 수신될 때까지 LSA를 보관합니다. 승인 메시지를 수신하지 못할 경우 라우터에서는 LSA를 다시 전송합니다.

이 매개변수를 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.

예

다음 예는 LSA의 재전송 간격을 변경하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ospf retransmit-interval 15
ciscoasa(config-if)#
```

관련 명령

명령	설명
show ospf interface	OSPF 관련 인터페이스 정보를 표시합니다.

ospf transmit-delay

인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 설정하려면 인터페이스 컨피그레이션 모드에서 **ospf transmit-delay** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

ospf transmit-delay [*seconds*]

no ospf transmit-delay [*seconds*]

구문 설명

seconds	인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 설정합니다. 기본값은 1이고 범위는 1~65535초입니다.

기본값

*seconds*의 기본값은 1초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

업데이트 패킷의 LSA에는 전송 전에 *seconds* 인수로 지정한 양만큼 증가된 기간이 포함됩니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다.

링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다.

예

다음 예는 선택한 인터페이스에 대해 전송 지연을 3초로 설정합니다.

```
ciscoasa(config-if)# ospf restransmit-delay 3
ciscoasa(config-if)#
```

관련 명령

명령	설명
show ospf interface	OSPF 관련 인터페이스 정보를 표시합니다.

otp expiration

로컬 CA(인증 기관) 등록 페이지용으로 발급된 OTP(일회용 비밀번호)의 유효 기간(시간 단위)을 지정하려면 ca 서버 컨피그레이션 모드에서 **otp expiration** 명령을 사용합니다. 기간을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

otp expiration *timeout*

no otp expiration

구문 설명

timeout	등록 페이지의 OTP가 만료되기까지 사용자가 로컬 CA의 인증서를 등록해야 하는 시간을 지정합니다. 유효한 값의 범위는 1~720시간(30일)입니다.

기본값

기본적으로 특정 등록에 대한 OTP 만료 기간은 72시간(3일)입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

OTP 만료 기간은 사용자가 CA 서버의 등록 페이지에 로그인해야 하는 시간을 지정합니다. 사용자가 로그인하여 인증서를 등록하면 **enrollment retrieval** 명령으로 지정한 기간이 시작됩니다.

참고 등록 인터페이스 페이지에서 인증서를 등록하는 데 필요한 사용자 OTP는 해당 사용자에 대해 발급된 인증서와 키 쌍이 포함된 PKCS12 파일을 잠금 해제하기 위한 비밀번호로도 사용됩니다.

예

다음 예는 등록 페이지용 OTP가 24시간 동안 적용되도록 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# otp expiration 24
ciscoasa(config-ca-server)#
```

다음 예는 OTP 기간을 기본값인 72시간으로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server))# no otp expiration
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 ca 서버 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다.
enrollment-retrieval	등록된 사용자가 PKCS12 등록 파일을 검색할 수 있는 기간(시간 단위)을 지정합니다.
show crypto ca server	인증 기관 컨피그레이션을 표시합니다.

output console

action 명령의 출력을 콘솔로 전송하려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **output console** 명령을 사용합니다. 출력 대상으로서의 콘솔을 제거하려면 이 명령의 **no** 형식을 사용합니다.

output console

no output console

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

action 명령의 출력을 콘솔로 전송하려면 이 명령을 사용합니다.

예

다음 예는 **action** 명령의 출력을 콘솔로 전송합니다.

```
ciscoasa(config-applet)# output console
```

관련 명령

명령	설명
output file append	**action** 명령 출력을 단일 파일에 기록하지만, 이 파일은 매번 추가됩니다.
output file new	**action** 명령의 출력을 호출되는 각 애플릿에 대한 새 파일로 전송합니다.
output file overwrite	**action** 명령 출력을 단일 파일에 기록하지만, 이 파일은 매번 잘립니다.
output file rotate	순환되는 파일의 집합을 만듭니다.
output none	**action** 명령의 모든 출력을 버립니다.

output file

action 명령 출력을 지정된 파일로 리디렉션하려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **output file** 명령을 사용합니다. 지정된 작업을 제거하려면 이 명령의 **no** 형식을 사용합니다.

output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]

no output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]

구문 설명

append *filename*	출력을 지정된 파일 이름(ASA 기준으로 로컬 파일 이름)에 계속 추가합니다.
new	eem-*applet-timestamp*.log라는 이름의 출력용 새 파일을 만듭니다. 여기서 *applet*은 이벤트 관리자 애플릿의 이름이고, *timestamp*는 YYYYMMDD-hhmmss 형식의 날짜가 지정된 타임스탬프입니다.
overwrite *filename*	지정된 파일 이름에 출력을 기록하지만, 이벤트 관리자 애플릿이 호출될 때마다 출력이 잘립니다.
rotate *n*	eem-*applet-x*.log라는 이름의 출력용 파일을 만듭니다. 여기서 *applet*은 이벤트 관리자 애플릿의 이름이고, *x*는 파일 번호입니다. 새 파일이 작성되면 가장 오래된 파일이 삭제되며, 첫 번째 파일이 작성되기 전에 모든 후속 파일의 번호가 다시 지정됩니다. 최신 파일은 0으로 표시되고, 기존 파일은 가장 높은 숫자(*n*-1)로 표시됩니다. *n* 인수는 순환 값을 지정합니다. 유효한 값의 범위는 2~100입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

action 명령 출력을 지정된 파일로 리디렉션하려면 **output file** 명령을 사용합니다.

예

다음 예는 출력을 단일 파일에 추가합니다.

```
ciscoasa(config-applet)# output file append examplefile1
```

다음 예는 **action** 명령의 출력을 새 파일로 전송합니다.

```
ciscoasa(config-applet)# output file new
```

다음 예는 잘리는 단일 파일에 출력을 기록합니다.

```
ciscoasa(config-applet)# output file overwrite examplefile1
```

다음 예는 순환되는 파일의 집합을 만듭니다.

```
ciscoasa(config-applet)# output file rotate 50
```

관련 명령

명령	설명
output console	**action** 명령의 출력을 콘솔로 전송합니다.
output none	**action** 명령의 모든 출력을 버립니다.

output none

action 명령의 출력을 버리려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **output none** 명령을 사용합니다. **action** 명령의 출력을 유지하려면 이 명령의 **no** 형식을 사용합니다.

output none

no output none

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본값은 **action** 명령의 모든 출력을 버리는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

action 명령의 출력을 버리려면 이 명령을 사용합니다.

예

다음 예는 **action** 명령의 모든 출력을 버립니다.

```
ciscoasa(config-applet)# output none
```

관련 명령

명령	설명
output console	**action** 명령의 출력을 콘솔로 전송합니다.
output file append	**action** 명령 출력을 단일 파일에 기록하지만, 이 파일은 매번 추가됩니다.
output file new	**action** 명령의 출력을 호출되는 각 애플릿에 대한 새 파일로 전송합니다.
output file overwrite	**action** 명령 출력을 단일 파일에 기록하지만, 이 파일은 매번 잘립니다.
output file rotate	순환되는 파일의 집합을 만듭니다.

outstanding

미인증 이메일 프록시 세션 수를 제한하려면 해당 이메일 프록시 컨피그레이션 모드에서 **outstanding** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

outstanding {*number*}

no outstanding

구문 설명

number 허용되는 미인증 세션의 수. 범위는 1~1000입니다.

기본값

기본값은 20일입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Pop3s	• 예	—	• 예	—	—
Imap4s	• 예	—	• 예	—	—
Smtps	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 버전을 사용합니다. 그러면 미인증 세션이 무제한 허용됩니다. 이메일 포트에 대한 DOS 공격도 제한합니다.

이메일 프록시 연결 상태는 세 가지입니다.

1. 새 이메일을 연결하면 "unauthenticated(미인증)" 상태가 됩니다.
2. 연결에 사용자 이름이 제공되면 "authenticating(인증 중)" 상태가 됩니다.
3. ASA에서 연결을 인증하면 "authenticated(인증됨)" 상태가 됩니다.

미인증 상태의 연결 수가 구성된 제한을 초과하면 ASA에서는 오버로드를 막기 위해 가장 오래된 미인증 상태의 연결을 종료합니다. 인증된 연결은 종료하지 않습니다.

예

다음 예는 POP3S 이메일 프록시에 대해 미인증 세션 제한을 12로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# outstanding 12
```

override-account-disable

AAA 서버의 account-disabled 표시를 무시하려면 tunnel-group general-attributes 컨피그레이션 모드에서 **override-account-disable** 명령을 사용합니다. 무시를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

override-account-disable

no override-account-disable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1.1	이 명령이 추가되었습니다.

사용 지침

이 명령은 "account-disabled" 표시를 반환하는 NT LDAP 포함 RADIUS 및 Kerberos 등의 서버에 대해 유효합니다.

IPsec RA 및 WebVPN 터널 그룹에 대해 이 특성을 구성할 수 있습니다.

예

다음 예는 WebVPN 터널 그룹 "testgroup"용 AAA 서버의 "account-disabled" 표시기를 무시하도록 허용합니다.

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

다음 예는 IPsec 원격 액세스 터널 그룹 "QAgroup"용 AAA 서버의 "account-disabled" 표시기를 무시하도록 허용합니다.

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

관련 명령

명령	설명
clear configure tunnel-group	특정 터널 그룹에 대한 컨피그레이션 또는 터널 그룹 데이터베이스를 지웁니다.
tunnel-group general-attributes	tunnel-group general-attributes 값을 구성합니다.

override-svc-download

AnyConnect 또는 SSL VPN 클라이언트 다운로드를 위한 그룹 정책 또는 사용자 이름 특성을 재지정하도록 연결 프로필을 구성하려면 tunnel-group webvpn attributes 컨피그레이션 모드에서 **override-svc-download** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

override-svc-download enable

no override-svc-download enable

기본값

기본값은 disabled입니다. ASA에서는 클라이언트 다운로드를 위한 그룹 정책 또는 사용자 이름 특성 컨피그레이션을 재지정하지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

보안 어플라이언스는 클라이언트리스 및/또는 SSL VPN이 그룹 정책 또는 사용자 이름 특성에서 활성화되어 있는지 여부를 기반으로(**vpn-tunnel-protocol** 명령 사용) 원격 사용자를 위한 클라이언트리스, AnyConnect 또는 SSL VPN 클라이언트 연결을 허용합니다. **svc ask** 명령은 사용자에게 클라이언트를 다운로드할지 아니면 WebVPN 홈 페이지로 돌아갈지를 묻는 프롬프트를 표시함으로써 클라이언트 사용자 환경을 추가로 수정합니다.

그러나 클라이언트리스 SSL VPN 홈 페이지로 돌아가기 전 다운로드 프롬프트의 만료를 대기하는 지연이 발생하지 않도록, 특정 터널 그룹에서는 클라이언트리스 사용자 로그인이 필요할 수 있습니다. **override-svc-download** 명령을 사용하면 연결 프로필 수준에서 이러한 사용자의 지연을 방지할 수 있습니다. 이 명령을 사용하면 **vpn-tunnel-protocol** 또는 **svc ask** 명령 설정과 상관없이, 연결 프로필을 통해 로그인하는 사용자에게 클라이언트리스 SSL VPN 홈 페이지가 즉시 표시됩니다.

예

다음 예에서는 사용자가 연결 프로필 *engineering*에 대해 tunnel-group webvpn attributes 컨피그레이션 모드로 들어가며, 연결 프로필을 활성화하여 클라이언트 다운로드 프롬프트를 위한 그룹 정책 및 사용자 이름 특성 설정을 재지정합니다.

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# override-svc-download
```

관련 명령

명령	설명
show webvpn svc	설치된 SSL VPN 클라이언트에 대한 정보를 표시합니다.
svc	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
svc image	원격 PC로 다운로드하기 위해 ASA가 캐시 메모리에서 확장하는 클라이언트 패키지 파일을 지정합니다.

15 장

packet-tracer through ping 명령

packet-tracer

방화벽 규칙 테스트를 위해 5-튜플을 지정하여 문제 해결을 위한 패킷 추적 기능을 활성화하려면 특별 권한 EXEC 모드에서 **packet-tracer** 명령을 사용합니다. 명확성을 위해 구문은 ICMP, TCP/UDP 및 IP 패킷 모델링에 대해 별도로 표시됩니다.

packet-tracer input *ifc_name* **icmp** [**inline-tag** *tag*]
{*sip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}
type code [*ident*]
{*dip* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}
[**detailed**] [**xml**]

packet-tracer input *ifc_name* {**tcp** | **udp**} [**inline-tag** *tag*]
{*sip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *sport*
{*dip* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dport*
[**detailed**] [**xml**]

packet-tracer input *ifc_name* **rawip** [**inline-tag** *tag*]
{*sip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *protocol*
{*dip* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}
[**detailed**] [**xml**]

구문 설명

code	ICMP 패킷 추적을 위한 ICMP 코드를 지정합니다.
detailed	(선택 사항) 자세한 추적 결과 정보를 제공합니다.
dip	패킷 추적을 위한 IPv4 또는 IPv6 수신 주소를 지정합니다.
dport	TCP/UDP 패킷 추적을 위한 목적지 포트를 지정합니다.
fqdn *fqdn-string*	소스 및 수신 IP 주소가 될 수 있는, 호스트의 정규화된 도메인 이름을 지정합니다. IPv4용 FQDN만 지원합니다.
icmp	사용할 프로토콜이 ICMP임을 지정합니다.
ident	(선택 사항) ICMP 패킷 추적용 ICMP 식별자를 지정합니다.
inline-tag *tag*	Layer 2 CMD 헤더에 삽입되는 보안 그룹 태그 값을 지정합니다. 유효한 값의 범위는 0~65533입니다.
input *ifc_name*	패킷을 추적할 소스 인터페이스의 이름을 지정합니다.
protocol	원시 IP 패킷 추적을 위한 프로토콜 번호를 지정합니다(0~255).
rawip	사용할 프로토콜이 원시 IP임을 지정합니다.
security-group {**name** *name* | **tag** *tag*}	Trustsec용 IP-SGT 조회를 기반으로 소스 및 대상 보안 그룹을 지정합니다. 보안 그룹 이름 또는 태그 번호를 지정할 수 있습니다.
sip	패킷 추적을 위한 IPv4 또는 IPv6 소스 주소를 지정합니다.
sport	TCP/UDP 패킷 추적을 위한 소스 포트를 지정합니다.
tcp	사용할 프로토콜이 TCP임을 지정합니다.
type	ICMP 패킷 추적을 위한 ICMP 유형을 지정합니다.
udp	사용할 프로토콜이 UDP임을 지정합니다.
user *username*	사용자를 소스 IP 주소로 지정하려는 경우 사용자 ID를 domain\user 형식으로 지정합니다. 사용자에 대해 가장 최근에 매핑된 주소(있는 경우)가 추적에 사용됩니다.
xml	(선택 사항) 추적 결과를 XML 형식으로 표시합니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	• 예	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.4(2)	두 개의 키워드-인수 쌍, **user** *username* 및 **fqdn** *fqdn string* 이 추가되었습니다. 여러 키워드의 이름 및 정의가 변경되었습니다. IPv6 소스 주소에 대한 지원이 추가되었습니다.
9.0(1)	사용자 ID에 대한 지원이 추가되었습니다. IPv4 FQDN(정규화된 도메인 이름)만 지원됩니다.
9.3(1)	Layer 2 CMD 헤더에 포함되는 보안 그룹 태그 값을 지원하기 위해 **inline-tag** *tag* 키워드-인수 쌍이 추가되었습니다.

사용 지침

패킷 캡처 외에도, 패킷이 올바르게 작동하는지 확인하기 위해 ASA를 통해 패킷의 수명을 추적할 수 있습니다. **packet-tracer** 명령을 통해 다음을 수행할 수 있습니다.

- 프로덕션 네트워크의 모든 패킷 삭제를 디버깅합니다 .
- 컨피그레이션이 예상대로 작동하는지 확인합니다 .
- 규칙 추가를 일으킨 CLI 명령줄과 함께 패킷에 적용되는 모든 규칙을 표시합니다 .
- 데이터 경로에 있는 패킷 변경의 타임라인을 표시합니다 .
- 추적기 패킷을 데이터 경로에 삽입합니다 .
- 사용자 ID 및 FQDN 을 기반으로 IPv4 또는 IPv6 주소를 검색합니다 .

packet-tracer 명령은 패킷 및 패킷이 ASA에서 처리되는 방법에 대한 자세한 정보를 제공합니다. 컨피그레이션의 명령으로 인해 패킷이 누락되지 않은 경우 **packet-tracer** 명령은 원인에 대한 정보를 읽기 쉬운 형식으로 제공합니다. 예를 들어 잘못된 헤더 검증 때문에 패킷이 삭제된 경우 "packet dropped due to bad ip header (reason)" 메시지가 표시됩니다.

이 명령의 소스 부분에서 사용자 ID를 domain\user 형식으로 지정할 수 있습니다. ASA는 사용자의 IP 주소를 검색하여 패킷 추적 테스트에 사용합니다. 한 사용자가 여러 IP 주소에 매핑된 경우 가장 최근의 로그인 IP 주소가 사용되며, 더 많은 IP 주소-사용자 매핑이 존재한다는 내용이 출력에 표시됩니다. 사용자 ID가 이 명령의 소스 부분에 지정되어 있으면 ASA에서는 사용자가 입력한 목적지 주소 유형을 기반으로 사용자의 IPv4 또는 IPv6 주소를 검색합니다.

이 명령의 소스 부분에 보안 그룹 이름 또는 보안 그룹 태그를 지정할 수 있습니다. ASA에서는 보안 그룹 이름 또는 보안 그룹 태그를 기반으로 IP 주소를 검색하여 패킷 추적 테스트에 사용합니다. 하나의 보안 그룹 태그 또는 보안 그룹 이름이 여러 IP 주소에 매핑된 경우 IP 주소 중 하나가 사용되며, 더 많은 IP 주소-보안 그룹 태그 매핑이 존재한다는 내용이 출력에 표시됩니다.

이 명령은 FQDN을 지원합니다. 즉, FQDN을 소스 및 수신 주소로서 지정할 수도 있습니다. ASA에서는 먼저 DNS 조회를 수행한 다음, 패킷 구조를 위한 첫 번째 반환 IP 주소를 검색합니다. 여러 IP 주소가 확인되면, 여러 DNS 확인 IP 주소가 존재한다는 내용이 출력에 표시됩니다. IPv4 FQDN만 지원됩니다.

예

다음 예는 10.100.10.10~10.100.11.11의 HTTP 포트에 대해 TCP 패킷을 추적합니다. 다음 결과는 패킷이 암시적 거부 액세스 규칙에 의해 삭제될 것임을 나타냅니다.

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10  80 10.100.11.11 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

다음 예는 사용자 이름 CISCO\abc로 내부 호스트 10.0.0.2에서 외부 호스트 20.0.0.2까지 패킷을 추적하는 방법을 보여줍니다.

```
ciscoasa# packet-tracer input inside icmp user CISCO\abc 0 0 1 20.0.0.2

Source: CISCO\abc 10.0.0.2

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interfce: outside
output-status: up
output-line-status: up
Action: allow
```

다음 예는 사용자 이름 CISCO\abc로 내부 호스트 10.0.0.2에서 외부 호스트 20.0.0.2까지 패킷을 추적하고 추적 결과를 XML 형식으로 표시합니다.

```
<Source>
<user>CISCO\abc</user>
<user-ip>10.0.0.2</user-ip>
<more-ip>1</more-ip>
</Source>

<Phase>
<id>1</id>
<type>ROUTE-LOOKUP</type>
<subtype>input</subtype>
<result>ALLOW</result>
<config>
</config>
<extra>
in 20.0.0.0 255.255.255.0 outside
</extra>
</Phase>
```

다음 예는 내부 호스트 xyz.example.com에서 외부 호스트 abc.example.com까지 패킷을 추적하는 방법을 보여줍니다.

```
ciscoasa# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com 23
Mapping FQDN xyz.example.com to IP address 10.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)

Mapping FQDN abc.example.com to IP address 20.0.0.2
(More IP addresses resolved. Please run "show dns-host" to check.)

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

다음 예는 IP 주소에 대한 보안 그룹 태그 매핑을 보여주는 **packet-tracer** 명령의 출력을 표시합니다.

```
ciscoasa# packet-tracer input inside tcp security-group name alpha 30 security-group tag
31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

다음 예는 Layer 2 SGT Imposition을 보여주는 **packet-tracer** 명령의 출력을 표시합니다.

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 10.1.1.2 30 192.168.1.2 300
```

관련 명령

명령	설명
capture	추적 패킷을 포함하여 패킷 정보를 캡처합니다.
show capture	옵션을 지정하지 않은 경우의 캡처 컨피그레이션을 표시합니다.

page style

WebVPN 사용자가 보안 어플라이언스에 연결할 때 표시되는 WebVPN 페이지를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **page style** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하고 값이 상속되도록 하려면 이 명령의 **no** 형식을 사용합니다.

page style *value*

[**no**] **page style** *value*

구문 설명

value	CSS(Cascading Style Sheet) 매개변수(최대 256자)

기본값

기본 페이지 스타일은 background-color:white;font-family:Arial,Helv,sans-serif입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 CSS(Cascading Style Sheet) 매개변수로서 표현됩니다. 이러한 매개변수에 대해 설명하는 것은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트 www.w3.org에서 제공하는 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수의 편리한 목록이 포함되어 있습니다.

WebVPN 페이지에 대한 가장 일반적인 변경 사항, 즉 페이지 색상과 관련된 몇 가지 팁은 다음과 같습니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값, 색상의 이름(HTML에서 인식되는 경우) 등을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며 각 색상은 0~255 범위의 십진수입니다. 쉼표로 구분된 엔트리는 다른 색상과 결합되는 각 색상의 강도 수준을 나타냅니다.
- HTML 형식은 #000000으로서, 여섯 자리 16진수 형식으로 되어 있습니다. 첫 번째와 두 번째는 빨강, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파랑을 나타냅니다.

참고 WebVPN 페이지를 손쉽게 사용자 지정하려면 색상 조각, 미리 보기 기능 등의 스타일 요소를 구성하기 위한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예는 페이지 스타일을 large로 사용자 지정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# page style font-size:large
```

관련 명령

명령	설명
logo	WebVPN 페이지의 로고를 사용자 지정합니다.
title	WebVPN 페이지의 제목을 사용자 지정합니다.

pager

텔넷 세션에 대해 "---More---" 프롬프트가 나타나기까지 페이지의 기본 줄 수를 설정하려면 글로벌 컨피그레이션 모드에서 **pager** 명령을 사용합니다.

pager [**lines**] *lines*

구문 설명

[**lines**] *lines*	"---More---" 프롬프트가 나타나기까지 페이지의 줄 수를 설정합니다. 기본값은 24줄이고, 0은 페이지 제한이 없음을 의미합니다. 범위는 0~2147483647줄입니다. **lines** 키워드는 선택 사항이고, 이 키워드의 유무와 상관없이 명령은 동일합니다.

기본값

기본값은 24줄입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령은 특별 권한 EXEC 모드 명령에서 글로벌 컨피그레이션 모드 명령으로 변경되었습니다. **terminal pager** 명령이 특별 권한 EXEC 모드 명령으로 추가되었습니다.

사용 지침

이 명령은 텔넷 세션에 대한 기본 pager 줄 설정을 변경합니다. 현재 세션에 대해서만 임시로 설정을 변경하려는 경우 **terminal pager** 명령을 사용합니다.

관리 컨텍스트에서 텔넷을 사용하는 경우 다른 컨텍스트로 변경하면, 지정된 컨텍스트의 **pager** 명령에 다른 설정이 있더라도 pager 줄 설정이 세션을 따라갑니다. 현재의 pager 설정을 변경하려면 새 설정과 함께 **terminal pager** 명령을 입력하거나, 현재 컨텍스트에서 **pager** 명령을 입력할 수 있습니다. **pager** 명령은 새 pager 설정을 컨텍스트 컨피그레이션에 저장하는 것 외에도, 현재의 텔넷 세션에 새 설정을 적용합니다.

예

다음 예는 표시되는 줄의 수를 20으로 변경합니다.

```
ciscoasa(config)# pager 20
```

관련 명령

명령	설명
clear configure terminal	터미널 표시 너비 설정을 지웁니다.
show running-config terminal	현재 터미널 설정을 표시합니다.
terminal	텔넷 세션에 시스템 로그 메시지가 표시되도록 허용합니다.
terminal pager	"---more---" 프롬프트가 나타나기까지 텔넷 세션에 표시할 줄 수를 설정합니다. 이 명령은 컨피그레이션에 저장되지 않습니다.
terminal width	글로벌 컨피그레이션 모드에서 터미널 표시 너비를 설정합니다.

parameters

검사 정책 맵용 매개변수 설정을 위해 매개변수 컨피그레이션 모드로 들어가려면 정책 맵 컨피그레이션 모드에서 **parameters** 명령을 사용합니다.

parameters

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

Modular Policy Framework를 사용하면 많은 애플리케이션 검사에 대한 특별 작업을 구성할 수 있습니다. Layer 3/4 정책 맵에서(**policy-map** 명령) **inspect** 명령을 사용하여 검사 엔진을 활성화할 때, **policy-map type inspect** 명령으로 만든 검사 정책 맵에 정의된 대로 작업을 활성화할 수도 있습니다. 예를 들면 **inspect dns dns_policy_map** 명령을 입력합니다. 여기서 dns_policy_map은 검사 정책 맵의 이름입니다.

검사 정책 맵은 하나 이상의 **parameters** 명령을 지원할 수 있습니다. 매개변수는 검사 엔진의 동작에 영향을 미칩니다. 매개변수 컨피그레이션 모드에서 사용 가능한 명령은 애플리케이션에 따라 다릅니다.

예

다음 예는 기본 검사 정책 맵에서 DNS 패킷의 최대 메시지 길이를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 512
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

participate

가상 로드 밸런싱 클러스터에 디바이스를 강제로 추가하려면 VPN 로드 밸런싱 컨피그레이션 모드에서 **participate** 명령을 사용합니다. 디바이스를 클러스터에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

participate

no participate

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 디바이스는 vpn 로드 밸런싱 클러스터에 추가되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
VPN 로드 밸런싱 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

먼저 **interface** 및 **nameif** 명령을 사용하여 인터페이스를 구성하고 **vpn load-balancing** 명령을 사용하여 VPN 로드 밸런싱 모드로 들어가야 합니다. 또한 **cluster ip** 명령을 사용하여 클러스터 IP 주소를 미리 구성해야 하며, 가상 클러스터 IP 주소가 가리킬 인터페이스도 구성해두어야 합니다.

이 명령을 사용하면 이 디바이스가 가상 로드 밸런싱 클러스터에 강제로 추가됩니다. 디바이스의 추가를 활성화하려면 명시적으로 이 명령을 실행해야 합니다.

클러스터에 추가된 모든 디바이스는 IP 주소, 암호화 설정, 암호화 키, 포트 등 클러스터와 관련된 동일한 값을 공유하게 됩니다.

참고 암호화를 사용할 경우 **isakmp enable** *inside* 명령을 미리 구성해두어야 합니다. 여기서 *inside*는 로드 밸런싱 내부 인터페이스를 지정합니다. 로드 밸런싱 내부 인터페이스에서 isakmp가 활성화되어 있지 않으면 클러스터 암호화를 구성하려고 시도할 때 오류 메시지가 표시됩니다.

isakmp가 **cluster encryption** 명령을 구성할 때에는 활성화되었지만 **participate** 명령을 구성하기 전에 비활성화되면, **participate** 명령을 입력할 때 오류 메시지가 표시되며 로컬 디바이스는 클러스터에 추가되지 않습니다.

예

다음은 현재 디바이스를 vpn 로드 밸런싱 클러스터에 추가하는 **participate** 명령이 포함된 VPN 로드 밸런싱 명령 시퀀스의 예입니다.

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
vpn load-balancing	VPN 로드 밸런싱 모드로 들어갑니다.

passive-interface(RIP)

인터페이스에서 RIP 라우팅 업데이트의 전송을 비활성화하려면 라우터 컨피그레이션 모드에서 **passive-interface** 명령을 사용합니다. 인터페이스에서 RIP 라우팅 업데이트를 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

구문 설명

default	(선택 사항) 모든 인터페이스를 패시브 모드로 설정합니다.
if_name	(선택 사항) 지정된 인터페이스를 패시브 모드로 설정합니다.

기본값

RIP가 활성화되면 활성 RIP에 대해 모든 인터페이스가 활성화됩니다.

인터페이스 또는 **default** 키워드를 지정하지 않으면 명령이 기본적으로 **default**로 설정되며 컨피그레이션에 passive-interface default로 나타납니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

인터페이스에서 패시브 RIP를 활성화합니다. 인터페이스는 RIP 라우팅 브로드캐스트를 수신 대기하고 해당 정보를 사용하여 라우팅 테이블을 채우지만, 라우팅 업데이트를 브로드캐스트하지는 않습니다.

예

다음 예는 외부 인터페이스를 패시브 RIP로 설정합니다. 보안 어플라이언스의 다른 인터페이스는 RIP 업데이트를 송수신합니다.

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

관련 명령

명령	설명
clear configure rip	실행 중인 컨피그레이션에서 모든 RIP 명령을 지웁니다.
router rip	RIP 라우팅 프로세스를 활성화하고 rip 라우터 컨피그레이션 모드로 들어갑니다.
show running-config rip	실행 중인 컨피그레이션의 RIP 명령을 표시합니다.

passive-interface(EIGRP)

인터페이스에서 EIGRP 라우팅 업데이트의 송수신을 비활성화하려면 라우터 컨피그레이션 모드에서 **passive-interface** 명령을 사용합니다. 인터페이스에서 라우팅 업데이트를 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

구문 설명

default	(선택 사항) 모든 인터페이스를 패시브 모드로 설정합니다.
if_name	(선택 사항) 패시브 모드에 대한 인터페이스의 이름(**nameif** 명령으로 지정).

기본값

해당 인터페이스에 대해 라우팅이 활성화되면 모든 인터페이스가 액티브 라우팅(라우팅 업데이트 송수신)에 대해 활성화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.0(2)	EIGRP 라우팅에 대한 지원이 추가되었습니다.

사용 지침

인터페이스에서 패시브 라우팅을 활성화합니다. EIGRP의 경우에는 해당 인터페이스에서 라우팅 업데이트의 송수신을 비활성화합니다.

EIGRP 컨피그레이션에 **passive-interface** 명령을 두 개 이상 포함할 수 있습니다. **passive-interface default** 명령을 사용하여 모든 인터페이스에서 EIGRP 라우팅을 비활성화한 다음, **no passive-interface** 명령을 사용하여 특정 인터페이스에서 EIGRP 라우팅을 활성화할 수 있습니다.

예

다음 예는 외부 인터페이스를 패시브 EIGRP로 설정합니다. 보안 어플라이언스의 다른 인터페이스는 EIGRP 업데이트를 송수신합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

다음 예는 내부 인터페이스를 제외한 모든 인터페이스를 패시브 EIGRP로 설정합니다. 내부 인터페이스만 EIGRP 업데이트를 송수신합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface default
ciscoasa(config-router)# no passive-interface inside
```

관련 명령

명령	설명
show running-config router	실행 중인 컨피그레이션에서 라우터 컨피그레이션 명령을 표시합니다.

passive-interface(OSPFv3)

한 인터페이스 또는 OSPFv3 프로세스를 사용하는 모든 인터페이스에서 라우팅 업데이트의 송수신을 억제하려면 라우터 컨피그레이션 모드에서 **passive-interface** 명령을 사용합니다. 한 인터페이스 또는 OSPFv3 프로세스를 사용하는 모든 인터페이스에서 라우팅 업데이트를 다시 활성화하려면 이 명령의 **no** 형식을 사용합니다.

passive-interface [*interface_name*]

no passive-interface [*interface_name*]

구문 설명

interface_name	(선택 사항) OSPFv3 프로세스가 실행 중인 인터페이스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 인터페이스에서 패시브 라우팅을 활성화합니다.

예

다음 예는 내부 인터페이스에서 라우팅 업데이트의 송수신을 억제합니다.

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# passive-interface interface
ciscoasa(config-rtr)#
```

관련 명령

명령	설명
show running-config router	실행 중인 컨피그레이션에서 라우터 컨피그레이션 명령을 표시합니다.

passwd, password

텔넷용 로그인 비밀번호를 설정하려면 글로벌 컨피그레이션 모드에서 **passwd** 또는 **password** 명령을 사용합니다. 비밀번호를 재설정하려면 이 명령의 **no** 형식을 사용합니다.

{**passwd** | **password**} *password* [**encrypted**]

no {**passwd** | **password**} *password*

구문 설명

encrypted	(선택 사항) 비밀번호가 암호화된 형식임을 지정합니다. 비밀번호는 암호화된 형태로 컨피그레이션에 저장되므로 비밀번호를 입력하더라도 원래의 비밀번호를 볼 수 없습니다. 어떤 이유로든 다른 ASA에 비밀번호를 복사해야 하는데 원래의 비밀번호를 모르는 경우 **passwd** 명령을 암호화된 비밀번호 및 이 키워드와 함께 입력할 수 있습니다. 일반적으로 **show running-config passwd** 명령을 입력해야 이 키워드를 볼 수 있습니다.
passwd | **password**	두 명령은 상호 별칭이므로 둘 중 하나를 사용할 수 있습니다.
password	대/소문자를 구분하여 최대 80자의 영숫자로 비밀번호를 설정합니다. 비밀번호에는 공백을 포함해서는 안 됩니다.

기본값

9.1(1): 기본 비밀번호는 "cisco"입니다.

9.1(2): 기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.4(2)	SSH 기본 사용자 이름은 더 이상 지원되지 않습니다. **pix** 또는 **asa** 사용자 이름 및 로그인 비밀번호와 함께 SSH를 사용하여 ASA에 연결할 수 없습니다.
9.0(2), 9.1(2)	기본 비밀번호 "cisco"가 제거되었습니다. 사용자가 직접 로그인 비밀번호를 설정해야 합니다. **no passwd** 또는 **clear configure passwd** 명령을 사용하면 비밀번호가 제거됩니다. 전에는 기본값인 "cisco"로 재설정되었습니다.

사용 지침

telnet 명령으로 텔넷을 활성화하면 **passwd** 명령으로 설정된 비밀번호를 사용하여 로그인할 수 있습니다. 로그인 비밀번호를 입력하면 사용자 EXEC 모드에 들어가게 됩니다. **aaa authentication telnet console** 명령을 사용하여 텔넷 사용자마다 CLI 인증을 구성하는 경우 이 비밀번호가 사용되지 않습니다.

이 비밀번호는 스위치에서 ASASM로 연결하는 텔넷 세션에도 사용됩니다(**session** 명령 참조).

예

다음 예는 비밀번호를 Pa$$w0rd로 설정합니다.

```
ciscoasa(config)# passwd Pa$$w0rd
```

다음 예는 비밀번호를 또 다른 ASA에서 복사한 암호화된 비밀번호로 설정합니다.

```
ciscoasa(config)# passwd jMorNbK0514fadBh encrypted
```

관련 명령

명령	설명
clear configure passwd	로그인 비밀번호를 지웁니다.
enable	특별 권한 EXEC 모드로 들어갑니다.
enable password	비밀번호 활성화를 설정합니다.
show curpriv	현재 로그인한 사용자 이름 및 사용자 권한 수준을 보여줍니다.
show running-config passwd	로그인 비밀번호를 암호화된 형식으로 보여줍니다.

password encryption aes

비밀번호 암호화를 활성화하려면 글로벌 컨피그레이션 모드에서 password encryption aes 명령을 사용합니다. 비밀번호 암호화를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

password encryption aes

no password encryption aes

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.

사용 지침

비밀번호 암호화가 활성화되고 마스터 패스프레이즈가 사용 가능해지는 즉시 모든 사용자 비밀번호가 암호화됩니다. 실행 중인 컨피그레이션에서는 암호화된 형식으로 비밀번호를 표시합니다. 비밀번호 암호화가 활성화된 시점에 패스프레이즈가 구성되지 않은 경우, 나중에 패스프레이즈가 만들어질 것이라는 예상과 함께 이 명령은 성공합니다. 이 명령은 장애 조치 피어 간에 자동으로 동기화됩니다.

write erase 명령 뒤에 **reload** 명령을 사용하면 마스터 패스프레이즈가 제거됩니다(손실된 경우).

예

다음 예는 비밀번호 암호화를 활성화합니다.

```
Router (config)# password encryption aes
```

관련 명령

명령	설명
key config-key password-encryption	암호화 키를 생성하는 데 사용되는 패스프레이즈를 설정합니다.
write erase	이 명령 뒤에 **reload** 명령을 사용하는 경우, 손실된 마스터 패스프레이즈를 제거합니다.

password(crypto ca trustpoint)

등록 중에 CA와 함께 등록되는 챌린지 구문(challenge phrase)을 지정하려면 crypto ca trustpoint 컨피그레이션 모드에서 **password** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

password *string*

no password

구문 설명

string	비밀번호의 이름을 문자열로 지정합니다. 첫 번째 문자는 숫자가 될 수 없습니다. 문자열은 공백을 포함하여 최대 80자까지 모든 영숫자 문자를 포함할 수 있습니다. number-space-anything 형식의 비밀번호는 지정할 수 없습니다. 숫자 뒤에 공백을 사용하면 문제가 발생합니다. 예를 들어 "hello 21"은 사용 가능하지만 "21 hello"는 사용할 수 없습니다. 비밀번호는 대/소문자를 구분합니다. 예를 들어 "Secret" 비밀번호는 "secret" 비밀번호와 다릅니다.

기본값

기본 설정은 비밀번호를 포함하지 않는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 실제 인증서 등록이 시작되기 전에 인증서에 대한 폐기 비밀번호를 지정할 수 있습니다. 지정한 비밀번호는 업데이트된 구성이 ASA에 의해 NVRAM에 기록될 때 암호화됩니다.

CA는 일반적으로 챌린지 구문을 사용하여 후속 폐기 요청을 인증합니다.

이 명령이 활성화되면 인증서 등록 중에 비밀번호 입력 프롬프트가 표시되지 않습니다.

예

다음 예는 trustpoint central을 위한 crypto ca trustpoint 컨피그레이션 모드로 들어가며, trustpoint central에 대한 등록 요청에서 CA로 등록한 챌린지 구문을 포함합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# password zzxxyy
```

관련 명령

명령	설명
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드로 들어갑니다.
default enrollment	enrollment 매개변수를 기본값으로 되돌립니다.

password-management(tunnel-group general-attributes, config-mdm-proxy)

비밀번호 관리를 활성화하려면 tunnel-group general-attributes 컨피그레이션 모드 및 config-mdm-proxy 모드에서 **password-management** 명령을 사용합니다. 비밀번호 관리를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 일수를 기본값으로 재설정하려면 **password-expire-in-days** 키워드를 지정하여 명령의 **no** 형식을 사용합니다.

password-management [**password-expire-in-days** *days*]

no password-management

no password-management password-expire-in-days [*days*]

구문 설명

days	현재 비밀번호가 만료되기까지의 일수(0~180)를 지정합니다. **password-expire-in-days** 키워드를 지정하는 경우 이 매개변수가 필요합니다.
password-expire-in-days	(선택 사항) ASA에서 만료 임박에 대해 사용자에게 경고하기 시작하는, 현재 비밀번호가 만료되기까지의 일수를 바로 뒤에 오는 매개변수로 지정함을 나타냅니다. 이 명령은 LDAP 서버에 대해서만 유효합니다. 자세한 내용은 사용법 참고 섹션을 참조하십시오.

기본값

기본값은 비밀번호 관리 없음(no password management)입니다. LDAP 서버에 대해 **password-expire-in-days** 키워드를 지정하지 않는 경우 현재 비밀번호가 만료되기까지의 시작 경고 기본값은 14일입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—
config-mdm-proxy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.
9.3(1)	이제 이 명령을 config-mdm-proxy 모드에서 사용할 수 있습니다.

사용 지침

ASA는 RADIUS 및 LDAP 프로토콜에 대한 비밀번호 관리를 지원합니다. "password-expire-in-days" 옵션은 LDAP에 대해서만 지원됩니다.

IPsec 원격 액세스 및 SSL VPN 터널 그룹에 대해 비밀번호 관리를 구성할 수 있습니다.

password-management 명령을 구성하면 ASA에서는 원격 사용자가 로그인할 때 사용자의 현재 비밀번호가 곧 만료되는지 또는 이미 만료되었는지를 알려줍니다. 그런 다음 ASA에서는 사용자에게 비밀번호를 변경할 기회를 제공합니다. 현재 비밀번호가 아직 만료되지 않은 경우 사용자는 해당 비밀번호를 사용하여 로그인할 수 있습니다.

이 명령은 그러한 알림을 지원하는 AAA 서버(즉, NT 4.0 또는 Active Directory 서버로 프록시 처리되는 LDAP 서버 및 RADIUS)에 대해 유효합니다. RADIUS 또는 LDAP 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

참고 MSCHAP를 지원하는 일부 RADIUS 서버는 현재 MSCHAPv2를 지원하지 않습니다. 이 명령을 사용하려면 MSCHAPv2가 필요하므로 공급업체에 문의하십시오.

ASA 릴리스 7.1 이상에서는 MS-CHAPv2를 지원하는 RADIUS 컨피그레이션 또는 LDAP로 인증할 때 일반적으로 다음 연결 유형에 대한 비밀번호 관리를 지원합니다.

- AnyConnect VPN Client(ASA 소프트웨어 버전 8.0 이상)
- IPsec VPN Client
- 클라이언트리스 SSL VPN(ASA 소프트웨어 버전 8.0 이상) WebVPN(ASA 소프트웨어 버전 7.1~7.2.x)
- SSL VPN Client 풀 터널링 클라이언트

이러한 RADIUS 컨피그레이션에는 RADIUS와 LOCAL 인증, RADIUS와 Active Directory/Kerberos Windows DC, RADIUS와 NT/4.0 도메인, RADIUS와 LDAP 등이 포함됩니다.

Kerberos/Active Directory(Windows 비밀번호) 또는 NT 4.0 도메인의 이러한 연결 유형에 대해서는 비밀번호 관리가 지원되지 *않습니다*. RADIUS 서버(예: Cisco ACS)는 인증 요청을 또 다른 인증 서버로 프록시 처리할 수 있습니다. 그러나 ASA 관점에서 보면 RADIUS 서버와만 통신하는 것입니다.

참고 LDAP의 경우 비밀번호를 변경하는 방법은 시장의 다른 LDAP 서버에 대해 독점적입니다. 현재 ASA는 Microsoft Active Directory 및 Sun LDAP 서버에 대해 독점적인 비밀번호 관리 논리를 구현합니다.

기본 LDAP에는 SSL 연결이 필요합니다. LDAP에 대한 비밀번호 관리를 시도하기 전에 LDAP over SSL을 활성화해야 합니다. 기본적으로 LDAP는 포트 636을 사용합니다.

이 명령은 비밀번호가 만료되기까지의 일수를 변경하지 않습니다. 그보다는 ASA에서 비밀번호가 곧 만료된다고 사용자에게 경고하기 시작하는, 만료 전의 일수를 변경합니다.

password-expire-in-days 키워드를 지정하는 경우 일수도 지정해야 합니다.

일수를 0으로 설정하여 이 명령을 지정하면 이 명령이 비활성화됩니다. ASA에서 만료 임박에 대해 사용자에게 알리지 않지만, 사용자는 만료 후에도 비밀번호를 변경할 수 있습니다.

참고 Radius에서는 비밀번호 변경 또는 비밀번호 변경 프롬프트를 제공하지 않습니다.

예

다음 예는 WebVPN 터널 그룹 "testgroup"이 만료된다고 사용자에게 경고하기 시작하는, 비밀번호 만료까지의 일수를 90으로 설정합니다.

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# password-management password-expire-in-days 90
ciscoasa(config-tunnel-general)#
```

다음 예는 IPsec 원격 액세스 터널 그룹 "QAgroup"이 만료된다고 사용자에게 경고하기 시작하는, 비밀번호 만료까지의 기본값으로 14일을 사용합니다.

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# password-management
ciscoasa(config-tunnel-general)#
```

다음 예는 기본 비밀번호 만료 설정을 사용하는 MDM 프록시를 보여줍니다.

```
ciscoasa (config)# mdm-proxy
ciscoasa (config-mdm-proxy)# password-managment
```

관련 명령

명령	설명
clear configure passwd	로그인 비밀번호를 지웁니다.
passwd	로그인 비밀번호를 설정합니다.
radius-with-expiry	RADIUS 인증 중에 비밀번호 업데이트의 협상을 활성화합니다(사용되지 않음).
show running-config passwd	로그인 비밀번호를 암호화된 형식으로 보여줍니다.
tunnel-group general-attributes	tunnel-group general-attributes 값을 구성합니다.
mdm-proxy	MDM 프록시를 구성합니다.

password-parameter

SSO 인증을 위한 사용자 비밀번호를 제출해야 하는 HTTP POST 요청 매개변수의 이름을 지정하려면 aaa-server-host 컨피그레이션 모드에서 **password-parameter** 명령을 사용합니다. 다음은 HTTP Forms 명령의 SSO입니다.

password-parameter *string*

참고 SSO와 HTTP를 정확히 구성하려면 인증 및 HTTP 교환에 대한 철저한 실무 지식이 필요합니다.

구문 설명

string	HTTP POST 요청에 포함되는 비밀번호 매개변수의 이름. 최대 비밀번호 길이는 128자입니다.

기본값

기본값 또는 동작이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server-host 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

ASA의 WebVPN 서버는 HTTP POST 요청을 사용하여 인증 웹 서버에 SSO(단일 로그인) 인증 요청을 제출합니다. 필수 명령 **password-parameter**는 POST 요청에 SSO 인증을 위한 사용자 비밀번호 매개변수를 포함해야 함을 지정합니다.

참고 로그인 시 사용자는 실제 비밀번호 값을 입력하며, 이 값은 POST 요청에 입력되어 인증 웹 서버에 전달됩니다.

예

aaa-server-host 컨피그레이션 모드에서 입력하는 다음 예는 user_password라는 비밀번호 매개변수를 지정합니다.

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# password-parameter user_password
```

관련 명령

명령	설명
action-uri	SSO 인증용 사용자 이름 및 비밀번호를 수신하기 위한 웹 서버 URI를 지정합니다.
auth-cookie-name	인증 쿠키용 이름을 지정합니다.
hidden-parameter	인증 웹 서버와 교환할 숨겨진 매개변수를 만듭니다.
start-url	사전 로그인 쿠키를 수신할 URL을 지정합니다.
user-parameter	SSO 인증을 위해 사용자 이름을 제출해야 할 HTTP POST 요청 매개변수의 이름을 지정합니다.

password-policy authenticate enable

사용자가 자신의 사용자 계정을 수정하도록 허용할지 여부를 지정하려면 글로벌 컨피그레이션 모드에서 **password-policy authenticate enable** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy authenticate enable

no password-policy authenticate enable

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

인증은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

인증이 활성화되어 있으면 **username** 명령은 사용자가 자신의 비밀번호를 변경하거나 자신의 계정을 삭제하도록 허용하지 않습니다. 또한 **clear configure username** 명령은 사용자가 자신의 계정을 삭제하도록 허용하지 않습니다.

예

다음 예는 사용자가 자신의 계정을 수정하도록 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# password-policy authenticate enable
```

관련 명령

명령	설명
password-policy minimum-changes	새 비밀번호와 기존 비밀번호 간에 변경해야 할 최소 문자 수를 설정합니다.
password-policy minimum length	비밀번호의 최소 길이를 설정합니다.
password-policy minimum-lowercase	비밀번호에 포함해야 할 소문자의 최소 개수를 설정합니다.

password-policy lifetime

비밀번호가 만료된 후 현재의 컨텍스트 및 간격(날짜)에 대한 비밀번호 정책을 설정하려면 글로벌 컨피그레이션 모드에서 **password-policy lifetime** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy lifetime *value*

no password-policy lifetime *value*

구문 설명

value	비밀번호 수명을 지정합니다. 유효한 값의 범위는 0~65535일입니다.

기본값

수명 기본값은 0일입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

비밀번호에는 지정된 최대 수명이 있습니다. 수명 간격이 0일이면 로컬 사용자 비밀번호가 만료되지 않습니다. 비밀번호는 수명 만료일 다음 날 오전 12시에 만료됩니다.

예

다음 예는 비밀번호 수명 값을 10일로 지정합니다.

```
ciscoasa(config)# password-policy lifetime 10
```

관련 명령

명령	설명
password-policy minimum-changes	새 비밀번호와 기존 비밀번호 간에 변경해야 할 최소 문자 수를 설정합니다.
password-policy minimum length	비밀번호의 최소 길이를 설정합니다.
password-policy minimum-lowercase	비밀번호에 포함해야 할 소문자의 최소 개수를 설정합니다.

password-policy minimum-changes

새 비밀번호와 기존 비밀번호 간에 변경해야 할 최소 문자 수를 설정하려면 글로벌 컨피그레이션 모드에서 **password-policy minimum-changes** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy minimum-changes *value*

no password-policy minimum-changes *value*

구문 설명

value	새 비밀번호와 기존 비밀번호 간에 변경해야 할 문자 수를 지정합니다. 유효한 값의 범위는 0~64자입니다.

기본값

기본 변경 문자 수는 0입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

새 비밀번호는 기존 비밀번호와 다른 문자를 최소 4개 포함해야 하며 기존 비밀번호의 어디에도 나타나지 않는 경우에만 변경된 것으로 간주됩니다.

예

다음 예는 기존 비밀번호와 새 비밀번호 간에 변경해야 할 최소 문자 수를 6으로 지정합니다.

```
ciscoasa(config)# password-policy minimum-changes 6
```

관련 명령

명령	설명
password-policy lifetime	비밀번호가 만료된 이후의 비밀번호 수명(일)을 설정합니다.
password-policy minimum-length	비밀번호의 최소 길이를 설정합니다.
password-policy minimum-lowercase	비밀번호에 포함해야 할 소문자의 최소 개수를 설정합니다.

password-policy minimum-length

비밀번호의 최소 길이를 설정하려면 글로벌 컨피그레이션 모드에서 **password-policy minimum-length** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy minimum-length *value*

no password-policy minimum-length *value*

구문 설명

value	비밀번호의 최소 길이를 지정합니다. 유효한 값의 범위는 0~64자입니다.

기본값

기본 최소 길이는 0입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

최소 길이가 다른 최소 특성(변경, 소문자, 대문자, 숫자, 특수 문자) 중 하나보다 작으면 오류 메시지가 표시되고 최소 길이가 변경되지 않습니다. 권장되는 비밀번호 길이는 8자입니다.

예

다음 예는 비밀번호의 최소 문자 수를 8로 지정합니다.

```
ciscoasa(config)# password-policy minimum-length 8
```

관련 명령

명령	설명
password-policy lifetime	비밀번호가 만료된 이후의 비밀번호 수명 값(일)을 설정합니다.
password-policy minimum-changes	이전 비밀번호와 새 비밀번호 간에 허용되는 최소 변경 문자 수를 설정합니다.
password-policy minimum-lowercase	비밀번호에 포함해야 할 소문자의 최소 개수를 설정합니다.

password-policy minimum-lowercase

비밀번호에 포함해야 할 소문자의 최소 개수를 설정하려면 글로벌 컨피그레이션 모드에서 **password-policy minimum-lowercase** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy minimum-lowercase *value*

no password-policy minimum-lowercase *value*

구문 설명

value	비밀번호에 포함해야 할 소문자의 최소 개수를 지정합니다. 유효한 값의 범위는 0~64자입니다.

기본값

최소 소문자의 기본 개수는 0입니다. 즉 최소 개수 제한이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 비밀번호에 포함해야 할 소문자의 최소 개수를 설정합니다. 유효한 값의 범위는 0~64자입니다.

예

다음 예는 비밀번호에 포함해야 할 소문자의 최소 개수를 6으로 지정합니다.

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

관련 명령

명령	설명
password-policy lifetime	비밀번호가 만료된 이후의 비밀번호 수명 값(일)을 설정합니다.
password-policy minimum-changes	새 비밀번호와 기존 비밀번호 간에 변경해야 할 최소 문자 수를 설정합니다.
password-policy minimum-length	비밀번호의 최소 길이를 설정합니다.

password-policy minimum-numeric

비밀번호에 포함해야 할 숫자의 최소 개수를 설정하려면 글로벌 컨피그레이션 모드에서 **password-policy minimum-numeric** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy minimum-numeric *value*

no password-policy minimum-numeric *value*

구문 설명

value	비밀번호에 포함해야 할 숫자의 최소 개수를 지정합니다. 유효한 값의 범위는 0~64자입니다.

기본값

최소 숫자의 기본 개수는 0입니다. 즉 최소 개수 제한이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 비밀번호에 포함해야 할 숫자의 최소 개수를 설정합니다. 유효한 값의 범위는 0~64자입니다.

예

다음 예는 비밀번호에 포함해야 할 숫자의 최소 개수를 8로 지정합니다.

```
ciscoasa(config)# password-policy minimum-numeric 8
```

관련 명령

명령	설명
password-policy lifetime	비밀번호가 만료된 이후의 비밀번호 수명 값(일)을 설정합니다.
password-policy minimum-changes	새 비밀번호와 기존 비밀번호 간에 변경해야 할 최소 문자 수를 설정합니다.
password-policy minimum-length	비밀번호의 최소 길이를 설정합니다.

password-policy minimum-special

비밀번호에 포함해야 할 특수 문자의 최소 개수를 설정하려면 글로벌 컨피그레이션 모드에서 **password-policy minimum-special** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy minimum-special *value*

no password-policy minimum-special *value*

구문 설명

value	비밀번호에 포함해야 할 특수 문자의 최소 개수를 지정합니다. 유효한 값의 범위는 0~64자입니다.

기본값

최소 특수 문자의 기본 개수는 0입니다. 즉 최소 개수 제한이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 비밀번호에 포함해야 할 특수 문자의 최소 개수를 설정합니다. 특수 문자에는 !, @, #, $, %, ^, &, *, '(' 및 ')'가 포함됩니다.

예

다음 예는 비밀번호에 포함해야 할 특수 문자의 최소 개수를 2로 지정합니다.

```
ciscoasa(config)# password-policy minimum-special 2
```

관련 명령

명령	설명
password-policy lifetime	비밀번호가 만료된 이후의 비밀번호 수명 값(일)을 설정합니다.
password-policy minimum-changes	새 비밀번호와 기존 비밀번호 간에 변경해야 할 최소 문자 수를 설정합니다.
password-policy minimum-length	비밀번호의 최소 길이를 설정합니다.

password-policy minimum-uppercase

비밀번호에 포함해야 할 대문자의 최소 개수를 설정하려면 글로벌 컨피그레이션 모드에서 **password-policy minimum-uppercase** 명령을 사용합니다. 해당 비밀번호 정책 특성을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

password-policy minimum-uppercase *value*

no password-policy minimum-uppercase *value*

구문 설명

value	비밀번호에 포함해야 할 대문자의 최소 개수를 지정합니다. 유효한 값의 범위는 0~64자입니다.

기본값

최소 대문자의 기본 개수는 0입니다. 즉 최소 개수 제한이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 비밀번호에 포함해야 할 대문자의 최소 개수를 설정합니다. 유효한 값의 범위는 0~64자입니다.

예

다음 예는 비밀번호에 포함해야 할 대문자의 최소 개수를 4로 지정합니다.

```
ciscoasa(config)# password-policy minimum-uppercase 4
```

관련 명령

명령	설명
password-policy lifetime	비밀번호가 만료된 이후의 비밀번호 수명 값(일)을 설정합니다.
password-policy minimum-changes	새 비밀번호와 기존 비밀번호 간에 변경해야 할 최소 문자 수를 설정합니다.
password-policy minimum-length	비밀번호의 최소 길이를 설정합니다.

password-prompt

WebVPN 사용자가 보안 어플라이언스에 연결할 때 표시되는 WebVPN 페이지 로그인 상자의 비밀번호 프롬프트를 사용자 지정하려면 webvpn 사용자 지정 모드에서 **password-prompt** 명령을 사용합니다.

password-prompt {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

컨피그레이션에서 명령을 제거하고 값이 상속되도록 하려면 이 명령의 **no** 형식을 사용합니다.

구문 설명

text	텍스트 변경을 지정합니다.
style	스타일 변경을 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자).

기본값

비밀번호 프롬프트의 기본 텍스트는 "PASSWORD:"입니다.

비밀번호 프롬프트의 기본 스타일은 color:black;font-weight:bold;text-align:right입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 사용자 지정	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 CSS(Cascading Style Sheet) 매개변수로서 표현됩니다. 이러한 매개변수에 대해 설명하는 것은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트 www.w3.org에서 제공하는 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수의 편리한 목록이 포함되어 있습니다.

WebVPN 페이지에 대한 가장 일반적인 변경 사항, 즉 페이지 색상과 관련된 몇 가지 팁은 다음과 같습니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값, 색상의 이름(HTML에서 인식되는 경우) 등을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며 각 색상은 0~255 범위의 십진수입니다. 쉼표로 구분된 엔트리는 다른 색상과 결합되는 각 색상의 강도 수준을 나타냅니다.
- HTML 형식은 #000000으로서, 여섯 자리 16진수 형식으로 되어 있습니다. 첫 번째와 두 번째는 빨강, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파랑을 나타냅니다.

참고 WebVPN 페이지를 손쉽게 사용자 지정하려면 색상 조각, 미리 보기 기능 등의 스타일 요소를 구성하기 위한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예에서 텍스트는 "Corporate Password:"로 변경되고, 기본 스타일은 글꼴 두께가 더 굵게 변경됩니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# password-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# password-prompt style font-weight:bolder
```

관련 명령

명령	설명
group-prompt	WebVPN 페이지의 그룹 프롬프트를 사용자 지정합니다.
username-prompt	WebVPN 페이지의 사용자 이름 프롬프트를 사용자 지정합니다.

password-storage

사용자가 클라이언트 시스템에 로그인 비밀번호를 저장하도록 하려면 그룹 정책 컨피그레이션 모드 또는 사용자 이름 컨피그레이션 모드에서 **password-storage enable** 명령을 사용합니다. 비밀번호 저장을 비활성화하려면 **password-storage disable** 명령을 사용합니다.

실행 중인 컨피그레이션에서 password-storage 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 경우 다른 그룹 정책으로부터 password-storage의 값을 상속하는 것이 허용됩니다.

password-storage {enable | disable}

no password-storage

구문 설명

disable	비밀번호 저장을 비활성화합니다.
enable	비밀번호 저장을 활성화합니다.

기본값

비밀번호 저장이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

비밀번호 저장 기능은 안전이 보장되는 사이트의 시스템에서만 이용하십시오.

이 명령은 대화형 하드웨어 클라이언트 인증 또는 하드웨어 클라이언트를 위한 개별 사용자 인증과 전혀 관련이 없습니다.

예

다음 예는 그룹 정책 FirstGroup에 대해 비밀번호 스토리지를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# password-storage enable
```

peer-id-validate

피어의 인증서를 사용하여 피어의 ID를 검증할지 여부를 지정하려면 tunnel-group ipsec-attributes 모드에서 **peer-id-validate** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

peer-id-validate *option*

no peer-id-validate

구문 설명

option	다음 옵션 중 하나를 지정합니다. • **req**: 필수 • **cert**: 인증서에서 지원되는 경우 • **nocheck**: 검사하지 않음

기본값

이 명령의 기본 설정은 **req**입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group ipsec attributes	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

모든 IPsec tunnel-group 유형에 이 특성을 적용할 수 있습니다.

예

컨피그레이션 모드에서 다음 예를 입력하는 경우 IPsec LAN-to-LAN 터널 그룹인 209.165.200.225에 대한 피어 인증서의 ID를 사용하여 피어를 검증해야 합니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPsec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# peer-id-validate req
ciscoasa(config-tunnel-ipsec)#
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 컨피그레이션을 보여줍니다.
tunnel-group ipsec-attributes	이 그룹에 대한 터널 그룹 IPsec 특성을 구성합니다.

perfmon

성능 정보를 표시하려면 특별 권한 EXEC 모드에서 **perfmon** 명령을 사용합니다.

perfmon {verbose | interval *seconds* **| quiet | settings} [***detail***]

구문 설명

verbose	ASA 콘솔에 성능 모니터 정보를 표시합니다.
interval *seconds*	콘솔에서 성능 표시를 새로 고치기까지의 시간(초)을 지정합니다.
quiet	성능 모니터 표시를 비활성화합니다.
settings	간격과 quiet 또는 verbose 여부를 표시합니다.
detail	성능에 대한 상세 정보를 표시합니다.

기본값

*seconds*는 120초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0	이 명령에 대한 지원이 ASA에 추가되었습니다.
7.2(1)	**detail** 키워드에 대한 지원이 추가되었습니다.

사용 지침

perfmon 명령을 사용하면 ASA의 성능을 모니터링할 수 있습니다. 정보를 즉시 표시하려면 **show perfmon** 명령을 사용합니다. 정보를 2분마다 계속해서 표시하려면 **perfmon verbose** 명령을 사용합니다. 정보를 지정한 간격으로 계속해서 표시하려면 **perfmon interval** *seconds* 명령과 **perfmon verbose** 명령을 함께 사용합니다.

성능 정보를 표시하는 예는 다음과 같습니다.

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s
FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s

PERFMON STATS:	Current	Average
AAA Author	9/s	5/s
AAA Account	3/s	3/s

이 정보는 1초마다 발생하는 변환, 연결, Websense 요청, 주소 변환("fixups"), AAA 변환의 수를 나열합니다.

예

다음 예는 ASA 콘솔에서 성능 모니터 통계를 30초마다 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# perfmon interval 120
ciscoasa(config)# perfmon quiet
ciscoasa(config)# perfmon settings
interval: 120 (seconds)
quiet
```

관련 명령

명령	설명
show perfmon	성능 정보를 표시합니다.

periodic

time-range 기능을 지원하는 함수의 반복(매주) 시간 범위를 지정하려면 time-range 컨피그레이션 모드에서 **periodic** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

구문 설명

days-of-the-week	(선택 사항) 이 인수의 첫 번째 표시는 관련 시간 범위가 적용되는 시작 요일을 나타냅니다. 두 번째 표시는 관련 명령문이 적용되는 종료 요일을 나타냅니다. 이 인수는 Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday 중 하나의 요일이거나 여러 요일의 조합입니다. 기타 가능한 값은 다음과 같습니다. • daily - 월요일~일요일 • weekdays - 월요일~금요일 • weekend - 토요일 및 일요일 주의 종료 요일이 시작 요일과 같으면 생략할 수 있습니다.
time	HH:MM 형식으로 시간을 지정합니다. 예를 들어, 8:00은 오전 8:00입니다. 그리고 20:00은 오후 8:00입니다.
to	"from start-time to end-time" 범위를 완료하려면 **to** 키워드를 입력해야 합니다.

기본값

periodic 명령으로 값을 입력하지 않으면 **time-range** 명령으로 정의한 대로 ASA에 대한 액세스가 즉시 적용되고 항상 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Time-range 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

시간 기준 ACL를 구현하려면 **time-range** 명령을 사용하여 구체적인 요일과 시간대를 정의합니다. 그런 다음 **access-list extended time-range** 명령을 사용하여 시간 범위를 ACL에 바인딩합니다.

periodic 명령은 시간 범위의 적용 시기를 지정하는 한 방법입니다. 또 다른 방법은 **absolute** 명령으로 절대 기간을 지정하는 것입니다. 시간 범위의 이름을 지정하는 **time-range** 글로벌 컨피그레이션 명령 이후에 이 두 명령 중 하나를 사용합니다. **time-range** 명령 이후 **periodic** 명령을 여러 번 사용할 수 있습니다.

종료 days-of-the-week 값이 시작 값과 동일하면 생략할 수 있습니다.

time-range 명령에 **absolute** 및 **periodic** 값이 모두 지정된 경우, **periodic** 명령은 **absolute start** 시간에 도달한 이후에야 평가되며 **absolute end** 시간에 도달하면 더 이상 평가되지 않습니다.

time-range 기능은 ASA의 시스템 클록에 의존하지만, NTP 동기화의 경우 가장 잘 작동합니다.

예

다음은 몇 가지 예입니다.

필요 기간:	다음 입력:
월요일~금요일, 오전 8:00~오후 6:00 동안에만	**periodic weekdays 8:00 to 18:00**
주중 매일, 오전 8:00~오후 6:00 동안에만	**periodic daily 8:00 to 18:00**
월요일 오전 8:00~금요일 오후 8:00, 매분	**periodic monday 8:00 to friday 20:00**
주말 내내, 토요일 아침~일요일 밤	**periodic weekend 00:00 to 23:59**
매주 토요일과 일요일, 정오에서 자정까지	**periodic weekend 12:00 to 23:59**

다음 예는 월요일에서 금요일까지 오전 8:00~오후 6:00 동안에만 ASA에 대한 액세스를 허용하는 방법을 보여줍니다.

```
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
ciscoasa(config-time-range)#
```

다음 예는 특정 요일(월, 화, 금)에 오전 10:30~오후 12:30 동안 ASA에 대한 액세스를 허용하는 방법을 보여줍니다.

```
ciscoasa(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
ciscoasa(config-time-range)#
```

관련 명령

명령	설명
absolute	시간 범위가 적용될 때 절대 시간을 정의합니다.
access-list extended	IP 트래픽의 ASA 통과를 허용하거나 거부하기 위한 정책을 구성합니다.
default	**time-range** 명령 **absolute** 및 **periodic** 키워드의 기본 설정을 복원합니다.
time-range	시간을 기반으로 ASA에 대한 액세스 제어를 정의합니다.

permit errors

유효하지 않은 GTP 패킷 또는 구문 분석에 실패하여 삭제될 수 있는 패킷을 허용하려면, **gtp-map** 명령을 사용하여 액세스할 수 있는 GTP 맵 컨피그레이션 모드에서 **permit errors** 명령을 사용합니다. 모든 유효하지 않은 패킷 또는 구문 분석에 실패한 패킷을 삭제하는 기본 동작으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

permit errors

no permit errors

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본적으로 모든 유효하지 않은 패킷 또는 구문 분석에 실패한 패킷은 삭제됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
GTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

유효하지 않은 패킷 또는 ASA를 통해 전송되는 메시지 검사 도중 오류가 발생한 패킷을 삭제하는 대신 허용하려면 GTP 맵 컨피그레이션 모드에서 **permit errors** 명령을 사용합니다.

예

다음 예는 유효하지 않은 패킷 또는 구문 분석 중 실패한 패킷을 포함하는 트래픽을 허용합니다.

```
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# permit errors
```

관련 명령

명령	설명
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
gtp-map	GTP 맵을 정의하고 GTP 맵 컨피그레이션 모드를 활성화합니다.
inspect gtp	애플리케이션 검사에 사용할 특정 GTP 맵을 적용합니다.
permit response	로드 밸런싱 GSN를 지원합니다.
show service-policy inspect gtp	GTP 컨피그레이션을 표시합니다.

permit response

로드 밸런싱 GSN를 지원하려면, **gtp-map** 명령을 사용하여 액세스할 수 있는 GTP 맵 컨피그레이션 모드에서 **permit response** 명령을 사용합니다. 요청이 전송된 호스트 이외의 GSN에서 오는 GTP 응답을 ASA에서 삭제하도록 허용하려면 이 명령의 **no** 형식을 사용합니다.

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

구문 설명

from-object-group *from_obj_group_id*	*to_obj_group_id* 인수로 지정한 객체 그룹의 GSN 집합에 응답을 보낼 수 있는 **object-group** 명령으로 구성된 객체 그룹의 이름을 지정합니다. ASA는 IPv4 주소의 네트워크 객체가 포함된 객체 그룹만 지원합니다. IPv6 주소는 현재 GTP에서 지원되지 않습니다.
to-object-group *to_obj_group_id*	*from_obj_group_id* 인수로 지정한 객체 그룹의 GSN 집합으로부터 응답을 받을 수 있는 **object-group** 명령으로 구성된 객체 그룹의 이름을 지정합니다. ASA는 IPv4 주소의 네트워크 객체가 포함된 객체 그룹만 지원합니다. IPv6 주소는 현재 GTP에서 지원되지 않습니다.

기본값

기본적으로 ASA는 요청이 전송된 호스트 이외의 GSN에서 오는 GTP 응답을 삭제합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
GTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.04	이 명령이 추가되었습니다.

사용 지침

로드 밸런싱 GSN을 지원하려면 GTP 맵 컨피그레이션 모드에서 **permit response** 명령을 사용합니다. **permit response** 명령은 응답이 전송된 GSN이 아닌 다른 GSN에서 오는 GTP 응답을 허용하도록 GTP 맵을 구성합니다.

로드 밸런싱 GSN의 풀을 네트워크 객체로서 식별합니다. 마찬가지로 SGSN을 네트워크 객체로서 식별합니다. GSN 응답이 GTP 요청을 전송한 GSN과 동일한 객체 그룹에 속하는 경우, 그리고 응답하는 GSN이 GTP 응답을 보내도록 허용된 객체 그룹에 SGSN이 속해 있는 경우 ASA에서는 응답을 허용합니다.

예

다음 예는 192.168.32.0 네트워크의 호스트에서 IP 주소 192.168.112.57의 호스트로 전송되는 GTP 응답을 허용합니다.

```
ciscoasa(config)# object-group network gsnpool32
ciscoasa(config-network)# network-object 192.168.32.0 255.255.255.0
ciscoasa(config)# object-group network sgsn1
ciscoasa(config-network)# network-object host 192.168.112.57
ciscoasa(config-network)# exit
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# permit response to-object-group sgsn1 from-object-group gsnpool32
```

관련 명령

명령	설명
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
gtp-map	GTP 맵을 정의하고 GTP 맵 컨피그레이션 모드를 활성화합니다.
inspect gtp	애플리케이션 검사에 사용할 특정 GTP 맵을 적용합니다.
permit errors	유효하지 않은 GTP 패킷을 허용합니다.
show service-policy inspect gtp	GTP 컨피그레이션을 표시합니다.

pfs

PFS를 활성화하려면 그룹 정책 컨피그레이션 모드에서 **pfs enable** 명령을 사용합니다. PFS을 비활성화하려면 **pfs disable** 명령을 사용합니다. 실행 중인 컨피그레이션에서 PFS 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

pfs {enable | disable}

no pfs

구문 설명

disable	PFS를 비활성화합니다.
enable	PFS를 활성화합니다.

기본값

PFS가 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

VPN 클라이언트 및 ASA의 PFS 설정은 일치해야 합니다.

다른 그룹 정책에서 PFS의 값을 상속하도록 허용하려면 이 명령의 **no** 형식을 사용하십시오.

IPsec 협상에서 PFS는 각각의 새로운 암호화 키가 이전 키와 관련이 없는지를 확인합니다.

예

다음 예는 그룹 정책 FirstGroup에 대해 PFS을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# pfs enable
```

phone-proxy

전화 프록시 인스턴스를 구성하려면 글로벌 컨피그레이션 모드에서 **phone-proxy** 명령을 사용합니다.

전화 프록시 인스턴스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

phone-proxy *phone_proxy_name*

no phone-proxy *phone_proxy_name*

구문 설명

phone_proxy_name	전화 프록시 인스턴스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(4)	이 명령이 추가되었습니다.

사용 지침

ASA에서는 전화 프록시 인스턴스를 하나만 구성할 수 있습니다.

HTTP 프록시 서버에 대해 NAT를 구성하면 IP Phone과 관련된 HTTP 프록시 서버의 전역 또는 매핑된 IP 주소가 전화 프록시 컨피그레이션 파일에 기록됩니다.

예

다음 예는 **phone-proxy** 명령을 사용하여 전화 프록시 인스턴스를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.0.2.25 interface inside
ciscoasa(config-phone-proxy)# media-termination address 128.106.254.3 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa(config-phone-proxy)# ctl-file asactl
ciscoasa(config-phone-proxy)# cluster-mode nonsecure
ciscoasa(config-phone-proxy)# timeout secure-phones 00:05:00
ciscoasa(config-phone-proxy)# disable service-settings
```

관련 명령

명령	설명
ctl-file (global)	전화 프록시 컨피그레이션을 만들기 위한 CTL 파일 또는 플래시 메모리에서 구문 분석하기 위한 CTL 파일을 지정합니다.
ctl-file (phone-proxy)	전화 프록시 컨피그레이션에 사용할 CTL 파일을 지정합니다.
tls-proxy	TLS 프록시 인스턴스를 구성합니다.

pim

인터페이스에서 PIM을 다시 활성화하려면 인터페이스 컨피그레이션 모드에서 **pim** 명령을 사용합니다. PIM을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

pim

no pim

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

multicast-routing 명령은 기본적으로 모든 인터페이스에서 PIM을 활성화합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

multicast-routing 명령은 기본적으로 모든 인터페이스에서 PIM을 활성화합니다. 컨피그레이션에서는 **pim** 명령의 **no** 형식만 저장됩니다.

참고 PIM은 PAT에서 지원되지 않습니다. PIM 프로토콜은 포트를 사용하지 않고 PAT는 포트를 사용하는 프로토콜에서만 작동합니다.

예

다음 예는 선택한 인터페이스에서 PIM을 비활성화합니다.

```
ciscoasa(config-if)# no pim
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim accept-register

PIM 레지스터 메시지를 필터링하도록 ASA를 구성하려면 글로벌 컨피그레이션 모드에서 **pim accept-register** 명령을 사용합니다. 필터링을 제거하려면 이 명령의 **no** 형식을 사용합니다.

pim accept-register {**list** *acl* | **route-map** *map-name*}

no pim accept-register

구문 설명

list *acl*	액세스 목록 이름 또는 번호를 지정합니다. 이 명령으로는 확장 호스트 ACL만 사용하십시오.
route-map *map-name*	경로 맵 이름을 지정합니다. 참조된 경로 맵에서는 확장 호스트 ACL을 사용하십시오.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 권한이 없는 소스가 RP로 등록되는 것을 막기 위해 사용됩니다. 권한이 없는 소스가 RP에 레지스터 메시지를 전송하면 ASA는 즉시 register-stop 메시지를 다시 전송합니다.

예

다음 예는 PIM 레지스터 메시지를 "no-ssm-range"라는 액세스 목록에 정의된 소스에서 오는 것으로 제한합니다.

```
ciscoasa(config)# pim accept-register list no-ssm-range
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim bidir-neighbor-filter

DF 선택에 참가할 수 있는 bidir 지원 인접 디바이스를 제어하려면 인터페이스 컨피그레이션 모드에서 **pim bidir-neighbor-filter** 명령을 사용합니다. 필터링을 제거하려면 이 명령의 **no** 형식을 사용합니다.

pim bidir-neighbor-filter *acl*

no pim bidir-neighbor-filter *acl*

구문 설명

acl	액세스 목록 이름 또는 번호를 지정합니다. 액세스 목록은 bidir DF 선택에 참가할 수 있는 인접 디바이스를 정의합니다. 이 명령에서는 표준 ACL만 사용하십시오. 확장 ACL은 지원되지 않습니다.

기본값

모든 라우터는 bidir을 지원하는 것으로 간주됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

양방향 PIM은 멀티캐스트 라우터가 축소된 상태 정보를 유지할 수 있게 합니다. 세그먼트의 모든 멀티캐스트 라우터가 bidir에 대해 양방향으로 활성화되어 있어야 DF를 선택할 수 있습니다.

pim bidir-neighbor-filter 명령은 DF 선택에 참여할 라우터 지정을 허용하는 동시에 모든 라우터가 sparse-mode 도메인에 참여할 수 있게 함으로써 sparse-mode-only 네트워크에서 bidir 네트워크로의 전환을 가능하게 합니다. bidir-enabled 라우터는 bidir 라우터가 세그먼트에 없어도 자기들 끼리 DF를 선택할 수 있습니다. non-bidir 라우터의 멀티캐스트 경계는 bidir 그룹의 PIM 메시지 및 데이터가 bidir 그룹이나 bidir 서브셋 클라우드에서 유출되지 않도록 합니다.

pim bidir-neighbor-filter 명령이 활성화된 경우 ACL에 의해 허용된 라우터는 양방향을 지원하는 것으로 간주됩니다. 따라서:

- 허용된 인접 디바이스가 bidir을 지원하지 않을 경우 DF 선택이 일어나지 않습니다.
- 거부된 인접 디바이스가 bidir을 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 인접 디바이스가 bidir을 지원하지 않을 경우 DF 선택이 일어날 수 있습니다.

예

다음 예는 10.1.1.1이 PIM bidir 인접 디바이스가 되도록 허용합니다.

```
ciscoasa(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list bidir_test deny any
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidir-neighbor-filter bidir_test
```

관련 명령

명령	설명
multicast boundary	관리적으로 범위가 지정된 멀티캐스트 주소에 대한 멀티캐스트 경계를 정의합니다.
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim dr-priority

전용 라우터 선택에 사용되는 ASA에서 인접 디바이스 우선순위를 구성하려면 인터페이스 컨피그레이션 모드에서 **pim dr-priority** 명령을 사용합니다. 기본 우선순위를 복원하려면 이 명령의 **no** 형식을 사용합니다.

pim dr-priority *number*

no pim dr-priority

구문 설명

number	0~4294967294의 숫자입니다. 이 번호는 전용 라우터를 결정할 때 디바이스의 우선순위를 확인하는 데 사용됩니다. 0을 지정하면 ASA는 전용 라우터가 되지 못합니다.

기본값

기본값은 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 우선순위 값이 가장 큰 디바이스가 PIM 전용 라우터가 됩니다. 여러 디바이스의 DR(전용 라우터) 우선순위가 동일한 경우 IP 주소가 가장 높은 디바이스가 DR이 됩니다. Hello 메시지에 DR-Priority 옵션이 포함되어 있지 않은 디바이스는 우선순위가 가장 높은 디바이스로 간주되어 전용 라우터가 됩니다. Hello 메시지에 이 옵션이 포함되지 않은 디바이스가 여러 개인 경우 IP 주소가 가장 높은 디바이스가 전용 라우터가 됩니다.

예

다음 예는 인터페이스의 DR 우선순위를 5로 설정합니다.

```
ciscoasa(config-if)# pim dr-priority 5
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim hello-interval

PIM hello 메시지의 빈도를 구성하려면 인터페이스 컨피그레이션 모드에서 **pim hello-interval** 명령을 사용합니다. Hello 간격을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

구문 설명

seconds	Hello 메시지를 보내기까지 ASA에서 대기하는 시간(초)입니다. 유효한 값의 범위는 1~3600초입니다. 기본값은 30입니다.

기본값

간격 기본값은 30초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 PIM hello 간격을 1분으로 변경합니다.

```
ciscoasa(config-if)# pim hello-interval 60
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim join-prune-interval

PIM join/prune 간격을 구성하려면 인터페이스 컨피그레이션 모드에서 **pim join-prune-interval** 명령을 사용합니다. 간격을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

구문 설명

seconds	join/prune 메시지를 보내기까지 ASA에서 대기하는 시간(초)입니다. 유효한 값의 범위는 10~600초입니다. 60초가 기본값입니다.

기본값

기본 간격은 60초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 PIM join/prune 간격을 2분으로 변경합니다.

```
ciscoasa(config-if)# pim join-prune-interval 120
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim neighbor-filter

PIM에 참가할 인접 라우터를 제어하려면 인터페이스 컨피그레이션 모드에서 **pim neighbor-filter** 명령을 사용합니다. 필터링을 제거하려면 이 명령의 **no** 형식을 사용합니다.

pim neighbor-filter *acl*

no pim neighbor-filter *acl*

구문 설명

acl	액세스 목록 이름 또는 번호를 지정합니다. 이 명령에서는 표준 ACL만 사용하십시오. 확장 ACL은 지원되지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

다음 명령은 PIM에 참가할 수 있는 인접 라우터를 정의합니다. 컨피그레이션에 이 명령이 없으면 제한이 없는 것입니다.

컨피그레이션에 이 명령이 나타나려면 멀티캐스트 라우팅과 PIM이 활성화되어 있어야 합니다. 멀티캐스트 라우팅을 비활성화하면 이 명령이 컨피그레이션에서 제거됩니다.

예

다음 예는 IP 주소 10.1.1.1의 라우터가 인터페이스 GigabitEthernet0/2에서 PIM 인접 디바이스가 되도록 허용합니다.

```
ciscoasa(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list pim_filter deny any
ciscoasa(config)# interface gigabitEthernet0/2
ciscoasa(config-if)# pim neighbor-filter pim_filter
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim old-register-checksum

이전 레지스터 체크섬 방법론을 사용하는 RP(Rendezvous Point)에서 이전 버전과의 호환성을 허용하려면 글로벌 컨피그레이션 모드에서 **pim old-register-checksum** 명령을 사용합니다. PIM RFC 규격 레지스터를 생성하려면 이 명령의 **no** 형식을 사용합니다.

pim old-register-checksum

no pim old-register-checksum

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

ASA는 PIM RFC 규격 레지스터를 생성합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA 소프트웨어는 모든 PIM 메시지 유형에 대해 전체 PIM 메시지로 레지스터 메시지를 허용하는 Cisco IOS 방법을 사용하는 대신, PIM 헤더의 체크섬과 다음 4바이트만으로 레지스터 메시지를 허용합니다. **pim old-register-checksum** 명령은 Cisco IOS 소프트웨어와 호환되는 레지스터를 생성합니다.

예

다음 예는 이전 체크섬 계산을 사용하도록 ASA를 구성합니다.

```
ciscoasa(config)# pim old-register-checksum
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

pim rp-address

PIM RP(Rendezvous Point)의 주소를 구성하려면 글로벌 컨피그레이션 모드에서 **pim rp-address** 명령을 사용합니다. RP 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

pim rp-address *ip_address* [*acl*] [**bidir**]

no pim rp-address *ip_address*

구문 설명

acl	(선택 사항) RP를 사용해야 할 멀티캐스트 그룹을 정의하는 표준 액세스 목록의 이름 또는 번호입니다. 호스트 ACL을 이 명령과 함께 사용하지 마십시오.
bidir	(선택 사항) 지정된 멀티캐스트 그룹이 양방향 모드에서 작동함을 나타냅니다. 이 옵션 없이 명령을 구성하면 지정된 그룹은 PIM sparse mode에서 작동합니다.
ip_address	PIM RP가 될 라우터의 IP 주소입니다. 점으로 구분된 4개의 십진수로 표기되는 유니캐스트 IP 주소입니다.

기본값

PIM RP 주소가 구성되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

일반 PIM sparse mode(PIM-SM) 또는 bidir 도메인 내의 모든 라우터는 잘 알려진 PIM RP 주소를 알고 있어야 합니다. 주소는 이 명령을 사용하여 고정으로 구성됩니다.

참고 ASA는 Auto-RP를 지원하지 않으므로, RP 주소를 지정하려면 **pim rp-address** 명령을 사용해야 합니다.

두 개 이상의 그룹에 대해 단일 RP를 구성할 수 있습니다. 액세스 목록에 지정된 그룹 범위가 PIM RP 그룹 매핑을 결정합니다. 액세스 목록이 지정되지 않은 경우 그룹에 대한 RP가 전체 IP 멀티캐스트 그룹 범위(224.0.0.0/4)에 적용됩니다.

참고 실제 bidir 컨피그레이션과 관계없이 ASA는 PIM hello 메시지에서 항상 bidir 기능을 광고합니다.

예

다음 예는 모든 멀티캐스트 그룹에 대해 PIM RP 주소를 10.0.0.1로 설정합니다.

```
ciscoasa(config)# pim rp-address 10.0.0.1
```

관련 명령

명령	설명
pim accept-register	PIM 레지스터 메시지를 필터링할 후보 RP를 구성합니다.

pim spt-threshold infinity

항상 공유 트리를 사용하고 SPT(최단 경로 트리) 전환을 사용하지 않도록 마지막 홉(hop) 라우터의 동작을 변경하려면 글로벌 컨피그레이션 모드에서 **pim spt-threshold infinity** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

pim spt-threshold infinity [**group-list** *acl*]

no pim spt-threshold

구문 설명

group-list *acl*	(선택 사항) 액세스 목록에 의해 제한되는 소스 그룹을 나타냅니다. *acl* 인수는 표준 ACL을 지정해야 합니다. 확장 ACL은 지원되지 않습니다.

기본값

마지막 홉(hop) PIM 라우터는 기본적으로 최단 경로 소스 트리로 전환됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

group-list 키워드를 사용하지 않으면 이 명령은 모든 멀티캐스트 그룹에 적용됩니다.

예

다음 예에서는 마지막 홉(hop) PIM 라우터가 최단 경로 소스 트리로 전환되는 대신 항상 공유 트리를 사용합니다.

```
ciscoasa(config)# pim spt-threshold infinity
```

관련 명령

명령	설명
multicast-routing	ASA에서 멀티캐스트 라우팅을 활성화합니다.

ping

지정된 인터페이스에서 IP 주소로의 연결을 테스트하려면 특별 권한 EXEC 모드에서 **ping** 명령을 사용합니다. 사용 가능한 매개변수는 일반 ICMP 기반 ping과 TCP ping에서 서로 다릅니다. 매개변수로서 사용할 수 없는 특성을 비롯하여 값을 입력하도록 프롬프트를 표시하려면 매개변수 없이 명령을 입력하십시오.

ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

ping tcp [*if_name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]

ping

참고 **source** 및 *port* 옵션은 **tcp** 옵션을 사용하는 경우에만 사용할 수 있습니다. **data**, **size** 및 **validate** 옵션은 **tcp** 옵션과 함께 사용할 수 없습니다.

구문 설명

data *pattern*	(선택 사항, ICMP 전용) 16진수 형식으로 16비트 데이터 패턴을 지정합니다(범위 0~FFFF). 기본값은 0xabcd입니다.
host	ping할 호스트의 이름 또는 IPv4 주소를 지정합니다. ICMP ping의 경우 IPv6 주소를 지정할 수 있습니다(TCP ping에서는 지원되지 않음). 호스트 이름 사용 시, DNS 이름 또는 **name** 명령으로 할당되는 이름을 사용할 수 있습니다. DNS 이름의 최대 문자 수는 128자이며, **name** 명령으로 생성하는 이름의 최대 문자 수는 63자입니다. DNS 이름을 사용하려면 DNS 서버를 구성해야 합니다.
if_name	(선택 사항) ICMP의 경우, **nameif** 명령으로 구성되며 *host*에서 액세스할 수 있는 인터페이스 이름입니다. 제공하지 않는 경우 *host*는 IP 주소로 변경되며, 수신 인터페이스를 확인하기 위해 라우팅 테이블을 참조하게 됩니다. TCP의 경우, 소스에서 SYN 패킷을 전송하는 입력 인터페이스입니다.
port	(TCP 전용) ping하는 호스트의 TCP 포트 번호를 지정합니다(1~65535).
repeat *count*	(선택 사항) ping 요청을 반복할 횟수를 지정합니다. 기본값은 5입니다.
size *bytes*	(선택 사항, ICMP 전용) 데이터그램 크기를 바이트 단위로 지정합니다. 기본값은 100입니다.
source *host port*	(선택 사항, TCP 전용) ping을 보낼 특정 IP 주소 및 포트를 지정합니다(무작위 포트에는 port = 0 사용).
tcp	(선택 사항) TCP를 통한 연결을 테스트합니다(기본값은 ICMP). TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다. 한 번에 최대 2개의 동시 TCP ping을 실행할 수 있습니다.
timeout *seconds*	(선택 사항) 시간 제한 간격을 초 단위로 지정합니다. 기본값은 2초입니다.
validate	(선택 사항, ICMP 전용) 응답 데이터를 검증합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

명령 모드	방화벽 모드		보안 컨텍스트		
	라우팅	투명성	단일	다중 컨텍스트	다중 시스템
특별 권한 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	DNS 이름 지원이 추가되었습니다.
8.4(1)	**tcp** 옵션이 추가되었습니다.

사용 지침

ping 명령을 사용하면 ASA에 연결이 있는지 또는 호스트를 네트워크에서 사용할 수 있는지 확인할 수 있습니다.

일반 ICMP 기반 ping을 사용하는 경우 이러한 패킷을 차단하는 **icmp** 규칙이 없는지 확인해야 합니다(ICMP 규칙을 사용하지 않는 경우 모든 ICMP 트래픽이 허용됨). 내부 호스트가 ICMP를 통해 외부 호스트에 ping하도록 하려면 다음 중 하나를 수행해야 합니다.

- 에코 응답에 대해 ICMP **access-list** 명령을 만듭니다. 예를 들어 모든 호스트에 ping 액세스를 제공하려면 **access-list acl_grp permit icmp any any** 명령을 사용하고, **access-list** 명령을 **access-group** 명령으로 테스트할 인터페이스에 연결합니다.
- **inspect icmp** 명령을 사용하여 ICMP 검사 엔진을 구성합니다. 예를 들어 **inspect icmp** 명령을 전역 서비스 정책용 **class default_inspection** 클래스에 추가하면 내부 호스트에서 시작된 에코 요청에 대해 에코 응답이 ASA를 통과할 수 있습니다.

TCP ping을 사용할 경우, 액세스 정책이 지정된 포트에서 TCP 트래픽을 허용하는지 확인해야 합니다.

ASA가 **ping** 명령에서 생성된 메시지에 응답하고 이를 허용하도록 하려면 이 구성이 필요합니다. **ping** 명령 출력은 응답이 수신되었는지를 보여줍니다. **ping** 명령을 입력한 후 호스트가 응답하지 않으면 다음과 유사한 메시지가 나타납니다.

```
ciscoasa(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ASA가 네트워크에 연결되어 있고 트래픽을 전달하는지 확인하려면 **show interface** 명령을 사용합니다. 지정된 *if_name*의 주소는 ping의 소스 주소로 사용됩니다.

매개변수 없이 **ping**을 입력하여 확장 ping을 수행할 수도 있습니다. 키워드로서 사용할 수 없는 일부 특성을 비롯한 매개변수에 대한 프롬프트가 표시됩니다.

예

다음 예는 ASA에서 다른 IP 주소가 보이는지를 확인하는 방법을 보여줍니다.

```
ciscoasa# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10-01-02 ms
```

다음 예는 DNS 이름을 사용하여 호스트를 지정합니다.

```
ciscoasa# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10-01-02 ms
```

다음은 확장 ping의 예입니다.

```
ciscoasa# ping
TCP [n]:
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10-01-02 ms
```

다음은 **ping tcp** 명령의 예입니다.

```
ciscoasa# ping
TCP [n]: yes
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]: y
Source IP address: 192.168.2.7
Source IP port: [0] 465
Repeat count: [5]
Timeout in seconds: [2] 5
Type escape sequence to abort.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 192.168.2.7 starting port 465, timeout is 5 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

ciscoasa# ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms


ciscoasa# ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 02-01-02 ms
```

```
ciscoasa(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 74.125.19.103 port 80
from 171.63.230.107, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 04-03-04 ms

ciscoasa# ping tcp 192.168.1.7 23 source 192.168.2.7 24966
Type escape sequence to abort.
Source port 24966 in use! Using port 24967 instead.
Sending 5 TCP SYN requests to 192.168.1.7 port 23
from 192.168.2.7 starting port 24967, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

관련 명령

명령	설명
icmp	인터페이스에서 종료되는 ICMP 트래픽에 대한 액세스 규칙을 구성합니다.
show interface	VLAN 구성에 대한 정보를 표시합니다.

16 장

police through pppoe client secondary 명령

police

클래스 맵에 QoS 폴리싱을 적용하려면 클래스 컨피그레이션 모드에서 **police** 명령을 사용합니다. 속도 제한 요구 사항을 제거하려면 이 명령의 **no** 형식을 사용합니다. 폴리싱은 어떠한 트래픽도 사용자가 구성한 최대 속도(비트/초 단위)를 초과하지 못하게 함으로써 하나의 트래픽 흐름이 전체 리소스를 차지할 수 없도록 하는 방법입니다. 트래픽이 최대 속도를 초과하면 ASA에서 초과 트래픽을 취소합니다. 또한 폴리싱은 허용되는 최대 단일 트래픽 버스트를 설정합니다.

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]

no police

구문 설명

conform-burst	준수 속도 값으로 조정되기 전 지속적인 버스트에서 허용되는 순간 바이트의 최대 수를 지정합니다(1000~512000000바이트).
conform-action	속도가 *conform_burst* 값보다 낮을 때 수행할 작업을 설정합니다.
conform-rate	이 트래픽 흐름에 대한 속도 제한을 설정합니다(초당 8000~2000000000 비트).
drop	패킷을 삭제합니다.
exceed-action	속도가 *conform-rate* 값과 *conform-burst* 값 사이인 경우 수행할 작업을 설정합니다.
input	입력 방향으로 흐르는 트래픽의 폴리싱을 활성화합니다.
output	출력 방향으로 흐르는 트래픽의 폴리싱을 활성화합니다.
transmit	패킷을 전송합니다.

기본값

기본 동작 또는 변수가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	**input** 옵션이 추가되었습니다. 이제 인바운드 방향의 폴리싱 트래픽이 지원됩니다.

사용 지침

폴리싱을 활성화하려면 Modular Policy Framework를 사용하십시오.

1. **class-map** - 폴리싱을 수행할 트래픽을 식별합니다.
2. **policy-map** - 각 클래스 맵과 관련된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다 .
   b. **police** - 클래스 맵에 대한 폴리싱을 활성화합니다.
3. **service-policy** - 정책 맵을 한 인터페이스에 또는 전체적으로 할당합니다.

참고 **police** 명령은 최대 속도 및 버스트 속도만을 적합한 속도 값으로 적용합니다. 이 두 옵션이 없으면 **conform-action** 또는 **exceed-action** 사양을 적용하지 않습니다.

참고 conform-burst 매개변수가 생략되면 기본값은 conform-rate의 1/32로 간주됩니다(바이트 단위). 즉, conform rate가 100,000이면 기본 conform-burst 값은 100,000/32 = 3,125입니다. conform-rate의 단위는 비트/초인 반면, conform-burst의 단위는 바이트입니다.

ASA에서 필요한 경우 QoS의 각 기능을 따로 구성할 수 있습니다. 그러나 예를 들면 일부 트래픽의 우선순위를 정하고 다른 트래픽이 대역폭 문제를 일으키지 못하도록 종종 ASA에서 여러 QoS 기능을 구성하기도 합니다.

다음은 인터페이스마다 지원되는 기능 조합입니다.

- 표준 우선순위 큐잉(특정 트래픽용) + 폴리싱(나머지 트래픽용).

  동일한 트래픽 집합에 대해서는 우선순위 큐잉과 폴리싱을 구성할 수 없습니다.
- 트래픽 셰이핑(인터페이스의 모든 트래픽) + 계층적 우선순위 큐잉(트래픽의 하위 집합)

일반적으로 트래픽 셰이핑을 활성화하는 경우 ASA에서 특별히 제한하는 것은 아니지만, 동일한 트래픽에 대해 폴리싱까지 활성화하지는 않습니다.

다음 지침을 참조하십시오.

- QoS는 단방향으로 적용되며, 정책 맵이 적용되는 인터페이스로 들어가는 트래픽만 영향을 받습니다(**input**을 지정하는지 **output**을 지정하는지에 따라 기존 인터페이스도 영향을 받음).
- 기존 트래픽이 이미 설정된 인터페이스에서 서비스 정책이 적용되거나 제거되면 QoS 정책은 트래픽 스트림에서 적용 또는 제거되지 않습니다. 그러한 연결에 대해 QoS 정책을 적용하거나 제거하려면 연결을 지우고 다시 설정해야 합니다. **clear conn** 명령을 참조하십시오.
- To-the-box 트래픽은 지원되지 않습니다.
- VPN 터널 바이패스 인터페이스를 드나드는 트래픽은 지원되지 않습니다.
- 터널 그룹 클래스 맵을 일치시키면 아웃바운드 폴리싱만 지원됩니다.

예

다음은 conform rate를 초당 100,000비트, 버스트 값을 20,000바이트로 설정하고 버스트 속도를 초과하는 트래픽을 삭제하도록 지정하는, 출력 방향에 대한 **police** 명령의 예입니다.

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class-map firstclass
ciscoasa(config-cmap)# class localclass
ciscoasa(config-pmap-c)# police output 100000 20000 exceed-action drop
ciscoasa(config-cmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

다음 예는 내부 웹 서버로 이동할 트래픽에 대해 속도 제한을 설정하는 방법을 보여줍니다.

```
ciscoasa# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
ciscoasa# class-map http_traffic
ciscoasa(config-cmap)# match access-list http_traffic
ciscoasa(config-cmap)# policy-map outside_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# police input 56000
ciscoasa(config-pmap-c)# service-policy outside_policy interface outside
ciscoasa(config)#
```

관련 명령

class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
clear configure policy-map	모든 정책 맵 구성을 제거합니다. 단, 정책 맵이 서비스 정책 명령에서 사용되고 있는 경우 해당 정책 맵은 제거되지 않습니다.
policy-map	트래픽 클래스 및 하나 이상의 작업을 결합한 정책을 구성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

policy

CRL 검색을 위한 소스를 지정하려면 ca-crl 컨피그레이션 모드에서 **policy** 명령을 사용합니다.

policy {**static** | **cdp** | **both**}

구문 설명

both	CRL 배포 지점을 사용하여 CRL을 얻지 못하는 경우 최대 5회까지 고정 CDP 사용을 시도하도록 지정합니다.
cdp	점검 중인 인증서 내에 포함된 CDP 확장을 사용합니다. 이 경우 ASA는 확인 중인 인증서의 CDP 확장에서 최대 5개의 CRL 배포 지점을 검색하고, 필요한 경우 구성된 기본값으로 정보를 보강합니다. 기본 CDP를 사용한 CRL 검색에 실패하는 경우 ASA는 목록에서 다음번 이용 가능한 CDP를 사용하여 다시 시도합니다. 이 작업은 ASA에서 CRL을 찾거나 목록의 모든 엔트리를 모두 시도할 때까지 계속됩니다.
static	최대 5개의 고정 CRL 배포 지점을 사용합니다. 이 옵션을 지정하는 경우 **protocol** 명령과 함께 LDAP 또는 HTTP URL도 지정하십시오.

기본값

기본 설정은 **cdp**입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crl 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 ca-crl 컨피그레이션 모드로 들어가서, 점검 중인 인증서의 CRL 배포 지점 확장을 사용하여 이루어지는 CRL 검색을 구성합니다. 실패 시 고정 CDP가 사용됩니다.

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# policy both
```

관련 명령

명령	설명
crl configure	ca-crl 컨피그레이션 모드로 들어갑니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드로 들어갑니다.
url	CRL 검색을 위한 고정 URL의 목록을 만들고 유지 관리합니다.

policy-list

BGP(Border Gateway Protocol) 정책 목록을 만들려면 정책 맵 컨피그레이션 모드에서 **policy-list** 명령을 사용합니다. 정책 목록을 제거하려면 이 명령의 **no** 형식을 사용합니다.

policy-list *policy-list-name* {**permit** | **deny**}

no policy-list *policy-list-name*

구문 설명

policy-list-name	구성된 정책 목록의 이름.
permit	일치 조건에 대한 액세스를 허용합니다.
deny	일치 조건에 대한 액세스를 거부합니다.

기본값

이 명령은 기본적으로 활성화되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

경로 맵 내에서 정책 목록이 참조되는 경우 정책 목록의 모든 일치 명령문이 평가 및 처리됩니다. 경로 맵 내에 둘 이상의 정책 목록을 구성할 수 있습니다. 경로 맵 내에 구성된 정책 목록은 AND 또는 OR 의미 체계로 평가됩니다. 정책 목록은 같은 경로 맵 내에 있으나 정책 목록 밖에서 구성된 기존 일치 항목 및 설정 명령문과도 공존할 수 있습니다. 여러 정책 목록이 하나의 경로 맵 엔트리 내에서 일치를 수행하는 경우 모든 정책 목록은 들어오는 특성에 대해서만 확인됩니다.

policy-list 하위 명령은 다음과 같습니다.

하위 명령	세부사항
match **as-path [path-list-number]**	as-path를 확인합니다. as-path path-list number를 여러 개 지정할 수 있습니다.
Match community [community-name] [exact-match]	Community name은 필수, exact-match는 선택 사항입니다. 여러 이름을 지정할 수 있습니다.
Match interface [interface-name]	여러 인터페이스 이름을 지정할 수 있습니다.

하위 명령	세부사항
match metric <0-4294967295>	여러 숫자를 지정할 수 있습니다.
Match ip address [acl name | prefix-list [prefix-listname]]	여러 acl 이름 또는 prefix-list 이름을 지정할 수 있지만 두 가지가 공존할 수는 없습니다. 두 정책 목록 중 하나만 prefixlist 또는 acl을 가질 수 있습니다.
Match ip next-hop [acl name | prefix-list [prefix-listname]]	여러 acl 이름 또는 prefix-list 이름을 지정할 수 있지만 두 가지가 공존할 수는 없습니다. 두 정책 목록 중 하나만 prefixlist 또는 acl을 가질 수 있습니다.
Match ip route-source [acl name | prefix-list [prefix-listname]]	여러 acl 이름 또는 prefix-list 이름을 지정할 수 있지만 두 가지가 공존할 수는 없습니다. 두 정책 목록 중 하나만 prefixlist 또는 acl을 가질 수 있습니다.
Default match	기본값은 "match" 아래에 위의 모든 옵션을 갖게 됩니다.
Help	후속 명령에 대한 도움말
No	명령에 대한 부정
Exit	정책 맵 모드 종료

예

다음 예에서는 AS 1 및 metric 10과 일치하는 모든 네트워크 접두사를 허용하도록 정책 목록을 구성합니다.

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-1 permit
ciscoasa(config-policy-list)# match as-path 1
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

다음 예에서는 community 20 및 metric 10과 일치하는 트래픽을 허용하도록 정책 목록을 구성합니다.

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-2 permit
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

다음 예에서는 community 20 및 metric 10과 일치하는 트래픽을 거부하도록 정책 목록을 구성합니다.

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-3 deny
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
```

policy-map

Modular Policy Framework를 사용할 경우 글로벌 컨피그레이션 모드에서 **policy-map** 명령(**type** 키워드 없이)을 사용하여 Layer 3/4 클래스 맵(**class-map** 또는 **class-map type management** 명령)으로 식별하는 트래픽에 작업을 할당합니다. Layer 3/4 정책 맵을 제거하려면 이 명령의 **no** 형식을 사용합니다.

policy-map *name*

no policy-map *name*

구문 설명

name	이 정책 맵의 이름을 최대 40자로 지정합니다. 모든 유형의 정책 맵은 동일한 네임스페이스를 사용하므로, 다른 정책 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

기본값

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며, 모든 인터페이스의 트래픽에 특정 검사가 적용됩니다(전역 정책). 모든 검사가 기본적으로 사용되는 것은 아닙니다. 전역 정책은 하나만 적용할 수 있으므로, 전역 정책을 변경하려면 기본 정책을 편집하거나 비활성화한 후 새 정책을 적용해야 합니다. 인터페이스 정책은 특정 기능에 대해 전역 정책을 재지정합니다.

기본 정책에는 다음 애플리케이션 검사가 포함됩니다.

- 최대 메시지 길이 512바이트에 대한 DNS 검사
- FTP
- H323(H225)
- H323(RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny(SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

기본 정책 컨피그레이션에는 다음 명령이 포함됩니다.

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
message-length maximum client auto
message-length maximum 512
```

```
dns-guard
protocol-enforcement
nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Modular Policy Framework의 구성은 네 작업으로 구성됩니다.

1. **class-map** 또는 **class-map type management** 명령을 사용하여 작업을 적용할 Layer 3 및 4 트래픽을 식별합니다.
2. (애플리케이션 검사 전용) **policy-map type inspect** 명령을 사용하여 애플리케이션 검사 트래픽에 대한 특별 작업을 정의합니다.
3. **policy-map** 명령을 사용하여 Layer 3 및 4 트래픽에 작업을 적용합니다.
4. **service-policy** 명령을 사용하여 인터페이스에 대한 작업을 활성화합니다.

최대 정책 맵 수는 64이지만 인터페이스당 정책 맵을 하나만 적용할 수 있습니다. 동일한 정책 맵을 여러 인터페이스에 적용할 수 있습니다. Layer 3/4 정책 맵에서 여러 Layer 3/4 클래스 맵을 식별할 수 있으며(**class** 명령 참조), 하나 이상의 기능 유형에서 각 클래스 맵으로 여러 작업을 할당할 수 있습니다.

예

다음은 연결 정책용 **policy-map** 명령의 예로, 웹 서버 10.1.1.1에 대해 허용된 연결 수를 제한합니다.

```
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)# policy-map global-policy
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 conn-max 256
```

다음 예는 정책 맵에서 multi-match의 작동 방식을 보여줍니다.

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80

ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

다음 예는 첫 번째 사용 가능한 클래스 맵으로 트래픽을 확인하고, 동일한 기능 도메인에서 작업을 지정하는 이후의 클래스 맵으로는 확인하지 않는 방법을 보여줍니다.

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

텔넷 연결이 시작되면 **class telnet_traffic**을 확인합니다. 마찬가지로 FTP 연결이 시작되면 **class ftp_traffic**을 확인합니다. 텔넷 및 FTP 이외의 TCP 연결에서는 **class tcp_traffic**을 확인합니다. 텔넷 또는 FTP 연결에서 **class tcp_traffic**을 확인할 수 있더라도, 전에 다른 클래스에서 일치를 확인했으므로 ASA는 이 일치를 수행하지 않습니다.

NetFlow 이벤트는 Modular Policy Framework를 통해 구성됩니다. Modular Policy Framework가 NetFlow에 대해 구성되지 않은 경우 이벤트가 기록되지 않습니다. 트래픽 일치 확인은 클래스가 구성된 순서대로 진행됩니다. 일치가 감지되면 다른 클래스가 더 이상 점검되지 않습니다. NetFlow 이벤트의 경우 컨피그레이션 요구 사항은 다음과 같습니다.

- flow-export 대상(즉, NetFlow 컬렉터)은 IP 주소로 고유하게 식별됩니다.
- 지원되는 이벤트 유형은 flow-create, flow-teardown, flow-denied, flow-update 및 all입니다. all은 앞에 나열된 4개의 이벤트 유형을 포함합니다.
- 어떤 NetFlow 레코드를 각 컬렉터로 전송할지를 결정하기 위해 NetFlow 컬렉터 및 필터의 주소를 구성하려면 **flow-export event-type** {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination** 명령을 사용합니다.
- Flow-export 작업은 인터페이스 정책에서 지원되지 않습니다.
- Flow-export 작업은 **class-default** 명령, 그리고 **match any** 또는 **match access-list** 명령의 클래스에서만 지원됩니다.
- NetFlow 컬렉터를 정의하지 않으면 컨피그레이션 작업이 발생하지 않습니다.
- NetFlow Secure Event Logging 필터링은 순서와 상관이 없습니다.

다음 예는 호스트 10.1.1.1과 20.1.1.1 사이의 모든 NetFlow 이벤트를 수신 15.1.1.1로 내보냅니다.

```
ciscoasa(config)# access-list flow_export_acl permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 15.1.1.1
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
clear configure policy-map	모든 정책 맵 컨피그레이션을 제거합니다. 정책 맵이 **service-policy** 명령에서 사용되고 있는 경우 해당 정책 맵은 제거되지 않습니다.
class-map	트래픽 클래스 맵을 정의합니다.
service-policy	정책 맵을 한 인터페이스에 또는 모든 인터페이스에 전체적으로 할당합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

policy-map type inspect

Modular Policy Framework를 사용할 경우 글로벌 컨피그레이션 모드에서 **policy-map type inspect** 명령을 사용하여 검사 애플리케이션 트래픽에 대한 특수 작업을 정의합니다. 검사 정책 맵을 제거하려면 이 명령의 **no** 형식을 사용합니다.

policy-map type inspect *application policy_map_name*

no policy-map [**type inspect** *application*] *policy_map_name*

구문 설명

application	작업을 수행할 애플리케이션 트래픽의 유형을 지정합니다. 사용 가능한 유형은 다음과 같습니다. • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **HTTP** • **im** • **ip-options** • **ipsec-pass-thru** • **ipv6** • **mgcp** • **netbios** • **radius-accounting** • **rtsp** • **scansafe** • **sip** • **skinny** • **snmp**
policy_map_name	이 정책 맵의 이름을 최대 40자로 지정합니다. "_internal" 또는 "_default"로 시작되는 이름은 예약되어 있으므로 사용할 수 없습니다. 모든 유형의 정책 맵은 동일한 네임스페이스를 사용하므로, 다른 정책 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.2(1)	IPv6 검사를 지원하기 위해 **ipv6** 키워드가 추가되었습니다.
9.0(1)	Cloud Web Security를 지원하기 위해 **scansafe** 키워드가 추가되었습니다.

사용 지침

Modular Policy Framework를 사용하면 많은 애플리케이션 검사에 대한 특별 작업을 구성할 수 있습니다. Layer 3/4 정책 맵에서(**policy-map** 명령) **inspect** 명령을 사용하여 검사 엔진을 활성화할 때, **policy-map type inspect** 명령으로 만든 검사 정책 맵에 정의된 대로 작업을 활성화할 수도 있습니다. 예를 들면 **inspect http http_policy_map** 명령을 입력합니다. 여기서 http_policy_map은 검사 정책 맵의 이름입니다.

검사 정책 맵은 정책 맵 컨피그레이션 모드에서 입력하는 다음과 같은 명령 중 하나 이상으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 명령은 애플리케이션에 따라 다릅니다.

- **match** 명령 - 애플리케이션 트래픽을 애플리케이션에 해당하는 기준(예: URL 문자열)과 맞춰볼 수 있도록, 검사 정책 맵에서 **match** 명령을 직접 정의할 수 있습니다. 그런 다음 일치 컨피그레이션 모드에서 작업(**drop**, **reset**, **log** 등)을 활성화할 수 있습니다. 사용 가능한 **match** 명령은 애플리케이션에 따라 다릅니다.
- **class** 명령 - 이 명령은 정책 맵에서 검사 정책 맵을 식별합니다(검사 클래스 맵 생성은 **class-map type inspect** 명령 참조). 검사 정책 맵에는 애플리케이션 트래픽을 애플리케이션 관련 기준(예: URL 문자열)과 맞춰보고 정책 맵에서 작업을 활성화할 수 있는 **match** 명령이 포함됩니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 **match** 명령을 사용하는 것의 차이는, 여러 일치를 그룹화할 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.
- **parameters** 명령 - 매개변수는 검사 엔진의 동작에 영향을 미칩니다. 매개변수 컨피그레이션 모드에서 사용 가능한 명령은 애플리케이션에 따라 다릅니다.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다.

일부 **match** 명령은 패킷 내부의 텍스트를 확인하기 위해 정규식을 사용할 수 있습니다. 여러 정규식을 그룹화하는 **regex** 명령 및 **class-map type regex** 명령을 참조하십시오.

기본 검사 정책 맵 컨피그레이션에는 다음 명령이 포함됩니다.

```
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
```

패킷이 서로 다른 여러 **match** 또는 **class** 명령과 일치하는 경우 ASA에서 작업을 적용하는 순서는 내부 ASA 규칙에 의해 결정되며, 정책 맵에 추가된 순서에 의해 결정되지 않습니다. 내부 규칙은 애플리케이션 유형 및 패킷 분석의 논리적 진행에 의해 결정되며, 사용자가 구성할 수 없습니다. 예를 들어 HTTP 트래픽의 경우, Request Method 필드 분석이 Header Host Length 필드 분석을 선행합니다. Header Host Length 필드에 대한 작업이 수행되기 전에 Request Method 필드에 대한 작업이 수행됩니다. 예를 들어 다음의 일치 명령을 임의의 순서로 입력할 수 있지만 **match request method get** 명령이 가장 먼저 적용됩니다.

```
ciscoasa(config-pmap)# match request header host length gt 100
ciscoasa(config-pmap-c)# reset
ciscoasa(config-pmap-c)# match request method get
ciscoasa(config-pmap-c)# log
```

작업에서 패킷을 삭제하는 경우 추가 작업이 수행되지 않습니다. 예를 들어, 첫 번째 작업에서 연결을 재설정하면 추가 **match** 명령이 사용되지 않습니다. 첫 번째 작업에서 패킷을 기록하면, 두 번째 작업(예: 연결 재설정)이 발생할 수 있습니다. 동일한 **match** 명령에 대해 **reset**(또는 **drop-connection** 등) 및 **log** 작업을 모두 구성할 수 있습니다. 이 경우 지정된 일치에 대해 재설정되기 전에 패킷이 기록됩니다.

패킷에 동일한 여러 **match** 또는 **class** 명령이 있는 경우 논리 맵에 나타나는 순서대로 적용됩니다. 예를 들어, 헤더 길이가 1001인 패킷의 경우 아래의 첫 번째 명령이 적용되고, 기록되고, 두 번째 명령이 적용된 후 재설정됩니다. 두 **match** 명령의 순서를 바꾸면, 두 번째 **match** 명령이 적용되기 전에 패킷이 삭제되고 연결이 재설정됩니다. 따라서 기록이 진행되지 않습니다.

```
ciscoasa(config-pmap)# match request header length gt 100
ciscoasa(config-pmap-c)# log
ciscoasa(config-pmap-c)# match request header length gt 1000
ciscoasa(config-pmap-c)# reset
```

클래스 맵은 클래스 맵 내 최저 우선순위 **match** 명령을 기준으로 다른 클래스 맵 또는 **match** 명령과 동일한 유형으로 확인됩니다(우선순위는 내부 규칙을 기반으로 함). 한 클래스 맵에 다른 클래스 맵과 동일한 유형의 최저 우선순위 **match** 명령이 있으면, 정책 맵에 추가된 순서대로 클래스 맵이 적용됩니다. 각 클래스 맵의 최저 우선순위 명령이 다른 경우, 더 높은 우선순위 **match** 명령의 클래스 맵이 먼저 적용됩니다.

검사 정책 맵을 수정하려는 경우 다음 지침을 참조하십시오.

- HTTP 검사 정책 맵 - 사용 중인 HTTP 검사 정책 맵을 수정하려는 경우(**policy-map type inspect http**), 변경 사항을 적용하려면 **inspect http** *map* 작업을 제거한 후 다시 적용해야 합니다. 예를 들어 "http-map" 검사 정책 맵을 수정하려면 Layer 3/4 정책에서 **inspect http http-map** 명령을 제거한 후 다시 추가해야 합니다.

  ```
  ciscoasa(config)# policy-map test
  ciscoasa(config-pmap)# class http0
  ciscoasa(config-pmap-c)# no inspect http http-map
  ciscoasa(config-pmap-c)# inspect http http-map
  ```

- 모든 검사 정책 맵 - 사용 중인 검사 정책 맵을 다른 맵 이름으로 교체하려면 **inspect** *protocol map* 명령을 제거한 후 새 맵으로 다시 추가해야 합니다. 예:

  ```
  ciscoasa(config)# policy-map test
  ciscoasa(config-pmap)# class sip
  ciscoasa(config-pmap-c)# no inspect sip sip-map1
  ciscoasa(config-pmap-c)# inspect sip sip-map2
  ```

예

다음은 HTTP 검사 정책 맵 및 관련 클래스 맵의 예입니다. 이 정책 맵은 서비스 정책에 의해 활성화되는 Layer 3/4 정책 맵에 의해 활성화됩니다.

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex example
ciscoasa(config-cmap)# match regex example2

ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs

ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log

ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test (a Layer 3/4 class map not shown)
ciscoasa(config-pmap-c)# inspect http http-map1

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

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
parameters	검사 정책 맵에 대한 매개변수 컨피그레이션 모드로 들어갑니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

policy-server-secret

SiteMinder SSO 서버에 대한 인증 요청을 암호화하는 데 사용되는 비밀 키를 구성하려면 webvpn-sso-siteminder 컨피그레이션 모드에서 **policy-server-secret** 명령을 사용합니다. 비밀 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

policy-server-secret *secret-key*

no policy-server-secret

참고 이 명령은 SiteMinder SSO 인증에 필요합니다.

구문 설명

secret-key	인증 통신을 암호화하기 위해 비밀 키로서 사용되는 문자열. 문자의 최대 또는 최소 길이 값은 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Config-webvpn-sso-siteminder 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

WebVPN에서만 사용 가능한 단일 로그인이 지원되므로, 사용자는 사용자 이름과 비밀번호를 한 번만 입력하여 다양한 서버의 서로 다른 보안 서비스에 안전하게 액세스할 수 있습니다. 먼저 **sso-server** 명령을 사용하여 SSO 서버를 만듭니다. SiteMinder SSO 서버의 경우 **policy-server-secret** 명령은 ASA와 SSO 서버 간 인증 통신을 보호합니다.

명령 인수 *secret-key*는 비밀번호와 비슷합니다. 만들고 저장하고 구성할 수 있습니다. 양쪽에 모두 구성할 수 있습니다. 즉, **policy-server-secret** 명령을 사용하여 ASA에 구성하고 Cisco Java 플러그인 인증 체계를 사용하여 SiteMinder Policy Server에 구성합니다.

이 명령은 SSO 서버의 SiteMinder 유형에만 적용됩니다.

예

다음 명령(config-webvpn-sso-siteminder 모드에서 입력하며 임의 문자열을 인수로 포함)은 SiteMinder SSO 서버 인증 통신을 위한 비밀 키를 생성합니다.

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
ciscoasa(config-webvpn-sso-siteminder)#
```

관련 명령

명령	설명
max-retry-attempts	실패한 SSO 인증 시도에 대해 ASA에서 재시도할 횟수를 구성합니다.
request-timeout	실패한 SSO 인증 시도 시간 제한(초 단위)을 지정합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso-server	단일 로그인 서버를 만듭니다.
test sso-server	SSO 서버를 평가 인증 요청으로 테스트합니다.
web-agent-url	ASA에서 SiteMinder SSO 인증 요청을 수행하는 SSO 서버 URL을 지정합니다.

policy static sgt

수동으로 구성된 Cisco TrustSec 링크에 정책을 적용하려면 cts 수동 인터페이스 컨피그레이션 모드에서 **policy static sgt** 명령을 사용합니다. 수동으로 구성된 CTS 링크에서 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

policy static sgt *sgt_number* [**trusted**]

no policy static sgt *sgt_number* [**trusted**]

구문 설명

sgt *sgt_number*	피어로부터 들어오는 트래픽에 적용할 SGT 번호를 지정합니다. 유효한 값은 2~65519입니다.
static	링크에서 들어오는 트래픽에 SGT 정책을 적용합니다.
trusted	명령에서 SGT가 지정된 인터페이스의 인그레스(ingress) 트래픽이 SGT를 덮어쓰면 안 됨을 나타냅니다. 기본값은 신뢰할 수 없음입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Cts 수동 인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 수동으로 구성된 CTS 링크에 정책을 적용합니다.

제한

- 물리적 인터페이스, VLAN 인터페이스, 포트 채널 인터페이스 및 중복 인터페이스에서만 지원됩니다.
- BVI, TVI, VNI 등의 논리적 인터페이스나 가상 인터페이스에서는 지원되지 않습니다.

예

다음 예는 Layer 2 SGT Imposition에 대한 인터페이스를 활성화하고 인터페이스 신뢰 여부를 지정합니다.

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

관련 명령

명령	설명
cts manual	Layer 2 SGT Imposition을 활성화하고 cts 수동 인터페이스 컨피그레이션 모드로 들어갑니다.
propagate sgt	인터페이스에서 보안 그룹 태그(**sgt**라고 함)를 전파합니다. 전파는 기본적으로 활성화되어 있습니다.

polltime interface

액티브/액티브 장애 조치 컨피그레이션에서 데이터 인터페이스 폴링 및 대기 시간을 지정하려면 장애 조치 그룹 컨피그레이션 모드에서 **polltime interface** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

polltime interface [**msec**] *time* [**holdtime** *time*]

no polltime interface [**msec**] *time* [**holdtime** *time*]

구문 설명

holdtime *time*	(선택 사항) 데이터 인터페이스가 피어 인터페이스에서 hello 메시지를 받아야 하는 시간을 설정합니다. 이 시간 이후에는 피어 인터페이스가 실패로 선언됩니다. 유효한 값은 5~75초입니다.
interface *time*	데이터 인터페이스 폴링 기간을 지정합니다. 유효한 값은 3~15초입니다. 선택 사항인 **msec** 키워드를 사용하는 경우 유효한 값은 500~999밀리초입니다.
msec	(선택 사항) 제공된 시간이 밀리초 단위임을 지정합니다.

기본값

poll *time*은 5초입니다.

holdtime *time*은 poll *time*의 5배입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
장애 조치 그룹 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	선택 사항인 **holdtime** *time* value 값 및 poll time을 밀리초 단위로 지정하는 기능을 포함하도록 이 명령이 변경되었습니다.

사용 지침

지정한 장애 조치 그룹과 연결된 인터페이스에서 hello 패킷을 내보내는 빈도를 변경하려면 **polltime interface** 명령을 사용합니다. 이 명령은 액티브/액티브 장애 조치에서만 이용할 수 있습니다. 액티브/스탠바이 장애 조치 컨피그레이션에서는 **failover polltime interface** 명령을 사용하십시오.

holdtime 값은 폴링 시간(poll time)의 5배보다 적게 입력할 수 없습니다. 폴링 시간이 빠를수록 ASA에서 더욱 신속하게 오류를 감지하고 장애 조치를 시행할 수 있습니다. 그러나 감지 기능이 빨라지면 네트워크에 일시적으로 정체 현상이 일어났을 때 불필요한 전환이 발생할 수 있습니다. 대기 시간(hold time)의 절반이 지나도록 인터페이스에서 hello 패킷이 수신되지 않으면 인터페이스 테스트가 시작됩니다.

컨피그레이션에 **failover polltime unit** 및 **failover polltime interface** 명령을 모두 포함할 수 있습니다.

참고 장애 조치 컨피그레이션에서 CTIQBE 트래픽이 ASA를 통과하는 경우 ASA에서 장애 조치 대기 시간을 30초 미만으로 설정해야 합니다. CTIQBE keepalive 시간 제한은 30초이므로, 장애 조치 상황에서 장애 조치가 발생하기 전에 시간이 초과될 수 있습니다. CTIQBE가 시간 초과되면 Cisco IP SoftPhone과 Cisco CallManager의 연결이 삭제되며, IP SoftPhone 클라이언트를 CallManager에서 다시 등록해야 합니다.

예

다음의 부분적인 예는 장애 조치 그룹에 대해 가능한 컨피그레이션을 보여줍니다. 장애 조치 그룹 1의 데이터 인터페이스에 대해 인터페이스 폴링 시간은 500밀리초, 대기 시간은 5초로 설정됩니다.

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
failover group	액티브/액티브 장애 조치에 대한 장애 조치 그룹을 정의합니다.
failover polltime	유닛 장애 조치 폴링 및 대기 시간을 지정합니다.
failover polltime interface	액티브/스탠바이 장애 조치 컨피그레이션에 대해 인터페이스 폴링 시간 및 대기 시간을 지정합니다.

pop3s

POP3S 컨피그레이션 모드로 들어가려면 글로벌 컨피그레이션 모드에서 **pop3s** 명령을 사용합니다. POP3S 명령 모드에서 입력한 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

POP3는 인터넷 서버에서 사용자 대신 이메일을 받아서 보관하는 데 사용하는 클라이언트/서버 프로토콜입니다. 주기적으로 사용자(또는 클라이언트 이메일 수신자)는 서버에서 사서함을 확인하여 메일을 다운로드합니다. 이 표준 프로토콜은 가장 널리 사용되는 이메일 제품에 내장되어 있습니다. POP3S를 사용하면 SSL 연결을 통해 이메일을 수신할 수 있습니다.

pop3s

no pop3

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 POP3S 컨피그레이션 모드로 들어가는 방법을 보여줍니다.

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

관련 명령

명령	설명
clear configure pop3s	POP3S 컨피그레이션을 제거합니다.
show running-config pop3s	POP3S에 대해 실행 중인 컨피그레이션을 표시합니다.

port(e-mail proxy)

이메일 프록시가 수신 대기할 포트를 지정하려면 해당 이메일 프록시 명령 모드에서 **port** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

port {*portnum*}

no port

구문 설명

portnum	이메일 프록시에서 사용할 포트. 로컬 TCP 서비스와의 충돌을 피하려면 1024~65535 범위의 포트 번호를 사용하십시오.

기본값

이메일 프록시용 기본 포트는 다음과 같습니다.

이메일 프록시	기본 포트
IMAP4S	993
POP3S	995
SMTPS	988

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Pop3s	• 예	—	• 예	—	—
Imap4s	• 예	—	• 예	—	—
Smtps	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

로컬 TCP 서비스와의 충돌을 피하려면 1024~65535 범위의 포트 번호를 사용하십시오.

예

다음 예는 IMAP4S 이메일 프록시에 대해 포트 1066을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# port 1066
```

port(config-mdm-proxy)

이 명령은 MDM 프록시 서비스가 MDM 등록 및 체크인을 수신 대기하는 포트를 구성합니다. 기본값으로 돌아가려면 구성된 값을 지정하는 이 명령의 **no** 형식을 사용합니다.

[no] port [enrollment *enroll_port*] **[checkin** *checkin_port*]

구문 설명

enroll_port	MDM 클라이언트 인증 및 등록 요청을 수신 대기하는 포트의 번호입니다. 유효한 범위는 1~65535입니다. 기본적으로 TCP 포트 443이 사용됩니다.
checkin_port	MDM 체크인 요청을 수신 대기하는 포트의 번호입니다. 기본값이 없습니다(값이 필요함). 유효한 범위는 1~65535입니다. 이 포트는 다른 서비스에서 사용되지 않는 것이어야 합니다.

기본값

MDM 프록시 등록을 위한 기본 포트는 TCP 포트 443입니다. 체크인을 위한 기본 포트는 없으므로 직접 구성해야 합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
config-mdm-proxy	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

포트 하위 명령의 'no' 형식으로 지정한 포트 번호 중 하나가 현재 컨피그레이션에 있는 한 줄과 일치하지 않으면 오류 메시지가 표시됩니다.

MDM 체크인 포트 번호가 현재 다른 서비스에서 사용 중인 포트와 일치하면, 해당 인터페이스에서 MDM 프록시를 활성화할 때 오류 메시지가 표시됩니다.

예

다음 예는 MDM 프록시용 체크인 포트를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# port checkin 1077
ciscoasa (config-mdm-proxy)# enable outside
```

port-channel load-balance

EtherChannels의 경우 로드 밸런싱 알고리즘을 지정하려면 인터페이스 컨피그레이션 모드에서 **port-channel load-balance** 명령을 사용합니다. 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

port-channel load-balance {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**}

no port-channel load-balance

구문 설명

dst-ip	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 수신 IP 주소
dst-ip-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 수신 IP 주소 • 목적지 포트
dst-mac	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 대상 MAC 주소
dst-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 목적지 포트
src-dst-ip	(기본값) 패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 IP 주소 • 수신 IP 주소
src-dst-ip-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 IP 주소 • 수신 IP 주소 • 소스 포트 • 목적지 포트
src-dst-mac	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 MAC 주소 • 대상 MAC 주소
src-dst-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 포트 • 목적지 포트
src-ip	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 IP 주소

src-ip-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 IP 주소 • 소스 포트
src-mac	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 MAC 주소
src-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • 소스 포트
vlan-dst-ip	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • VLAN • 수신 IP 주소
vlan-dst-ip-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • VLAN • 수신 IP 주소 • 목적지 포트
vlan-only	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • VLAN
vlan-src-dst-ip	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • VLAN • 소스 IP 주소 • 수신 IP 주소
vlan-src-dst-ip-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • VLAN • 소스 IP 주소 • 수신 IP 주소 • 소스 포트 • 목적지 포트
vlan-src-ip	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • VLAN • 소스 IP 주소
vlan-src-ip-port	패킷의 다음 특성에 따라 인터페이스에서 패킷을 로드 밸런싱합니다. • VLAN • 소스 IP 주소 • 소스 포트

명령 기본값

기본값은 **src-dst-ip**입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.

사용 지침

ASA에서는 패킷의 소스 및 수신 IP 주소를 해싱하여 EtherChannel의 인터페이스에 패킷을 분산시킵니다(**src-dst-ip**). 결과의 나머지 부분에 따라 흐름을 보유하는 인터페이스가 결정되는 모듈로 작업의 액티브 링크 수를 기준으로 결과 해시가 분할됩니다. *hash_value* **mod** *active_links*의 결과가 0인 모든 패킷은 EtherChannel의 첫 번째 인터페이스가 되고, 결과가 1인 패킷은 두 번째 인터페이스, 결과가 2인 패킷은 세 번째 인터페이스 등으로 이어집니다. 예를 들어, 액티브 링크가 15개 있는 경우 모듈로 작업에서는 0에서 14까지의 값을 제공합니다. 액티브 링크가 6개인 경우 해당 값은 0~5가 되며, 이런 식으로 계속 적용할 수 있습니다.

클러스터링에서 Spanned EtherChannel의 경우 ASA 단위로 로드 밸런싱이 이루어집니다. 예를 들어, 8개의 ASA 전체에서 Spanned EtherChannel에 32개의 액티브 인터페이스가 있는 경우 EtherChannel의 ASA 하나당 인터페이스는 4개이며 ASA의 4개 인터페이스에만 로드 밸런싱이 실행됩니다.

액티브 인터페이스가 중단되고 스탠바이 인터페이스로 대체되지 않을 경우, 나머지 링크 간의 트래픽이 다시 밸런싱됩니다. 오류는 Layer 2의 스패닝 트리와 Layer 3의 라우팅 테이블에서 모두 마스킹되므로, 전환 작업은 다른 네트워크 디바이스에 투명하게 이루어집니다.

예

다음 예는 소스 및 대상 IP 주소와 포트를 사용하기 위한 로드 밸런싱 알고리즘을 설정합니다.

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel load-balance src-dst-ip-port
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 지정합니다.
lacp port-priority	채널 그룹에서 물리적 인터페이스의 우선순위를 설정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel min-bundle	포트 채널 인터페이스를 액티브 상태로 설정하는 데 필요한 액티브 인터페이스의 최소 개수를 지정합니다.
show lacp	트래픽 통계, 시스템 식별자, 인접 디바이스 세부사항 같은 LACP 정보가 표시됩니다.

명령	설명
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령을 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel load-balance	정해진 매개변수 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

port-channel min-bundle

EtherChannels의 경우, 포트 채널 인터페이스를 액티브 상태로 전환하기 위해 필요한 액티브 인터페이스의 최소 개수를 지정하려면 인터페이스 컨피그레이션 모드에서 **port-channel min-bundle** 명령을 사용합니다. 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

port-channel min-bundle *number*

no port-channel min-bundle

구문 설명

number	포트 채널 인터페이스를 액티브 상태로 전환하기 위해 필요한 액티브 인터페이스의 최소 개수를 1~8 범위로 지정합니다. 9.2(1) 이상에서는 액티브 인터페이스의 범위가 1~16입니다.

명령 기본값

기본값은 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.
9.2(1)	액티브 인터페이스의 개수가 8에서 16으로 증가했습니다.

사용 지침

포트 채널 인터페이스에 대해 이 명령을 입력합니다. 채널 그룹의 액티브 인터페이스가 이 값의 범위에 속할 경우, 포트 채널 인터페이스가 종료되며 디바이스 수준 장애 조치가 일어납니다.

예

다음 예는 포트 채널 인터페이스를 액티브 상태로 전환하는 데 필요한 액티브 인터페이스의 최소 개수를 2로 설정합니다.

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel min-bundle 2
```

관련 명령

명령	설명
channel-group	EtherChannel에 인터페이스를 추가합니다.
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 지정합니다.
lacp port-priority	채널 그룹에서 물리적 인터페이스의 우선순위를 설정합니다.
lacp system-priority	LACP 시스템 우선순위를 설정합니다.
port-channel load-balance	로드 밸런싱 알고리즘을 구성합니다.
show lacp	트래픽 통계, 시스템 식별자, 인접 디바이스 세부사항 같은 LACP 정보가 표시됩니다.
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령을 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel load-balance	정해진 매개변수 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

port-channel span-cluster

ASA 클러스터에서 이 EtherChannel을 Spanned EtherChannel로 설정하려면 인터페이스 컨피그레이션 모드에서 **port-channel span-cluster** 명령을 사용합니다. Spanning을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

port-channel span-cluster [**vss-load-balance**]

no port-channel span-cluster [**vss-load-balance**]

구문 설명

vss-load-balance	(선택 사항) VSS 로드 밸런싱을 활성화합니다. ASA를 VSS 또는 vPC에 있는 두 개의 스위치에 연결할 경우 VSS 로드 밸런싱을 활성화해야 합니다. 이 기능은 VSS(또는 vPC) 쌍에 대한 ASA 간의 물리적 링크 연결이 균형을 이루도록 보장합니다. 로드 밸런싱을 활성화하기 전에 **channel-group** 명령에서 **vss-id** 키워드를 각 멤버 인터페이스에 대해 구성해야 합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 기능은 Spanned EtherChannel 모드(**cluster interface-mode spanned**)에서만 사용할 수 있습니다.

이 기능을 사용하면 유닛당 하나 이상의 인터페이스를 클러스터 내의 모든 유닛을 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. Spanned EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 IP 주소가 인터페이스가 아닌 브릿지 그룹에 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.

예

다음 예는 tengigabitethernet 0/8 인터페이스가 유일한 멤버인 EtherChannel(port-channel 2)을 생성한 다음 클러스터 전체에 적용합니다. 두 개의 하위 인터페이스가 port-channel 2에 추가됩니다.

```
interface tengigabitethernet 0/8
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
interface port-channel 2.10
    vlan 10
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE
interface port-channel 2.20
    vlan 20
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

관련 명령

명령	설명
interface	인터페이스 컨피그레이션 모드로 진입합니다.
cluster interface-mode	Spanned EtherChannels 또는 개별 인터페이스에 대해 클러스터 인터페이스 모드를 설정합니다.

port-forward

클라이언트리스 SSL VPN 세션 사용자가 포워딩된 TCP 포트를 통해 액세스할 수 있는 애플리케이션 집합을 구성하려면 webvpn 컨피그레이션 모드에서 **port-forward** 명령을 사용합니다.

port-forward {*list_name local_port remote_server remote_port description*}

여러 애플리케이션에 대한 액세스를 구성하려면 동일한 *list_name*과 함께, 각 애플리케이션에 대해 한 번씩 이 명령을 여러 번 사용합니다.

구성된 애플리케이션을 목록에서 제거하려면 **no port-forward** *list_name local_port* 명령을 사용합니다(*remote_server* 및 *remote_port* 매개변수는 포함할 필요 없음).

no port-forward *listname localport*

전체 구성된 목록을 제거하려면 **no port-forward** *list_name* 명령을 사용합니다.

no port-forward *list_name*

구문 설명

description	최종 사용자 Port Forwarding Java 애플릿 화면에 표시되는 애플리케이션 이름 또는 짧은 설명을 제공합니다. 최대 64자.
list_name	클라이언트리스 SSL VPN 세션의 사용자가 액세스할 수 있는 애플리케이션 집합을 그룹화합니다(포워딩된 TCP 포트). 최대 64자.
local_port	애플리케이션에 대한 TCP 트래픽을 수신 대기하는 로컬 포트를 지정합니다. 로컬 포트 번호는 *list_name*에 대해 한 번만 사용할 수 있습니다. 1~65535 범위의 포트 번호를 입력합니다. 기존 서비스와의 충돌을 피하려면 1024보다 큰 포트 번호를 사용하십시오.
remote_port	원격 서버에서 이 애플리케이션에 대해 연결할 포트를 지정합니다. 애플리케이션이 사용하는 실제 포트입니다. 1~65535 범위의 포트 번호 또는 포트 이름을 입력합니다.
remote_server	애플리케이션에 대한 원격 서버의 DNS 이름 또는 IP 주소를 제공합니다. IP 주소를 입력하는 경우 IPv4 또는 IPv6 형식으로 입력할 수 있습니다. 특정 IP 주소에 대해 클라이언트 애플리케이션을 구성할 필요가 없도록 호스트 이름을 사용하는 것이 좋습니다. dns 서버 그룹 명령 **name-server**는 IP 주소에 대한 호스트 이름을 확인합니다.

기본값

기본 포트 포워딩 목록은 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.0(2)	명령 모드가 webvpn으로 변경되었습니다.

사용 지침

포트 포워딩은 MAPI(Microsoft Outlook Exchange) 프록시를 지원하지 않습니다. 그러나 Microsoft Outlook Exchange 2010에 대한 스마트 터널 지원을 구성할 수 있습니다.

예

다음은 애플리케이션 예에 사용된 값을 보여줍니다.

애플리케이션	로컬 포트	서버 NDS 이름	원격 포트	설명
IMAP4S e-mail	20143	IMAP4Sserver	143	메일 수신
SMTPS e-mail	20025	SMTPSserver	25	메일 전송
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

다음 예에서는 이러한 애플리케이션에 대한 액세스를 제공하는 *SalesGroupPorts*라는 포트 포워딩 목록을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
ciscoasa(config-webvpn)# port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
ciscoasa(config-webvpn)# port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
ciscoasa(config-webvpn)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

관련 명령

명령	설명
port-forward auto-start	이 명령은 그룹 정책 webvpn 또는 사용자 이름 webvpn 모드로 들어가서 자동으로 포트 포워딩을 시작하고, 사용자가 클라이언트리스 SSL VPN 세션에 로그인할 때 지정된 포트 포워딩 목록을 할당합니다.
port-forward enable	이 명령은 그룹 정책 webvpn 또는 사용자 이름 webvpn 모드로 들어가서 사용자가 로그인할 때 지정된 포트 포워딩 목록을 할당합니다. 그러나 사용자는 클라이언트리스 SSL VPN 포털 페이지에서 **Application Access > Start Applications** 버튼을 사용하여 포트 포워딩을 수동으로 시작해야 합니다.
port-forward disable	이 명령은 그룹 정책 webvpn 또는 사용자 이름 webvpn 모드로 들어가서 포트 포워딩을 끕니다.

port-forward-name

특정 사용자 또는 그룹 정책에서 엔드 유저에 대한 TCP 포트 포워딩을 식별하는 표시 이름을 구성하려면 그룹 정책 또는 사용자 이름 모드에서 들어가는 webvpn 모드에서 **port-forward-name** 명령을 사용합니다. **port-forward-name none** 명령을 사용하여 만드는 null 값을 포함하여 표시 이름을 삭제하려면 이 명령의 no 형식을 사용합니다. **no** 옵션은 기본 이름인 "Application Access"를 복원합니다. 표시 이름을 차단하려면 **port-forward none** 명령을 사용합니다.

port-forward-name {**value** *name* | **none**}

no port-forward-name

구문 설명

none	표시 이름이 없음을 나타냅니다. Null 값을 설정하여 표시 이름을 허용하지 않습니다. 값의 상속을 차단합니다.
value *name*	엔드 유저에 대한 포트 포워딩을 설명합니다. 최대 255자.

기본값

기본 이름은 "Application Access"입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 그룹 정책 FirstGroup에 대해 "Remote Access TCP Applications"라는 이름을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

관련 명령

명령	설명
webvpn	그룹 정책 컨피그레이션 모드 또는 사용자 이름 컨피그레이션 모드에서 사용합니다. 사용자는 webvpn 모드로 들어가서 그룹 정책 또는 사용자 이름에 적용되는 매개변수를 구성할 수 있습니다.
webvpn	글로벌 컨피그레이션 모드에서 사용합니다. WebVPN용 전역 설정을 구성할 수 있습니다.

port-object

TCP, UDP 또는 TCP-UDP 유형의 서비스 객체 그룹에 포트 객체를 추가하려면 객체 그룹 서비스 컨피그레이션 모드에서 **port-object** 명령을 사용합니다. 포트 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

port-object {**eq** *port* | **range** *begin_port end_port*}

no port-object {**eq** *port* | **range** *begin_port end_port*}

구문 설명

range *begin_port end_port*	0~65535의 포트 범위(포함)를 지정합니다.
eq *port*	서비스 객체의 TCP 또는 UDP 포트에 대해 이름을 지정하거나 십진수 번호(0~65535)를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
객체 네트워크 서비스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

특정 포트 또는 포트의 범위인 객체를 정의하려면 **port-object** 명령을 **object-group service** *protocol* 명령과 함께 사용합니다.

TCP 또는 UDP 서비스에 대해 이름을 지정하는 경우 해당 이름은 지원되는 TCP 및/또는 UDP 이름 중 하나여야 하며, 객체 그룹의 프로토콜 유형과 일치해야 합니다. 예를 들어 tcp, udp 및 tcp-udp 프로토콜 유형의 경우 이름은 각각 유효한 TCP 서비스 이름, 유효한 UDP 서비스 이름, 유효한 TCP 및 UDP 서비스 이름이어야 합니다.

번호를 지정하는 경우 객체를 표시할 때 프로토콜 유형 기반으로 해당 이름(있는 경우)에 대한 변환이 수행됩니다.

다음의 서비스 이름이 지원됩니다.

TCP	UDP	TCP 및 UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
HTTP	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
POP3		
SMTP		
sqlnet		
telnet		
uucp		
whois		
www		

예

다음 예는 서비스 컨피그레이션 모드에서 **port-object** 명령을 사용하여 새 포트(서비스) 객체 그룹을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service)# port-object eq smtp
ciscoasa(config-service)# port-object eq telnet
ciscoasa(config)# object-group service eng_service udp
ciscoasa(config-service)# port-object eq snmp
ciscoasa(config)# object-group service eng_service tcp-udp
ciscoasa(config-service)# port-object eq domain
ciscoasa(config-service)# port-object range 2000 2005
ciscoasa(config-service)# quit
```

관련 명령

명령	설명
clear configure object-group	컨피그레이션에서 모든 **object-group** 명령을 제거합니다.
group-object	네트워크 객체 그룹을 추가합니다.
network-object	네트워크 객체를 네트워크 객체 그룹에 추가합니다.
object-group	컨피그레이션을 최적화하기 위해 객체 그룹을 정의합니다.
show running-config object-group	현재 객체 그룹을 표시합니다.

portal-access-rule

고객은 이 명령을 사용하여 HTTP 헤더에 있는 데이터를 기반으로 클라이언트 SSL VPN 세션을 허용 또는 거부하도록 전역 클라이언트리스 SSL VPN 액세스 정책을 구성할 수 있습니다. 거부되면 오류 코드가 클라이언트로 반환됩니다. 이러한 거부는 사용자 인증 전에 수행되므로 처리 리소스의 사용이 최소화됩니다.

portal-access-rule none

portal-access-rule *priority* **[{permit | deny [code** *code*]**} {any | user-agent match** *string*}

no portal-access-rule *priority* **[{permit | deny [code** *code*]**} {any | user-agent match** *string*}]

clear configure webvpn portal-access-rule

구문 설명

none	모든 포털 액세스 규칙을 제거합니다. 클라이언트리스 SSL VPN 세션은 HTTP 헤더를 기반으로 제한되지 않습니다.
priority	규칙의 우선순위. 범위: 1~65535.
permit	HTTP 헤더를 기반으로 액세스를 허용합니다.
deny	HTTP 헤더를 기반으로 액세스를 거부합니다.
code	반환된 HTTP 상태 코드를 기반으로 액세스를 허용 또는 거부합니다. 기본값: 403.
code	액세스를 허용 또는 거부하기 위한 기반이 되는 HTTP 상태 코드 번호. 범위: 200~599.
any	HTTP 헤더 문자열을 확인합니다.
user-agent match	HTTP 헤더에서 문자열 비교를 활성화합니다.
string	HTTP 헤더에서 확인할 문자열을 지정합니다. 문자열이 포함된 일치 내용을 찾으려면 검색하는 문자열을 와일드카드(*)로 둘러쌉니다. 문자열과 정확히 일치하는 내용을 지정하려면 와일드카드를 사용하지 않습니다. **참고** 검색 문자열에서 와일드카드를 사용하는 것이 좋습니다. 와일드카드를 사용하지 않으면 규칙과 일치하는 문자열이 없거나 예상보다 훨씬 적을 수 있습니다. 검색하는 문자열에 공백이 있는 경우 큰따옴표로 둘러싸야 합니다(예: "*a string*"). 큰따옴표와 와일드카드를 함께 사용하는 경우 "**a string**"처럼 검색 문자열을 사용할 수 있습니다.
no portal-access-rule	단일 portal-access-rule을 삭제하기 위해 사용합니다.
clear configure webvpn portal-access-rule	portal-access-rule none 명령과 같습니다.

기본값

portal-access-rule none

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

명령 모드	방화벽 모드		보안 컨텍스트		
	라우팅	투명성	단일	다중 컨텍스트	다중 시스템
webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(5)	ASA 8.2.5 및 8.4(2)에서 동시에 이 명령이 추가되었습니다.
8.4(2)	ASA 8.2.5 및 8.4(2)에서 동시에 이 명령이 추가되었습니다.

사용 지침

이 점검은 사용자 인증 전에 수행됩니다.

예

다음 예는 세 가지 포털 액세스 규칙을 생성합니다.

- 포털 액세스 규칙 1은 ASA가 코드 403을 반환하고 HTTP 헤더에 Thunderbird가 있는 경우 클라이언트리스 SSL VPN 연결 시도를 거부합니다.
- 포털 액세스 규칙 10은 HTTP 헤더에 MSIE 8.0(Microsoft Internet Explorer 8.0)이 있는 경우 클라이언트리스 SSL VPN 연결 시도를 거부합니다.
- 포털 액세스 규칙 65535는 기타 모든 클라이언트리스 SSL VPN 연결을 허용합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
ciscoasa(config-webvpn)# portal-access-rule 10 permit user-agent match "*MSIE 8.0*"
ciscoasa(config-webvpn)# portal-access-rule 65535 permit any
```

관련 명령

명령	설명
show run webvpn	모든 portal-access-rule이 포함된 webvpn 컨피그레이션을 표시합니다.
show vpn-sessiondb detail webvpn	VPN 세션에 대한 정보를 표시합니다. 이 명령은 전체 정보 또는 상세 정보 표시를 위한 옵션을 포함하며, 표시할 세션 유형을 지정하도록 허용하고, 정보의 필터링과 정렬을 위한 옵션을 제공합니다.
debug webvpn request *n*	특정 디버깅 수준에서 디버깅 메시지의 로깅을 활성화합니다. 기본값: 1. 범위: 1~255.

post-max-size

게시할 객체에 허용되는 최대 크기를 지정하려면 그룹 정책 webvpn 컨피그레이션 모드에서 **post-max-size** 명령을 사용합니다. 컨피그레이션에서 이 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

post-max-size <*size*>

no post-max-size

구문 설명

size	게시되는 객체에 허용되는 최대 크기를 지정합니다. 범위는 0~2147483647입니다.

기본값

기본 크기는 2147483647입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Group-policy webvpn 컨피그레이션 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

크기를 0으로 설정하면 객체 게시를 효과적으로 거부할 수 있습니다.

예

다음 예는 게시되는 객체의 최대 크기를 1500바이트로 설정합니다.

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# post-max-size 1500
```

관련 명령

명령	설명
download-max-size	다운로드할 객체의 최대 크기를 지정합니다.
upload-max-size	업로드할 객체의 최대 크기를 지정합니다.
webvpn	그룹 정책 컨피그레이션 모드 또는 사용자 이름 컨피그레이션 모드에서 사용합니다. 사용자는 webvpn 모드로 들어가서 그룹 정책 또는 사용자 이름에 적용되는 매개변수를 구성할 수 있습니다.
webvpn	글로벌 컨피그레이션 모드에서 사용합니다. WebVPN용 전역 설정을 구성할 수 있습니다.

pppoe client route distance

PPPoE를 통해 학습하는 경로에 대한 관리 거리를 구성하려면 인터페이스 컨피그레이션 모드에서 **pppoe client route distance** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

pppoe client route distance *distance*

no pppoe client route distance *distance*

구문 설명

distance	PPPoE를 통해 학습하는 경로에 적용할 관리 거리. 유효한 값은 1~255입니다.

기본값

PPPoE를 통해 학습하는 경로에는 기본적으로 관리 거리 1이 지정됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

PPPoE에서 경로를 학습하는 경우에만 **pppoe client route distance** 명령이 점검됩니다. PPPoE에서 경로를 학습한 후 **pppoe client route distance** 명령을 입력하면, 기존의 학습된 경로에는 지정된 관리 거리가 적용되지 않습니다. 지정된 관리 거리는 명령을 입력한 후에 학습되는 경로에만 적용됩니다.

PPPoE를 통해 경로를 얻으려면 **ip address pppoe** 명령에서 **setroute** 옵션을 지정해야 합니다.

PPPoE를 여러 인터페이스에 구성하는 경우 각 인터페이스에서 **pppoe client route distance** 명령을 사용하여 설치된 경로의 우선순위를 지정해야 합니다. 여러 인터페이스에서 PPPoE 클라이언트를 활성화하는 것은 객체 추적에서만 지원됩니다.

PPPoE를 사용하여 IP 주소를 얻는 경우 장애 조치를 구성할 수 없습니다.

예

다음 예는 GigabitEhternet0/2에서 PPPoE를 통해 기본 경로를 얻습니다. 엔트리 객체 1을 추적하여 경로가 추적됩니다. SLA 작업은 외부 인터페이스로부터 10.1.1.1 게이트웨이의 가용성을 모니터링합니다. SLA 작업이 실패하면 PPPoE를 통해 GigabitEthernet0/3에서 얻은 보조 경로가 사용됩니다.

```
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
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

관련 명령

명령	설명
ip address pppoe	PPPoE를 통해 얻은 IP 주소로 지정된 인터페이스를 구성합니다.
ppoe client secondary	보조 PPPoE 클라이언트 인터페이스에 대한 추적을 구성합니다.
pppoe client route track	PPPoE를 통해 학습한 경로를 추적 엔트리 객체와 연결합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.
track rtr	SLA를 폴링하기 위한 추적 엔트리를 만듭니다.

pppoe client route track

추가된 경로를 지정된 추적 객체 번호와 연결하도록 PPPoE 클라이언트를 구성하려면 인터페이스 컨피그레이션 모드에서 **pppoe client route track** 명령을 사용합니다. PPPoE 경로 추적을 제거하려면 이 명령의 **no** 형식을 사용합니다.

pppoe client route track *number*

no pppoe client route track

구문 설명

number	추적 엔트리 객체 ID. 유효한 값은 1~500입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

PPPoE에서 경로를 학습하는 경우에만 **pppoe client route track** 명령이 점검됩니다. PPPoE에서 경로를 학습한 후 **pppoe client route track** 명령을 입력하면, 기존의 학습된 경로가 추적 객체와 연결되지 않습니다. 명령을 입력한 후에 학습되는 경로만 지정된 추적 객체와 연결됩니다.

PPPoE를 통해 경로를 얻으려면 **ip address pppoe** 명령에서 **setroute** 옵션을 지정해야 합니다.

PPPoE를 여러 인터페이스에 구성하는 경우 각 인터페이스에서 **pppoe client route distance** 명령을 사용하여 설치된 경로의 우선순위를 지정해야 합니다. 여러 인터페이스에서 PPPoE 클라이언트를 활성화하는 것은 객체 추적에서만 지원됩니다.

PPPoE를 사용하여 IP 주소를 얻는 경우 장애 조치를 구성할 수 없습니다.

예

다음 예는 GigabitEhternet0/2에서 PPPoE를 통해 기본 경로를 얻습니다. 엔트리 객체 1을 추적하여 경로가 추적됩니다. SLA 작업은 외부 인터페이스로부터 10.1.1.1 게이트웨이의 가용성을 모니터링합니다. SLA 작업이 실패하면 PPPoE를 통해 GigabitEthernet0/3에서 얻은 보조 경로가 사용됩니다.

```
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
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

관련 명령

명령	설명
ip address pppoe	PPPoE를 통해 얻은 IP 주소로 지정된 인터페이스를 구성합니다.
ppoe client secondary	보조 PPPoE 클라이언트 인터페이스에 대한 추적을 구성합니다.
pppoe client route distance	PPPoE를 통해 학습하는 경로에 관리 거리를 할당합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.
track rtr	SLA를 폴링하기 위한 추적 엔트리를 만듭니다.

pppoe client secondary

추적 객체의 클라이언트로서 등록하고 추적 상태를 기반으로 작동 여부가 결정되도록 PPPoE 클라이언트를 구성하려면 인터페이스 컨피그레이션 모드에서 **pppoe client secondary** 명령을 사용합니다. 클라이언트 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

pppoe client secondary track *number*

no pppoe client secondary track

구문 설명

number	추적 엔트리 객체 ID. 유효한 값은 1~500입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

PPPoE 세션이 시작된 경우에만 **pppoe client secondary** 명령이 점검됩니다. PPPoE에서 경로를 학습한 후 **pppoe client route track** 명령을 입력하면, 기존의 학습된 경로가 추적 객체와 연결되지 않습니다. 명령을 입력한 후에 학습되는 경로만 지정된 추적 객체와 연결됩니다.

PPPoE를 통해 경로를 얻으려면 **ip address pppoe** 명령에서 **setroute** 옵션을 지정해야 합니다.

PPPoE를 여러 인터페이스에 구성하는 경우 각 인터페이스에서 **pppoe client route distance** 명령을 사용하여 설치된 경로의 우선순위를 지정해야 합니다. 여러 인터페이스에서 PPPoE 클라이언트를 활성화하는 것은 객체 추적에서만 지원됩니다.

PPPoE를 사용하여 IP 주소를 얻는 경우 장애 조치를 구성할 수 없습니다.

예

다음 예는 GigabitEhternet0/2에서 PPPoE를 통해 기본 경로를 얻습니다. 엔트리 객체 1을 추적하여 경로가 추적됩니다. SLA 작업은 외부 인터페이스로부터 10.1.1.1 게이트웨이의 가용성을 모니터링합니다. SLA 작업이 실패하면 PPPoE를 통해 GigabitEthernet0/3에서 얻은 보조 경로가 사용됩니다.

```
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
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute

ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

관련 명령

명령	설명
ip address pppoe	PPPoE를 통해 얻은 IP 주소로 지정된 인터페이스를 구성합니다.
ppoe client secondary	보조 PPPoE 클라이언트 인터페이스에 대한 추적을 구성합니다.
pppoe client route distance	PPPoE를 통해 학습하는 경로에 관리 거리를 할당합니다.
pppoe client route track	PPPoE를 통해 학습한 경로를 추적 엔트리 객체와 연결합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.

17 장

pre-fill-username through pwd 명령

pre-fill-username

인증 및 권한 부여에 사용할 클라이언트 인증서에서 사용자 이름을 추출하는 기능을 활성화하려면 tunnel-group webvpn-attributes 모드에서 **pre-fill-username** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

pre-fill-username {**ssl-client** | **clientless**}

no pre-fill-username

구문 설명

ssl-client	AnyConnect VPN 연결을 위해 이 기능을 활성화합니다.
clientless	클라이언트리스 연결을 위해 이 기능을 활성화합니다.

기본값

기본값 또는 동작이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group webvpn-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(4)	이 명령이 추가되었습니다.

사용 지침

pre-fill-username 명령은 **username-from-certificate** 명령에서 지정한 인증서 필드에서 추출된 사용자 이름을 username/password 인증 및 권한 부여용 사용자 이름으로서 사용하는 기능을 활성화합니다. 인증서에서 사용자 이름을 미리 채우는 이 기능을 사용하려면 두 명령을 모두 구성해야 합니다.

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

참고 릴리스 8.0.4 및 8.1.2에서는 사용자 이름이 미리 채워지지 않습니다. 대신 사용자 이름 필드에 전송된 데이터가 무시됩니다.

예

다음 예(글로벌 컨피그레이션 모드에서 입력)는 remotegrp라는 IPsec 원격 액세스 터널 그룹을 만들고, SSL VPN 클라이언트에 대한 인증 또는 권한 부여용 이름이 디지털 인증서에서 파생되도록 지정합니다.

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

관련 명령

명령	설명
pre-fill-username	사용자 이름 미리 채우기 기능을 활성화합니다.
show running-config tunnel-group	지정한 터널 그룹 컨피그레이션을 보여줍니다.
tunnel-group general-attributes	명명된 터널 그룹에 대한 일반 특성을 지정합니다.
username-from-certificate	권한 부여용 사용자 이름으로 사용할 인증서의 필드를 지정합니다.

preempt

우선순위가 더 높은 유닛이 부팅 시 활성화되도록 지정하려면 장애 조치 그룹 컨피그레이션 모드에서 **preempt** 명령을 사용합니다. 선점을 제거하려면 이 명령의 **no** 형식을 사용합니다.

preempt [*delay*]

no preempt [*delay*]

구문 설명

seconds	피어가 선점되기까지의 대기 시간(초). 유효한 값은 1~1200초입니다.

기본값

기본적으로 지연이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
장애 조치 그룹 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

장애 조치 그룹에 제1 또는 제2 우선순위를 할당하면 두 유닛이 동시에 부팅할 경우(unit polltime 내에서) 장애 조치 그룹이 어떤 유닛에서 액티브 상태가 될지를 지정하게 됩니다. 한 유닛이 다른 유닛보다 먼저 부팅될 경우 두 장애 조치 그룹 모두 해당 유닛에서 액티브 상태가 됩니다. 다른 유닛이 온라인 상태가 되면, 장애 조치 그룹을 **preempt** 명령으로 구성하지 않은 경우 또는 **no failover active** 명령으로 다른 유닛에 수동으로 할당하지 않은 경우 두 번째 유닛을 우선순위로 가지고 있는 모든 장애 조치 그룹은 두 번째 유닛에서 액티브 상태가 되지 않습니다. **preempt** 명령으로 구성한 장애 조치 그룹은 지정된 유닛에서 자동으로 액티브 상태가 됩니다.

참고 스테이트풀 장애 조치를 사용할 경우, 장애 조치 그룹이 현재 액티브 상태로 있는 유닛에서 연결이 복제될 때까지 사전 대응이 지연됩니다.

예

다음 예는 failover group 1을 우선순위가 더 높은 기본 유닛으로 구성하고 failover group 2를 우선순위가 더 높은 보조 유닛으로 구성합니다. 두 장애 조치 그룹이 대기 시간 100의 **preempt** 명령으로 구성되므로, 두 그룹은 유닛이 사용 가능해지면 100초 후 기본 설정 유닛에서 자동으로 액티브 상태가 됩니다.

```
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	액티브/액티브 장애 조치에 대한 장애 조치 그룹을 정의합니다.
primary	구성하는 장애 조치 그룹에 대해 장애 조치 쌍 우선순위에서 기본 유닛을 제공합니다.
secondary	구성하는 장애 조치 그룹에 대해 장애 조치 쌍 우선순위에서 보조 유닛을 제공합니다.

prefix-list

OSPFv2, EIGRP 및 BGP 프로토콜은 모두 글로벌 컨피그레이션 모드에서 **prefix-list** 명령을 사용합니다. 접두사 목록 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

no prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

구문 설명

/	*network* 및 *len* 값 사이의 필수 구분 기호.
deny	일치 조건에 대한 액세스를 거부합니다.
ge *min_value*	(선택 사항) 확인할 최소 접두사 길이를 지정합니다. *min_value* 인수의 값은 *len* 인수의 값보다 커야 하며 *max_value* 인수(있는 경우)보다 작거나 같아야 합니다.
le *max_value*	(선택 사항) 확인할 최대 접두사 길이를 지정합니다. *max_value* 인수의 값은 *min_value* 인수(있는 경우)의 값보다 크거나 같아야 하며, *min_value* 인수가 없는 경우에는 *len* 인수의 값보다 커야 합니다.
len	네트워크 마스크의 길이. 유효한 값은 0~32입니다.
network	네트워크 주소.
permit	일치 조건에 대한 액세스를 허용합니다.
prefix-list-name	접두사 목록의 이름. 접두사 목록의 이름에는 공백을 포함할 수 없습니다.
seq *seq_num*	(선택 사항) 지정된 순차 번호를 생성 중인 접두사 목록에 적용합니다.

기본값

순차 번호를 지정하지 않으면 접두사 목록의 첫 번째 엔트리에는 순차 번호 5가 할당되고, 각각의 다음 엔트리에 대한 순차 번호는 5씩 증가합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.
9.2(1)	BGP에 대한 지원이 추가되었습니다.

사용 지침

prefix-list 명령은 ABR Type 3 LSA 필터링 명령입니다. ABR Type 3 LSA 필터링은 OSPF를 실행하여 서로 다른 OSPF 영역 간 Type 3 LSA를 필터링하는 ABR의 기능을 확장합니다. 일단 접두사 목록이 구성되면 지정된 접두사만 하나의 영역에서 다른 영역으로 전송됩니다. 모든 다른 접두사는 OSPF 영역으로 제한됩니다. 이 영역 필터링 유형을 OSPF 영역에서 수신 또는 발신 트래픽에 적용하거나 해당 영역의 수신 및 발신 트래픽 모두에 적용할 수 있습니다.

접두사 목록의 여러 엔트리가 주어진 접두사와 일치하는 경우 순차 번호가 가장 낮은 엔트리가 사용됩니다. ASA는 접두사 목록의 맨 위에서 순차 번호가 가장 낮은 엔트리로 검색을 시작합니다. 일치가 발견되면 ASA는 목록의 나머지를 진행하지 않습니다. 목록 상단 근처의 가장 일반적인 일치 또는 거부에 가장 낮은 순차 번호를 할당하는 것이 효율적일 수 있습니다.

기본적으로 순차 번호는 자동으로 생성되며, **no prefix-list sequence-number** 명령으로 억제할 수 있습니다. 순차 번호는 5씩 증가하며 생성됩니다. 접두사 목록에서 생성되는 첫 번째 순차 번호는 5이고, 해당 목록에서 다음 엔트리의 순차 번호는 10이며, 이와 같이 진행됩니다. 한 엔트리에 대한 값을 지정한 다음 이후 엔트리에 대한 값을 지정하지 않으면, 지정된 값에서 5씩 증가하며 순차 번호가 생성됩니다. 예를 들어, 접두사 목록의 첫 번째 항목에 대해 순차 번호 3을 지정한 다음 순차 번호를 지정하지 않은 채 두 개의 엔트리를 더 추가하면 이 두 엔트리에 대해 순차 번호 8과 13이 자동으로 생성됩니다.

접두사에 대해 확인할 접두사 길이의 범위를 지정하려면 **ge** 및 **le** 키워드를 사용할 수 있습니다. 이 두 인수가 *network/len* 인수보다 좀 더 구체적입니다. **ge** 또는 **le** 키워드를 둘 다 지정하지 않으면 정확한 일치로 간주됩니다. **ge** 키워드만 지정하면 범위는 *min_value*~32이고, **le** 키워드만 지정하면 범위는 *len~max_value*입니다.

min_value 및 *max_value* 인수의 값은 다음 조건을 충족해야 합니다.

len < *min_value* <= *max_value* <= 32

접두사 목록에서 특정 엔트리를 제거하려면 명령의 **no** 형식을 사용합니다. 접두사 목록을 제거하려면 **clear configure prefix-list** 명령을 사용합니다. clear **configure prefix-list** 명령 역시 관련된 **prefix-list description** 명령(있는 경우)을 컨피그레이션에서 제거합니다.

예

다음 예는 기본 경로 0.0.0.0/0을 거부합니다.

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0
```

다음 예는 접두사 0.0.0.0/8을 허용합니다.

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
```

다음 예는 접두사 192/8의 경로에서 최대 24비트의 마스크 길이를 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

다음 예는 접두사 192/8의 경로에서 25비트보다 큰 마스크 길이를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

다음 예는 모든 주소 공간에서 8~24비트의 마스크 길이를 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

다음 예는 모든 주소 공간에서 25비트보다 큰 마스크 길이를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

다음 예는 접두사 10/8의 모든 경로를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

다음 예는 접두사 192.168.1/24의 경로에서 길이가 25비트보다 큰 모든 마스크를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

다음 예는 접두사 0/0의 모든 경로를 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

관련 명령

명령	설명
clear configure prefix-list	실행 중인 컨피그레이션에서 **prefix-list** 명령을 제거합니다.
prefix-list description	접두사 목록에 대한 설명을 입력할 수 있습니다.
prefix-list sequence-number	접두사 목록 순차 번호 지정을 활성화합니다.
show running-config prefix-list	실행 중인 컨피그레이션에서 **prefix-list** 명령을 표시합니다.

prefix-list description

접두사 목록에 설명을 추가하려면 글로벌 컨피그레이션 모드에서 **prefix-list description** 명령을 사용합니다. 접두사 목록 설명을 제거하려면 이 명령의 **no** 형식을 사용합니다.

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

구문 설명

prefix-list-name	접두사 목록의 이름.
text	접두사 목록 설명의 텍스트. 최대 80자를 입력할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

특별한 접두사 목록 이름에 대해 **prefix-list** 및 **prefix-list description** 명령을 임의의 순서로 입력할 수 있습니다. 접두사 목록 설명을 입력하기 전에 접두사 목록을 만들어야 할 필요는 없습니다. 명령을 어떤 순서로 입력하든, **prefix-list description** 명령은 항상 컨피그레이션에서 관련된 접두사 목록 이전의 줄에 나타납니다.

이미 설명이 있는 접두사 목록 엔트리에 대해 **prefix-list description** 명령을 입력하면 새 설명이 원래 설명을 대체합니다.

이 명령의 **no** 형식을 사용할 경우에는 텍스트 설명을 입력할 필요가 없습니다.

예

다음 예는 MyPrefixList라는 접두사 목록에 대한 설명을 추가합니다. **show running-config prefix-list** 명령은, 실행 중인 컨피그레이션에 접두사 목록 설명이 추가되었지만 접두사 목록 자체는 구성되지 않았음을 보여줍니다.

```
ciscoasa(config)# prefix-list MyPrefixList description A sample prefix list description
ciscoasa(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
!
```

관련 명령

명령	설명
clear configure prefix-list	실행 중인 컨피그레이션에서 **prefix-list** 명령을 제거합니다.
prefix-list	ABR Type 3 LSA 필터링용 접두사 목록을 정의합니다.
show running-config prefix-list	실행 중인 컨피그레이션에서 **prefix-list** 명령을 표시합니다.

prefix-list sequence-number

접두사 목록 순차 번호 지정을 활성화하려면 글로벌 컨피그레이션 모드에서 **prefix-list sequence-number** 명령을 사용합니다. 접두사 목록 순차 번호 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

prefix-list sequence-number

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

접두사 목록 순차 번호 지정은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

컨피그레이션에는 이 명령의 **no** 형식만 나타납니다. 컨피그레이션에 이 명령의 **no** 형식이 있으면 컨피그레이션의 **prefix-list** 명령에서 순차 번호(수동으로 구성한 것 포함)가 제거되며, 새로운 접두사 목록 엔트리에 순차 번호가 할당되지 않습니다.

접두사 목록 순차 번호 지정이 활성화되어 있으면 기본 번호 지정 방법(5로 시작하여 각 번호가 5씩 증가)을 사용하여 모든 접두사 목록 엔트리에 순차 번호가 할당됩니다. 번호 지정이 비활성화되기 전에 접두사 목록 엔트리에 순차 번호가 수동으로 할당된 경우, 수동으로 할당된 번호가 복원됩니다. 자동 번호 지정이 비활성화되어 있는 동안 수동으로 할당된 순차 번호도 역시 복원됩니다(번호 지정이 비활성화되어 있는 동안에는 표시되지 않음).

예

다음 예는 접두사 목록 순차 번호 지정을 비활성화합니다.

```
ciscoasa(config)# no prefix-list sequence-number
```

관련 명령

명령	설명
prefix-list	ABR Type 3 LSA 필터링용 접두사 목록을 정의합니다.
show running-config prefix-list	실행 중인 컨피그레이션에서 **prefix-list** 명령을 표시합니다.

prf

AnyConnect IPsec 연결을 위한 IKEv2 SA(Security Association)에서 PRF(의사 난수 함수)를 지정하려면 IKEv2 정책 컨피그레이션 모드에서 **prf** 명령을 사용합니다. 이 명령을 제거하고 기본 설정을 사용하려면 이 명령의 **no** 형식을 사용합니다.

prf {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

no prf {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

구문 설명

md5	MD5 알고리즘을 지정합니다.
sha	(기본값) Secure Hash Algorithm SHA 1을 지정합니다.
sha256	256비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha384	384비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.
sha512	512비트 다이제스트로 Secure Hash Algorithm SHA 2를 지정합니다.

기본값

기본값은 **sha**(SHA 1)입니다.

사용 지침

IKEv2 SA는 IKEv2 피어가 phase 2에서 안전하게 통신할 수 있도록 phase 1에서 사용되는 키입니다. **crypto ikev2 policy** 명령을 입력한 후 **prf** 명령을 사용하여 SA에서 사용되는 모든 암호화 알고리즘에 대한 키 관련 자료 구성에 사용되는 의사 난수 함수를 선택합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.
8.4(2)	SHA 2 지원을 위해 **sha256**, **sha384** 및 **sha512** 키워드가 추가되었습니다.

예

다음 예는 IKEv2 정책 컨피그레이션 모드로 들어가서 PRF를 MD5로 설정합니다.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# prf md5
```

관련 명령

명령	설명
encryption	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 암호화 알고리즘을 지정합니다.
group	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 Diffie-Hellman 그룹을 지정합니다.
integrity	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 ESP 무결성 알고리즘을 지정합니다.
lifetime	AnyConnect IPsec 연결을 위한 IKEv2 SA에서 SA 수명을 지정합니다.

primary

기본 유닛에 장애 조치 그룹을 위한 더 높은 우선순위를 지정하려면 장애 조치 그룹 컨피그레이션 모드에서 **primary** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

primary

no primary

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

장애 조치 그룹에 대해 **primary** 또는 **secondary**를 지정하지 않으면 장애 조치 그룹 기본값은 **primary**가 됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
장애 조치 그룹 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

장애 조치 그룹에 제1 또는 제2 우선순위를 할당하면 두 유닛이 동시에 부팅할 경우(unit polltime 내에서) 장애 조치 그룹이 어떤 유닛에서 액티브 상태가 될지를 지정하게 됩니다. 한 유닛이 다른 유닛보다 먼저 부팅될 경우, 기본 또는 보조 설정에 관계없이 두 장애 조치 그룹 모두 해당 유닛에서 액티브 상태가 됩니다. 다른 유닛이 온라인 상태가 되면, 장애 조치 그룹을 **preempt** 명령으로 구성하지 않은 경우 또는 **no failover active** 명령으로 다른 유닛에 수동으로 할당하지 않은 경우 두 번째 유닛을 우선순위로 가지고 있는 모든 장애 조치 그룹은 두 번째 유닛에서 액티브 상태가 되지 않습니다.

예

다음 예는 failover group 1을 우선순위가 더 높은 기본 유닛으로 구성하고 failover group 2를 우선순위가 더 높은 보조 유닛으로 구성합니다. 두 장애 조치 그룹이 **preempt** 명령으로 구성되므로, 두 그룹은 유닛이 사용 가능해지면 기본 설정 유닛에서 자동으로 액티브 상태가 됩니다.

```
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	액티브/액티브 장애 조치에 대한 장애 조치 그룹을 정의합니다.
preempt	유닛이 사용 가능해지면 장애 조치 그룹이 기본 설정 유닛에서 액티브 상태가 되도록 지정합니다.
secondary	보조 유닛에 기본 유닛보다 더 높은 우선순위를 제공합니다.

priority(class)

QoS 우선순위 큐잉을 활성화하려면 클래스 컨피그레이션 모드에서 **priority**명령을 사용합니다. VoIP(Voice over IP)와 같이 레이턴시가 허용되지 않는 중요한 트래픽의 경우, 항상 최저 속도로 전송되도록 LLQ(Low Latency Queuing)에 대한 트래픽을 식별할 수 있습니다. 우선순위 요구 사항을 제거하려면 이 명령의 **no** 형식을 사용합니다.

참고 ASA Services Module에서는 이 명령이 지원되지 않습니다.

priority

no priority

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 변수가 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

LLQ 우선순위 큐잉은 다른 트래픽에 앞서 특정 트래픽 흐름(예: 음성과 비디오 등 레이턴시에 민감한 트래픽)에 우선순위를 지정하도록 허용합니다.

ASA는 두 가지 유형의 우선순위 큐잉을 지원합니다.

- 표준 우선순위 큐잉 - 표준 우선순위 큐잉은 인터페이스에서 LLQ 우선순위 큐를 사용하는 반면(**priority-queue** 명령 참조), 다른 모든 트래픽은 "BE(Best Effort)" 큐로 들어갑니다. 큐의 크기는 무한하지 않으므로 가득 차서 오버플로될 수 있습니다. 큐가 가득 차면 해당 큐로 추가 패킷이 들어갈 수 없어 삭제됩니다. 이를 *tail drop*이라고 합니다. 큐가 가득 차는 것을 막으려면 큐 버퍼 크기를 늘릴 수 있습니다. 또한 전송 큐에 대해 허용되는 패킷의 최대 수를 조정할 수 있습니다. 이러한 옵션을 통해 우선순위 큐잉의 레이턴시와 안정성을 제어할 수 있습니다. LLQ 큐에 있는 패킷은 항상 BE 큐에 있는 패킷보다 먼저 전송됩니다.

- 계층형 우선순위 큐잉 - 계층형 우선순위 큐잉은 트래픽 셰이핑 큐(**shape** 명령)를 활성화하는 인터페이스에서 사용됩니다. 셰이핑된 트래픽의 하위 집합에 대해 우선순위를 지정할 수 있습니다. 표준 우선순위 큐는 사용되지 않습니다. 계층형 우선순위 큐잉에 대한 다음 지침을 참조하십시오.
  - 우선순위 패킷은 항상 셰이프 큐의 맨 위에 추가되기 때문에 , 우선순위가 지정되지 않은 다른 패킷보다 항상 먼저 전송됩니다 .
  - 우선순위 트래픽의 지속 속도가 셰이프 속도를 초과하지 않는 한 우선순위 패킷은 셰이프 큐에서 절대 삭제되지 않습니다 .
  - IPsec 암호화 패킷의 경우 DSCP 또는 우선순위 설정만을 기반으로 트래픽을 확인할 수 있습니다 .
  - IPsec-over-TCP 는 우선순위 트래픽 분류에서 지원되지 않습니다 .

Modular Policy Framework 로 QoS 구성

우선순위 큐잉을 활성화하려면 Modular Policy Framework를 사용하십시오. 표준 우선순위 큐잉 또는 계층형 우선순위 큐잉을 사용할 수 있습니다.

표준 우선순위 큐잉의 경우 다음 작업을 수행합니다.

1. **class-map** - 우선순위 큐잉을 수행할 트래픽을 식별합니다.
2. **policy-map** - 각 클래스 맵과 관련된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **priority** - 클래스 맵에 대해 우선순위 큐잉을 활성화합니다.
3. **service-policy** - 정책 맵을 한 인터페이스에 또는 전체적으로 할당합니다.

계층형 우선순위 큐잉의 경우 다음 작업을 수행합니다.

1. **class-map** - 우선순위 큐잉을 수행할 트래픽을 식별합니다.
2. **policy-map**(우선순위 큐잉의 경우) - 각 클래스 맵과 관련된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **priority** - 클래스 맵에 대해 우선순위 큐잉을 활성화합니다. 계층형으로 사용하려는 경우 이 정책 맵에 우선순위 명령만 포함할 수 있습니다.
3. **policy-map**(트래픽 셰이핑의 경우) - **class-default** 클래스 맵과 관련된 작업을 식별합니다.
   a. **class class-default** - 작업을 수행할 **class-default** 클래스 맵을 식별합니다.
   b. **shape** - 클래스 맵에 트래픽 셰이핑을 적용합니다.
   c. **service-policy** - 우선순위 큐잉을 셰이핑된 트래픽의 하위 집합에 적용할 수 있도록 **priority** 명령으로 구성한 우선순위 큐잉 정책 맵을 호출합니다.
4. **service-policy** - 정책 맵을 한 인터페이스에 또는 전체적으로 할당합니다.

예

다음은 정책 맵 컨피그레이션 모드에서 **priority** 명령을 사용하는 예입니다.

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class firstclass
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

관련 명령

class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
clear configure policy-map	모든 정책 맵 구성을 제거합니다. 단, 정책 맵이 서비스 정책 명령에서 사용되고 있는 경우 해당 정책 맵은 제거되지 않습니다.
policy-map	트래픽 클래스 및 하나 이상의 작업을 결합한 정책을 구성합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

priority(cluster group)

ASA 클러스터에서 마스터 유닛을 선택하기 위해 이 유닛의 우선순위를 설정하려면 클러스터 그룹 컨피그레이션 모드에서 **priority** 명령을 사용합니다. 우선순위를 제거하려면 이 명령의 **no** 형식을 사용합니다.

priority *priority_number*

no priority [*priority_number*]

구문 설명

priority_number	마스터 유닛 선택을 위해 이 유닛의 우선순위를 1에서 100까지 설정하며, 1의 우선순위가 가장 높습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

클러스터의 구성원은 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 마스터 유닛을 선택합니다.

1. 유닛에 클러스터링을 사용할 경우(또는 이미 사용 설정된 클러스터링을 처음 시작할 경우), 선택 요청이 3초마다 전송됩니다.
2. 다른 유닛의 우선순위가 더 높을 경우 해당 유닛이 선택 요청에 응답하게 됩니다. 우선순위는 1에서 100까지 설정되며 1이 가장 높은 우선순위입니다.
3. 45초 후에 우선순위가 더 높은 다른 유닛에서 응답을 받지 못한 유닛은 마스터 유닛이 됩니다.

참고 가장 우선순위가 높은 유닛이 공동으로 여러 개인 경우 , 클러스터 유닛 이름과 일련 번호를 사용하여 마스터 유닛을 결정합니다 .

4. 유닛이 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 유닛이 자동으로 마스터 유닛이 되는 것은 아닙니다. 기존 마스터 유닛은 응답이 중지되지 않는 한 항상 마스터 유닛으로 유지되며 응답이 중지될 때에 새 마스터 유닛이 선택됩니다.

참고 유닛을 수동으로 마스터 유닛이 되도록 지정하려면 **cluster master unit** 명령을 사용할 수 있습니다. 중앙 집중식 기능의 경우 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다. 중앙 집중식 기능 목록은 컨피그레이션 가이드를 참조하십시오.

예

다음 예는 우선순위를 1(최고)로 설정합니다.

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용할 경우 ASA에서는 cLACP를 사용하여 EtherChannel과 인접 스위치의 협상을 수행합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드로 들어갑니다.
cluster-interface	클러스터 제어 링크 인터페이스를 지정합니다.
cluster interface-mode	클러스터 인터페이스 모드를 설정합니다.
conn-rebalance	연결 리밸런싱을 활성화합니다.
console-replicate	슬레이브 유닛에서 마스터 유닛으로의 콘솔 복제를 활성화합니다.
enable (cluster group)	클러스터링을 활성화합니다.
health-check	유닛 검사 모니터링 및 인터페이스 상태 모니터링이 포함된 클러스터 상태 검사 기능을 활성화합니다.
key	클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 설정합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스의 최대 전송 유닛을 지정합니다.

priority(vpn load balancing)

가상 로드 밸런싱 클러스터에 참가한 로컬 디바이스의 우선순위를 설정하려면 VPN 로드 밸런싱 모드에서 **priority** 명령을 사용합니다. 기본 우선순위 사양으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

priority *priority*

no priority

구문 설명

priority	이 디바이스에 할당할 우선순위(범위 1~10)

기본값

기본 우선순위는 디바이스의 모델 번호에 따라 다릅니다.

모델 번호	기본 우선순위
5520	5
5540	7

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
VPN 로드 밸런싱	—	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

먼저 **vpn load-balancing** 명령을 사용해야 VPN 로드 밸런싱 모드로 들어갈 수 있습니다.

이 명령은 가상 로드 밸런싱 클러스터에 참가하는 로컬 디바이스의 우선순위를 설정합니다.

우선순위는 1(최저)에서 10(최고)까지의 정수여야 합니다.

우선순위는 마스터 선정 과정에서 VPN 로드 밸런싱 클러스터에 있는 디바이스 중 어떤 디바이스가 클러스터의 마스터 또는 기본 디바이스가 될 것인지를 결정하는 방법 중 하나로서 사용됩니다. 마스터 선정 과정에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

이 명령의 **no** 형식을 사용하면 우선순위 사양이 기본값으로 되돌아갑니다.

예

다음은 현재 디바이스의 우선순위를 9로 설정하는 **priority** 명령이 포함된 VPN 로드 밸런싱 명령 시퀀스의 예입니다.

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
vpn load-balancing	VPN 로드 밸런싱 모드로 들어갑니다.

priority-queue

priority 명령으로 인터페이스에서 사용할 표준 우선순위 큐를 만들려면 글로벌 컨피그레이션 모드에서 **priority-queue** 명령을 사용합니다. 큐를 제거하려면 이 명령의 **no** 형식을 사용합니다.

참고 ASA 5580 Ten Gigabit Ethernet 인터페이스에서는 이 명령이 지원되지 않습니다 (Ten Gigabit Ethernet 인터페이스는 ASA 5585-X의 우선순위 큐에 지원됩니다.). ASA 5512-X~ASA 5555-X 관리 인터페이스에서는 이 명령이 지원되지 않습니다.

ASA Services Module에서는 이 명령이 지원되지 않습니다.

priority-queue *interface-name*

no priority queue *interface-name*

구문 설명

interface-name	우선순위 큐를 활성화할 물리적 인터페이스의 이름(ASA 5505 또는 ASASM의 경우 VLAN 인터페이스의 이름)을 지정합니다.

기본값

기본적으로 우선순위 큐잉은 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.2(3)/8.4(1)	ASA 5585-X에 대한 Ten Gigabit Ethernet 인터페이스의 지원이 추가되었습니다.

사용 지침

LLQ 우선순위 큐잉은 다른 트래픽에 앞서 특정 트래픽 흐름(예: 음성과 비디오 등 레이턴시에 민감한 트래픽)에 우선순위를 지정하도록 허용합니다.

ASA는 두 가지 유형의 우선순위 큐잉을 지원합니다.

- 표준 우선순위 큐잉 - 표준 우선순위 큐잉은 **priority-queue** 명령을 사용하여 만든 인터페이스에서 LLQ 우선순위 큐를 사용하는 반면, 다른 모든 트래픽은 "BE(Best Effort)" 큐로 들어갑니다. 큐의 크기는 무한하지 않으므로 가득 차서 오버플로될 수 있습니다. 큐가 가득 차면 해당 큐로 추가 패킷이 들어갈 수 없어 삭제됩니다. 이를 *tail drop*이라고 합니다. 큐가 가득 차는 것을 막으려면 큐 버퍼 크기를 늘릴 수 있습니다(**queue-limit** 명령). 또한 전송 큐에 대해 허용되는 패킷의 최대 수를 조정할 수 있습니다(**tx-ring-limit** 명령). 이러한 옵션을 통해 우선순위 큐잉의 레이턴시와 안정성을 제어할 수 있습니다. LLQ 큐에 있는 패킷은 항상 BE 큐에 있는 패킷보다 먼저 전송됩니다.
- 계층형 우선순위 큐잉 - 계층형 우선순위 큐잉은 트래픽 셰이핑 큐를 활성화할 인터페이스에서 사용됩니다. 셰이핑된 트래픽의 하위 집합에 대해 우선순위를 지정할 수 있습니다. 표준 우선순위 큐는 사용되지 않습니다.

참고 (ASA 5505 전용) 한 인터페이스에서 우선순위 큐를 구성하는 경우 다른 모든 인터페이스의 동일한 컨피그레이션을 덮어씁니다. 마지막으로 적용한 컨피그레이션이 모든 인터페이스에 사용됩니다. 또한 한 인터페이스에서 우선순위 큐 컨피그레이션을 제거하면 모든 인터페이스에서 제거됩니다. 이 문제를 해결하려면 한 인터페이스에서만 **priority-queue** 명령을 구성하십시오. 인터페이스마다 **queue-limit** 및/또는 **tx-ring-limit** 명령의 서로 다른 설정이 필요한 경우, 모든 큐 제한의 최대값과 모든 tx-ring-limit의 최소값을 어느 한 인터페이스에서 사용하십시오(CSCsi13132).

예

다음 예는 test라는 인터페이스에 대해 우선순위 큐를 구성하면서, 큐 제한은 패킷 30,000개로 지정하고 전송 큐 제한은 패킷 256개로 지정합니다.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 30000
ciscoasa(priority-queue)# tx-ring-limit 256
ciscoasa(priority-queue)#
```

관련 명령

명령	설명
queue-limit	데이터를 삭제하기 전에 우선순위 큐에 추가할 수 있는 최대 패킷 수를 지정합니다.
tx-ring-limit	이더넷 전송 드라이버에서 특정 시간에 큐에 추가할 수 있는 최대 패킷 수를 설정합니다.
policy-map	트래픽 클래스 및 하나 이상의 작업을 결합한 정책을 구성합니다.
clear configure priority-queue	현재의 우선순위 큐 컨피그레이션을 제거합니다.
show running-config [all] priority-queue	현재의 우선순위 큐 컨피그레이션을 표시합니다. **all** 키워드를 지정하면 현재의 우선순위 큐, queue-limit 및 tx-ring-limit 컨피그레이션 값이 모두 표시됩니다.

privilege

명령 권한 부여와 함께 사용할 명령 권한 레벨을 구성하려면(로컬, RADIUS 및 LDAP(매핑됨) 전용) 글로벌 컨피그레이션 모드에서 **privilege** 명령을 사용합니다. 컨피그레이션을 허용하지 않으려면 이 명령의 **no** 형식을 사용합니다.

privilege [**show** | **clear** | **configure**] **level** *level* [**mode** *cli_mode*] **command** *command*

no privilege [**show** | **clear** | **configure**] **level** *level* **mode** *cli_mode*] **command** *command*

구문 설명

clear	(선택 사항) 명령의 clear 형식에 대해서만 권한을 설정합니다. **clear**, **show** 또는 **configure** 키워드를 사용하지 않는 경우 명령의 모든 형식이 영향을 받습니다.
command *command*	구성 중인 명령을 지정합니다. *주(main)* 명령의 권한 레벨만 구성할 수 있습니다. 이를테면 모든 **aaa** 명령의 레벨을 구성할 수 있으나, **aaa authentication** 명령과 **aaa authorization** 명령의 레벨을 각각 구성할 수는 없습니다.
configure	(선택 사항) 명령의 configure 형식에 대해서만 권한을 설정합니다. 명령의 configure 형식은 일반적으로 컨피그레이션 변경을 일으키는 형식으로서 수정되지 않은 명령(**show** 또는 **clear** 접두사 없음)이거나 **no** 형식입니다. **clear**, **show** 또는 **configure** 키워드를 사용하지 않는 경우 명령의 모든 형식이 영향을 받습니다.
level *level*	권한 레벨을 지정합니다. 유효한 값은 0~15입니다. 권한 레벨 숫자가 낮을수록 권한 레벨이 낮습니다.
mode *cli_mode*	(선택 사항) 사용자 EXEC/특별 권한 EXEC 모드, 글로벌 컨피그레이션 모드 또는 명령 컨피그레이션 모드 등 여러 CLI 모드에서 명령을 입력할 수 있는 경우 이러한 모드에 대해 별도로 권한 레벨을 설정할 수 있습니다. 모드를 지정하지 않으면 명령의 모든 버전이 동일한 레벨을 사용합니다. 다음 모드를 참조하십시오. • **enable** - 사용자 EXEC 모드와 특별 권한 EXEC 모드를 모두 지정합니다. • **configure** - **configure terminal** 명령을 사용하여 액세스하는 컨피그레이션 모드를 지정합니다. • *command_config_mode* - 전역 또는 또 다른 명령 컨피그레이션 모드에서 명령 이름을 사용하여 액세스할 수 있는 명령 컨피그레이션 모드를 지정합니다. 예를 들어 **mac-address** 명령은 전역 및 인터페이스 컨피그레이션 모드에서 입력할 수 있습니다. mode 키워드를 사용하면 각 모드에 대한 레벨을 별도로 설정할 수 있습니다. 명령에 대한 레벨을 설정하는 데에는 이 명령을 사용할 수 없습니다.
show	(선택 사항) 명령의 show 형식에 대해서만 권한을 설정합니다. **clear**, **show** 또는 **configure** 키워드를 사용하지 않는 경우 명령의 모든 형식이 영향을 받습니다.

기본값

기본적으로 다음 명령에 권한 레벨 0이 할당됩니다. 다른 모든 명령은 레벨 15입니다.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

어떤 컨피그레이션 모드 명령을 15보다 낮은 레벨로 이동한 경우, 그 **configure** 명령도 그 레벨로 이동해야 합니다. 그러지 않으면 사용자가 컨피그레이션 모드를 시작할 수 없게 됩니다.

모든 권한 레벨을 보려면 **show running-config all privilege all** 명령을 사용합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	Cisco VSA CVPN3000-Privilege-Level의 RADIUS 사용자에 대한 지원이 추가되었습니다. **ldap map-attributes** 명령을 사용하여 LDAP 특성을 CVPN3000-Privilege-Level에 매핑하는 경우 LDAP 사용자가 지원됩니다.

사용 지침

privilege 명령을 사용하면 **aaa authorization command LOCAL** 명령을 구성할 때 ASA 명령에 대해 권한 레벨을 설정할 수 있습니다. 명령에서 **LOCAL** 키워드를 사용하더라도 이 키워드는 로컬, RADIUS 및 LDAP(매핑됨) 권한 부여를 활성화합니다.

예

예를 들어 **filter** 명령의 형식은 다음과 같습니다.

- **filter**(**configure** 옵션으로 표시됨)
- **show running-config filter**
- **clear configure filter**

각 형식의 권한 레벨을 개별적으로 설정하거나, 이 옵션을 생략하여 모든 형식에 동일한 권한 레벨을 설정할 수 있습니다. 예를 들면 각 형식을 다음과 같이 설정합니다.

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

또는 모든 필터 명령을 동일한 레벨로 설정할 수도 있습니다.

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege 명령은 화면에서 형식을 구분합니다.

다음 예는 **mode** 키워드의 사용 방법을 보여줍니다. **enable** 명령은 사용자 EXEC 모드에서 입력해야 하지만, 컨피그레이션 모드에서 액세스 가능한 **enable password** 명령을 사용하려면 최고 권한 레벨이 필요합니다.

```
ciscoasa(config)# privilege cmd level 0 mode exec command enable
ciscoasa(config)# privilege cmd level 15 mode configure command enable
ciscoasa(config)# privilege show level 15 mode configure command enable
```

다음 예는 **mac-address** 명령을 두 가지 모드에서 보여주며 show, clear 및 cmd 버전에 대해 다른 레벨을 보여줍니다.

```
ciscoasa(config)# privilege cmd level 10 mode configure command mac-address
ciscoasa(config)# privilege cmd level 15 mode interface command mac-address
ciscoasa(config)# privilege clear level 10 mode configure command mac-address
ciscoasa(config)# privilege clear level 15 mode interface command mac-address
ciscoasa(config)# privilege show level 2 mode configure command mac-address
ciscoasa(config)# privilege show level 2 mode interface command mac-address
```

관련 명령

명령	설명
clear configure privilege	컨피그레이션에서 권한 명령문을 제거합니다.
show curpriv	현재의 권한 레벨을 표시합니다.
show running-config privilege	명령에 대한 권한 레벨을 표시합니다.

prompt

CLI 프롬프트를 사용자 지정하려면 글로벌 컨피그레이션 모드에서 **prompt** 명령을 사용합니다. 기본 프롬프트로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]

구문 설명

cluster-unit	클러스터 유닛 이름을 표시합니다. 클러스터의 각 유닛은 고유한 이름을 가질 수 있습니다.
context	(다중 모드만) 현재 컨텍스트를 표시합니다.
domain	도메인 이름을 표시합니다.
hostname	호스트 이름을 표시합니다.
priority	장애 조치 우선순위를 pri(1차) 또는 sec(2차)로 표시합니다. **failover lan unit** 명령을 사용하여 우선순위를 설정합니다.
state	유닛의 트래픽 전달 상태 또는 역할을 표시합니다. 장애 조치의 경우 **state** 키워드에 대해 다음 값이 표시됩니다. • act - 장애 조치가 활성화되었으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • stby - 장애 조치가 활성화되었으며, 해당 유닛은 트래픽을 전달하는 중이 아니고 대기, 실패 또는 그 밖의 비활성 상태에 있습니다. • actNoFailover - 장애 조치가 활성화되지 않았으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • stbyNoFailover - 장애 조치가 활성화되지 않았으며, 해당 유닛은 트래픽을 전달하는 중이 아닙니다. 대기 유닛의 임계값을 초과하는 인터페이스 오류가 있을 경우 이러한 상황이 발생할 수 있습니다. 클러스터링의 경우 **state** 키워드에 대해 다음 값이 표시됩니다. • master • slave 예를 들어 **prompt hostname cluster-unit state**를 설정하는 경우 "ciscoasa/cl2/slave>" 프롬프트에서 호스트 이름은 ciscoasa, 유닛 이름은 cl2, 상태 이름은 slave입니다.

기본값

기본 프롬프트는 hostname입니다. 다중 컨텍스트 모드에서 호스트 이름 뒤에는 현재의 컨텍스트 이름이 옵니다(*hostname/context*).

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
9.0(1)	**cluster-unit** 옵션이 추가되었습니다. 클러스터링을 위해 **state** 키워드가 업데이트되었습니다.

사용 지침

키워드를 입력하는 순서는 프롬프트에서 요소가 나타나는 순서를 결정하며, 슬래시(/)로 구분됩니다.

다중 컨텍스트 모드에서 시스템 실행 공간 또는 관리 컨텍스트에 로그인하면 확장 프롬프트를 볼 수 있습니다. 비관리 컨텍스트 내에서는 호스트 이름 및 컨텍스트 이름인 기본 프롬프트만 볼 수 있습니다.

프롬프트에 정보를 추가하는 기능 덕분에 여러 모듈이 있는 경우 어떤 ASA에 로그인했는지를 한눈에 알 수 있습니다. 장애 조치 중에 두 ASA의 호스트 이름이 동일한 경우 이 기능이 유용합니다.

예

다음 예는 장애 조치 시 사용 가능한 프롬프트의 모든 요소를 보여줍니다.

```
ciscoasa(config)# prompt hostname context slot state priority
```

프롬프트가 다음 문자열로 변경됩니다.

```
ciscoasa/admin/pri/act(config)#
```

관련 명령

명령	설명
clear configure prompt	구성된 프롬프트를 지웁니다.
show running-config prompt	구성된 프롬프트를 표시합니다.

propagate sgt

인터페이스에서 보안 그룹 태그(**sgt**라고 함) 전파를 활성화하려면 cts 수동 인터페이스 컨피그레이션 모드에서 **propagate sgt** 명령을 사용합니다. 인터페이스에서 보안 그룹 태그(**sgt**라고 함) 전파를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

propagate sgt

no propagate sgt

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

전파는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Cts 수동 인터페이스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
9.3(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 CTS Layer 2 SGT Imposition에서 보안 그룹의 전파를 활성화 및 비활성화합니다.

제한

- 물리적 인터페이스, VLAN 인터페이스, 포트 채널 인터페이스 및 중복 인터페이스에서만 지원됩니다.
- BVI, TVI, VNI 등의 논리적 인터페이스나 가상 인터페이스에서는 지원되지 않습니다.

예

다음 예는 Layer 2 SGT Imposition에 대한 인터페이스를 활성화하고 SGT가 전파되지 않음을 나타냅니다.

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# no propagate sgt
```

관련 명령

명령	설명
cts manual	Layer 2 SGT Imposition을 활성화하고 cts 수동 인터페이스 컨피그레이션 모드로 들어갑니다.
policy static sgt	수동으로 구성된 CTS 링크에 정책을 적용합니다.

protocol

IKEv2 연결용 IPsec Proposal의 프로토콜 및 암호화 유형을 지정하려면 IPsec Proposal 컨피그레이션 모드에서 **protocol** 명령을 사용합니다. 프로토콜 및 암호화 유형을 제거하려면 이 명령의 **no** 형식을 사용합니다.

protocol esp {encryption {des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null} | integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

no protocol esp {encryption {des | 3des | aes | aes-192 | aes-256 | | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null} | integrity {md5 | sha-1 | sha-256 | sha-384 | sha-512 | null}

구문 설명

esp	ESP(Encapsulating Security Payload) IPsec 프로토콜(현재 IPsec에 대해 지원되는 유일한 프로토콜)을 지정합니다.
des	ESP에 대해 56비트 DES-CBC 암호화를 지정합니다.
3des	(기본값) ESP에 대해 Triple DES 암호화 알고리즘을 지정합니다.
aes	ESP에 대해 128비트 키 암호화 포함 AES를 지정합니다.
aes-192	ESP에 대해 192비트 키 암호화 포함 AES를 지정합니다.
aes-256	ESP에 대해 256비트 키 암호화 포함 AES를 지정합니다.
aes-gcm	어떤 AES-GCM 또는 AES-GMAC 알고리즘을 사용할지를 지정합니다.
aes-gcm-192	어떤 AES-GCM 또는 AES-GMAC 알고리즘을 사용할지를 지정합니다.
aes-gcm-256	어떤 AES-GCM 또는 AES-GMAC 알고리즘을 사용할지를 지정합니다.
aes-gmac	어떤 AES-GCM 또는 AES-GMAC 알고리즘을 사용할지를 지정합니다.
aes-gmac-192	어떤 AES-GCM 또는 AES-GMAC 알고리즘을 사용할지를 지정합니다.
aes-gmac-256	어떤 AES-GCM 또는 AES-GMAC 알고리즘을 사용할지를 지정합니다.
null	ESP에 대해 암호화를 사용하지 않습니다.
integrity	IPsec 프로토콜에 대해 무결성 알고리즘을 지정합니다.
md5	ESP 무결성 보호를 위해 md5 알고리즘을 지정합니다.
sha-1	(기본값) ESP 무결성 보호를 위해 SHA(Secure Hash Algorithm) SHA-1(미국 FIPS(Federal Information Processing Standard)에서 정의)을 지정합니다.
sha-256	IPsec 무결성 알고리즘으로 어떤 알고리즘을 사용할지를 지정합니다.
sha-384	IPsec 무결성 알고리즘으로 어떤 알고리즘을 사용할지를 지정합니다.
sha-512	IPsec 무결성 알고리즘으로 어떤 알고리즘을 사용할지를 지정합니다.
null	암호화 알고리즘으로 AES-GCM/GMAC를 구성한 경우 선택합니다.

기본값

IPsec Proposal의 기본 설정은 암호화 유형 3DES 및 무결성 유형 SHA-1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
IPsec proposal 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
8.4(1)	이 명령이 추가되었습니다.
9.0(1)	AES-GCM 또는 AES-GMAC 알고리즘 지원이 추가되었습니다. IPsec 무결성 알고리즘으로서 사용할 알고리즘을 선택하는 기능이 추가되었습니다.

사용 지침

IKEv2 IPsec Proposal에는 암호화 및 무결성 유형이 여러 개 있을 수 있습니다. 유형을 지정하는 데 이 명령을 사용하면 피어에서는 원하는 유형을 선택할 수 있습니다.

예

다음 예는 IPsec Proposal *proposal_1*을 생성하고, ESP 암호화 유형 DES 및 3DES를 구성하며, 무결성 보호를 위해 암호화 알고리즘 MD5 및 SHA-1을 지정합니다.

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
ciscoasa(config-ipsec-proposal)# protocol ESP encryption des 3des
ciscoasa(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

관련 명령

명령	설명
crypto ikev2 enable	IPsec 피어가 통신하는 인터페이스에서 ISAKMP IKEv2 협상을 활성화합니다.
crypto ipsec ikev2 ipsec-proposal	IPsec Proposal을 생성하고, Proposal을 위해 여러 암호화 및 무결성 유형을 지정할 수 있는 IPsec Proposal 컨피그레이션 모드로 들어갑니다.
show running-config ipsec	모든 Transform Set의 컨피그레이션을 표시합니다.
crypto map set transform-set	암호화 맵 엔트리에서 사용할 Transform Set을 지정합니다.
crypto dynamic-map set transform-set	동적 암호화 맵 엔트리에서 사용할 Transform Set을 지정합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.
show running-config crypto dynamic-map	동적 암호화 맵 컨피그레이션을 표시합니다.

protocol-enforcement

도메인 이름, 레이블 길이, 형식 확인(압축 및 반복 포인터 확인 포함)을 활성화하려면 매개변수 컨피그레이션 모드에서 **protocol-enforcement** 명령을 사용합니다. 프로토콜 적용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

protocol-enforcement

no protocol-enforcement

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

프로토콜 적용은 기본적으로 활성화되어 있습니다. **policy-map type inspect dns**가 정의되지 않았어도 **inspect dns**가 구성되어 있으면 이 기능을 활성화할 수 있습니다. 비활성화하려면 정책 맵 컨피그레이션에서 **no protocol-enforcement**를 명시적으로 작성해야 합니다. **inspect dns**가 구성되어 있지 않으면 NAT 재작성이 수행되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

특정 조건에서는 명령이 비활성화된 경우에도 프로토콜 적용이 수행됩니다. 이러한 상황은 DNS 리소스 레코드 분류, NAT 또는 TSIG 점검 등의 다른 이유로 DNS 리소스 레코드의 구문 분석이 필요한 경우 발생합니다.

예

다음 예는 DNS 검사 정책 맵에서 프로토콜 적용을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-enforcement
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

protocol http

CRL 검색을 위한 허용된 배포 지점 포로토콜로서 HTTP를 지정하려면 ca-crl 컨피그레이션 모드에서 **protocol http** 명령을 사용합니다. CRL 검색을 위한 허용된 방법으로서 HTTP를 제거하려면 이 명령의 **no** 형식을 사용합니다.

protocol http

no protocol http

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 설정은 HTTP를 허용하는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-crl 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용할 경우 공개 인터페이스 필터에 HTTP 규칙을 할당해야 합니다. 권한에 따라, CRL 배포 지점의 내용이 검색 방법(HTTP, LDAP 및/또는 SCEP)을 결정합니다.

예

다음 예는 ca-crl 컨피그레이션 모드로 들어가서, trustpoint central용 CRL 검색을 위한 배포 지점 포로토콜로서 HTTP를 허용합니다.

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol http
```

관련 명령

명령	설명
crl configure	ca-crl 컨피그레이션 모드로 들어갑니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드로 들어갑니다.
protocol ldap	CRL의 검색 방법으로서 LDAP를 지정합니다.
protocol scep	CRL의 검색 방법으로서 SCEP를 지정합니다.

protocol ldap

CRL 검색을 위한 배포 지점 포로토콜로서 LDAP를 지정하려면 ca-crl 컨피그레이션 모드에서 **protocol ldap** 명령을 사용합니다. 권한에 따라, CRL 배포 지점의 내용이 검색 방법(HTTP, LDAP 및/또는 SCEP)을 결정합니다.

CRL 검색을 위한 허용된 방법으로서 LDAP 프로토콜을 제거하려면 이 명령의 **no** 형식을 사용합니다.

protocol ldap

no protocol ldap

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 설정은 LDAP를 허용하는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
crl 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 ca-crl 컨피그레이션 모드로 들어가서, trustpoint central용 CRL 검색을 위한 배포 지점 포로토콜로서 LDAP를 허용합니다.

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

관련 명령

명령	설명
crl configure	ca-crl 컨피그레이션 모드로 들어갑니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드로 들어갑니다.
protocol http	CRL의 검색 방법으로서 HTTP를 지정합니다.
protocol scep	CRL의 검색 방법으로서 SCEP를 지정합니다.

protocol scep

CRL 검색을 위한 배포 지점 포로토콜로서 SCEP를 지정하려면 crl 컨피그레이션 모드에서 **protocol scep** 명령을 사용합니다. 권한에 따라, CRL 배포 지점의 내용이 검색 방법(HTTP, LDAP 및/또는 SCEP)을 결정합니다.

CRL 검색을 위한 허용된 방법으로서 SCEP 프로토콜을 제거하려면 이 명령의 **no** 형식을 사용합니다.

protocol scep

no protocol scep

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 설정은 SCEP를 허용하는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crl 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 ca-crl 컨피그레이션 모드로 들어가서, trustpoint central용 CRL 검색을 위한 배포 지점 포로토콜로서 SCEP를 허용합니다.

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol scep
ciscoasa(ca-crl)#
```

관련 명령

명령	설명
crl configure	ca-crl 컨피그레이션 모드로 들어갑니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드로 들어갑니다.
protocol http	CRL의 검색 방법으로서 HTTP를 지정합니다.
protocol ldap	CRL의 검색 방법으로서 LDAP를 지정합니다.

protocol-object

프로토콜 객체 그룹에 프로토콜 객체를 추가하려면 프로토콜 컨피그레이션 모드에서 **protocol-object** 명령을 사용합니다. 포트 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

protocol-object *protocol*

no protocol-object *protocol*

구문 설명

protocol	프로토콜 이름 또는 번호

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
프로토콜 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

프로토콜 컨피그레이션 모드에서 프로토콜 객체를 정의하려면 **protocol-object** 명령을 **object-group** 명령과 함께 사용합니다.

protocol 인수를 사용하여 IP프로토콜 이름 또는 번호를 지정할 수 있습니다. udp 프로토콜 번호는 17, tcp 프로토콜 번호는 6, egp 프로토콜 번호는 47입니다.

예

다음 예는 프로토콜 객체를 정의하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol)# protocol-object udp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# exit
ciscoasa(config)# object-group protocol proto_grp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# group-object proto_grp_1
ciscoasa(config-protocol)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure object-group	컨피그레이션에서 모든 **object group** 명령을 제거합니다.
group-object	네트워크 객체 그룹을 추가합니다.
network-object	네트워크 객체를 네트워크 객체 그룹에 추가합니다.
object-group	컨피그레이션을 최적화하기 위해 객체 그룹을 정의합니다.
show running-config object-group	현재 객체 그룹을 표시합니다.

protocol-violation

HTTP 및 NetBIOS 검사에서 프로토콜 위반이 발생할 경우의 작업을 정의하려면 매개변수 컨피그레이션 모드에서 **protocol-violation** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

protocol-violation action [**drop** [**log**] | **log**]

no protocol-violation action [**drop** [**log**] | **log**]

구문 설명

drop	프로토콜을 준수하지 않는 패킷을 삭제하도록 지정합니다.
log	프로토콜 위반을 기록하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 HTTP 또는 NetBIOS 정책 맵에서 구성할 수 있습니다. HTTP 또는 NetBIOS 파서가 메시지의 처음 몇 바이트에서 유효한 HTTP 또는 NetBIOS 메시지를 감지할 수 없는 경우 syslog가 발생합니다. 이러한 상황은 예를 들어 청크 분할 인코딩의 형식이 잘못되어 메시지를 구문 분석할 수 없는 경우 발생합니다.

예

다음 예는 정책 맵에서 프로토콜 위반에 대한 작업을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

proxy-auth

터널 그룹을 특정 프록시 인증 터널 그룹으로 플래그 지정하려면 webvpn 컨피그레이션 모드에서 **proxy-auth** 명령을 사용합니다.

proxy-auth [**sdi**]

구문 설명I

sdi	SDI 지시문에 대해 RADIUS/TACACS SDI 프록시 메시지를 구문 분석합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

기본 프로토콜 지시문에 대한 aaa-server 프록시 인증 문자 메시지의 구문 분석을 활성화하려면 **proxy-auth** 명령을 사용합니다.

proxy-auth_map sdi

RADIUS 프록시 서버에서 반환된 RADIUS 챌린지 메시지를 기본 SDI 메시지에 매핑하려면 aaa-server 컨피그레이션 모드에서 **proxy-auth_map sdi** 명령을 사용합니다.

proxy-auth_map sdi [**sdi_message**] [**radius_challenge_message**]

구문 설명

radius_challenge_message	특정 SDI 메시지의 매핑에 사용되는 RADIUS 챌린지 메시지를 지정합니다. 다음 중 하나가 될 수 있습니다. • new-pin-meth—New PIN Method, [default] Do you want to enter your own pin • new-pin-reenter—Reenter new PIN, [default] Reenter PIN: • new-pin-req—New PIN requested, [default] Enter your new Alpha-Numerical PIN • new-pin-sup—New PIN supplied, [default] Please remember your new PIN • new-pin-sys-ok—New PIN accepted, [default] New PIN Accepted • next-ccode-and-reauth—Reauthenticate on token change, [default] new PIN with the next card code • next-code—Provide the tokencode without PIN, [default] Enter Next PASSCODE • ready-for-sys-pin—Accept system generated PIN, [default] ACCEPT A SYSTEM GENERATED PIN
sdi_message	기본 SDI 메시지를 지정합니다.

기본값

ASA의 기본 매핑은 Cisco ACS의 기본 설정(시스템 관리, 구성 및 RSA SecureID 프롬프트 포함)에 해당하며, RSA Authentication Manager의 기본 설정과도 동기화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

RADIUS 프록시의 RADIUS 챌린지 메시지에 대한 구문 분석 및 매핑을 활성화하려면 tunnel-group 컨피그레이션 모드에서 **proxy-auth** 명령을 활성화해야 합니다. 그러면 기본 매핑 값이 사용됩니다. **proxy-auth_map** 명령을 사용하여 기본 매핑 값을 변경할 수 있습니다.

원격 사용자는 AnyConnect 클라이언트로 ASA에 연결하고 RSA SecurID 토큰을 사용하여 인증을 시도합니다. ASA는 RADIUS 프록시 서버를 사용하여 구성할 수 있으며, 이 프록시 서버는 해당 인증에 대해 SDI 서버와 통신합니다.

인증 중에 RADIUS 서버는 ASA에 액세스 챌린지 메시지를 보여줍니다. 이러한 챌린지 메시지 내에는 SDI 서버의 텍스트를 포함하는 응답 메시지가 있습니다. ASA가 SDI 서버와 직접 통신할 경우에는 ASA가 RADIUS 프록시를 통해 통신할 경우와 메시지 텍스트가 다릅니다.

따라서 AnyConnect 클라이언트에 기본 SDI 서버로 보이려면 ASA는 RADIUS 서버의 메시지를 해석해야 합니다. 또한 SDI 메시지는 SDI 서버에서 구성 가능하므로 ASA의 메시지 텍스트는 SDI 서버의 메시지 텍스트와 전체적으로 또는 부분적으로 일치해야 합니다. 그러지 않으면 원격 클라이언트 사용자에게 표시되는 프롬프트가 인증 도중에 필요한 작업에 적절하지 않을 수 있습니다. AnyConnect 클라이언트는 응답에 실패할 수 있으며, 인증이 실패할 수 있습니다.

관련 명령

명령	설명
proxy-auth	RADIUS 프록시에서 오는 RADIUS 챌린지 메시지의 구문 분석 및 매핑을 활성화합니다.

proxy-bypass

최소 콘텐츠 재작성을 수행하고 재작성할 콘텐츠 유형(외부 링크 및/또는 XML)을 지정하도록 ASA를 구성하려면 webvpn 컨피그레이션 모드에서 **proxy-bypass** 명령을 사용합니다. 프록시 바이패스를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

proxy-bypass interface *interface name* {**port** *port number*| **path-mask** *path mask*} **target** *url* **[rewrite {link | xml | none}]**

no proxy-bypass interface *interface name* {**port** *port number*| **path-mask** *path mask*} **target** *url* **[rewrite {link | xml | none}]**

구문 설명

host	트래픽을 포워딩할 호스트를 지정합니다. 호스트 IP 주소 또는 호스트 이름을 사용합니다.
interface	프록시 바이패스를 위한 ASA 인터페이스를 지정합니다.
interface name	ASA 인터페이스를 이름으로 지정합니다.
link	절대 외부 링크의 재작성을 지정합니다.
none	재작성 없음을 지정합니다.
path-mask	확인할 패턴을 지정합니다.
path-mask	정규식을 포함할 수 있는, 확인할 패턴을 지정합니다. 다음 와일드카드를 사용할 수 있습니다. * - 모든 것이 일치합니다 . 이 와일드카드는 단독으로 사용할 수 없습니다 . 영숫자 문자열과 함께 사용해야 합니다 . ? - 단일 문자와 일치합니다 . [!seq] - 시퀀스에 없는 문자와 일치합니다 . [seq] - 시퀀스에 있는 문자와 일치합니다 . 최대 128바이트.
port	프록시 바이패스에 예약된 포트를 지정합니다.
port number	프록시 바이패스에 예약된 높은 번호의 포트를 지정합니다. 포트 범위는 20000~21000입니다. 하나의 바이패스 프록시 규칙에 대해 하나의 포트만 사용할 수 있습니다.
rewrite	(선택 사항) 재작성을 위한 추가 규칙(없음 또는 XML과 링크의 조합)을 지정합니다.
target	트래픽을 포워딩할 원격 서버를 지정합니다.
url	URL을 **http(s)://***fully_qualified_domain_name*[:*port*] 형식으로 입력합니다. 최대 128바이트. 달리 지정하지 않는 한 HTTP용 포트는 80, HTTPS용 포트는 443입니다.
xml	XML 콘텐츠 재작성을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
WebVPN 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

최소 콘텐츠 재작성에서 더 잘 작동하는 애플리케이션 및 웹 리소스에 대해 프록시 바이패스를 사용합니다. proxy-bypass 명령은 ASA를 통과하는 특정 웹 애플리케이션을 처리하는 방법을 결정합니다.

이 명령을 여러 번 사용할 수 있습니다. 엔트리 구성 순서는 중요하지 않습니다. 인터페이스와 경로 마스크 또는 인터페이스와 포트는 프록시 바이패스 규칙을 고유하게 식별합니다.

경로 마스크가 아닌 포트를 사용하여 프록시 바이패스를 구성하는 경우 네트워크 컨피그레이션에 따라, 이러한 포트가 ASA에 액세스하도록 허용하려면 방화벽 컨피그레이션을 변경해야 할 수 있습니다. 이 제한을 피하려면 경로 마스크를 사용하십시오. 그러나 경로 마스크는 변경될 수 있으므로, 이런 가능성을 없애려면 pathmask 명령문을 여러 번 사용해야 할 수 있습니다.

경로란 URL에서 .com, .org 또는 기타 도메인 이름 유형 뒤에 나오는 모든 것입니다. 예를 들어 URL www.example.com/hrbenefits에서는 *hrbenefits*가 경로입니다. 마찬가지로 URL www.example.com/hrinsurance에서는 *hrinsurance*가 경로입니다. 모든 hr 사이트에 대해 프록시 바이패스를 사용하려면 /hr*처럼 * 와일드카드를 사용하여 명령을 여러 번 사용하는 것을 피할 수 있습니다.

예

다음 예는 webvpn 인터페이스에 대한 프록시 바이패스에 포트 20001을 사용하고, HTTP 및 기본 포트 80을 사용하여 example.com으로 트래픽을 포워딩하고 XML 콘텐츠를 재작성하도록 ASA를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# proxy-bypass interface webvpn port 20001 target
http://example.com rewrite xml
```

다음 예는 외부 인터페이스에서 프록시 바이패스에 경로 마스크 mypath/*를 사용하고, HTTPS 및 기본 포트 443을 사용하여 example.com으로 트래픽을 포워딩하고 XML 및 링크 콘텐츠를 재작성하도록 ASA를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://example.com rewrite xml,link
```

관련 명령

명령	설명
apcf	특정 애플리케이션에 사용할 비표준 규칙을 지정합니다.
rewrite	트래픽이 ASA를 통과할지 여부를 결정합니다.

proxy-ldc-issuer

TLS 프록시 로컬 동적 인증서를 발급하려면 crypto ca trustpoint 컨피그레이션 모드에서 **proxy-ldc-issuer** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

proxy-ldc-issuer

no proxy-ldc-issuer

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

TLS 프록시 로컬 동적 인증서를 발급하려면 **proxy-ldc-issuer** 명령을 사용합니다. **proxy-ldc-issuer** 명령은 암호화 신뢰 지점에 LDC를 발급할 수 있는 로컬 CA로서의 역할을 허용하며, crypto ca trustpoint 컨피그레이션 모드에서 액세스할 수 있습니다.

proxy-ldc-issuer 명령은 신뢰 지점에 대해 TLS 프록시용 동적 인증서를 발급할 수 있는 로컬 CA 역할을 정의합니다. 이 명령은 "enrollment self"의 신뢰 지점에서만 구성할 수 있습니다.

예

다음 예는 전화기용 LDC 서명을 위한 내부 로컬 CA를 생성하는 방법을 보여줍니다. 이 로컬 CA는 **proxy-ldc-issuer**가 활성화된 상태로 일반 자체 서명 신뢰 지점으로서 생성됩니다.

```
ciscoasa(config)# crypto ca trustpoint ldc_server
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
ciscoasa(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
ciscoasa(config)# crypto ca enroll ldc_server
```

관련 명령

명령	설명
ctl-provider	CTL 공급자 인스턴스를 정의하고 컨피그레이션 모드로 들어갑니다.
server trust-point	TLS 핸드셰이크 중에 표시될 프록시 신뢰 지점 인증서를 지정합니다.
show tls-proxy	TLS 프록시를 보여줍니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

proxy-server

IP Phone의 컨피그레이션 파일에서 <proxyServerURL> 태그 아래에 기록되는 Phone Proxy 기능에 대해 HTTP 프록시를 구성하려면 phone-proxy 컨피그레이션 모드에서 **proxy-server** 명령을 사용합니다. Phone Proxy에서 HTTP 프록시 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

구문 설명

interface *ifc*	ASA에서 HTTP 프록시가 상주하는 인터페이스를 지정합니다.
ip_address	HTTP 프록시의 IP 주소를 지정합니다.
listen_port	HTTP 프록시의 수신 대기 포트를 지정합니다. 지정하지 않는 경우 기본값은 8080입니다.

기본값

수신 포트를 지정하지 않으면 포트는 기본적으로 8080으로 구성됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Phone-proxy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(4)	이 명령이 추가되었습니다.

사용 지침

전화 서비스를 위해 모든 IP Phone URL이 프록시 서버로 이동하는 외부 네트워크 또는 DMZ의 HTTP 프록시에 대해 Phone Proxy를 위한 프록시 서버 컨피그레이션 옵션을 설정할 수 있습니다. 이 설정에서는 비보안 HTTP 트래픽도 수용하는데, 이러한 트래픽은 회사 네트워크로 다시 들어갈 수 없습니다.

입력하는 *ip_address*는 IP Phone 및 HTTP 프록시 서버의 위치를 기반으로 하는 전역 IP 주소여야 합니다.

프록시 서버가 DMZ에 있고 IP Phone이 네트워크 외부에 있으면 ASA는 NAT 규칙이 있는지 조회한 후 전역 IP 주소를 사용하여 컨피그레이션 파일에 기록합니다.

ASA에서 호스트 이름을 IP 주소로 해석할 수 있는 경우(예: DNS 조회가 구성됨) *ip_address* 인수에 호스트 이름을 입력할 수 있습니다. ASA에서 호스트 이름이 IP 주소로 해석되기 때문입니다.

기본적으로 Enterprise Parameters 아래에 구성된 Phone URL Parameters는 URL에 FQDN을 사용합니다. HTTP 프록시에 대한 DNS 조회가 FQDN을 해석하지 못하는 경우 IP 주소를 사용하도록 매개변수를 변경해야 할 수 있습니다.

프록시 서버 URL이 IP Phone 컨피그레이션 파일에 올바르게 기록되었는지 확인하려면 Settings > Device Configuration > HTTP configuration >Proxy Server URL에서 IP Phone의 URL을 점검하십시오.

Phone Proxy는 프록시 서버에 대해 HTTP 트래픽을 검사하지 않습니다.

ASA가 IP Phone 및 HTTP 프록시 서버의 경로에 있는 경우, 프록시 서버의 문제를 해결하려면 기존의 디버깅 방법(예: syslog 및 캡처)을 사용합니다.

Phone Proxy가 사용 중인 경우 하나의 프록시 서버만 구성할 수 있습니다. 그러나 프록시 서버 구성 이후 IP Phone에서 이미 자체 컨피그레이션 파일을 다운로드한 경우, 프록시 서버의 주소가 포함된 컨피그레이션을 사용할 수 있도록 IP Phone을 다시 시작해야 합니다.

예

다음 예는 **proxy-server** 명령을 사용하여 Phone Proxy에 대한 HTTP 프록시 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

관련 명령

명령	설명
phone-proxy	Phone Proxy 인스턴스를 구성합니다.

publish-crl

다른 ASA가 로컬 CA에서 발급한 인증서의 폐기 상태를 검증하도록 허용하려면, ASA의 인터페이스에서 직접 CRL을 다운로드할 수 있도록 ca-server 컨피그레이션 모드에서 **publish-crl** 명령을 사용합니다. TCRL을 다운로드하지 못하게 하려면 이 명령의 **no** 형식을 사용합니다.

[**no**] **publish-crl interface** *interface* [**port** *portnumber*]

구문 설명

interface *interface*	인터페이스에 사용할 *nameif*(예: **gigabitethernet0/1**)를 지정합니다. 자세한 내용은 **interface** 명령을 참조하십시오.
port *portnumber*	(선택 사항) 인터페이스 디바이스가 CRL을 다운로드할 수 있는 포트를 지정합니다. 포트 번호의 범위는 1~65535입니다.

기본값

기본 **publish-crl** 상태는 **no publish**입니다. TCP 포트 80은 HTTP의 기본값입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Ca-server 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

CRL에는 기본적으로 액세스할 수 없습니다. 필요한 인터페이스 및 포트에서 CRL 파일에 대한 액세스를 활성화해야 합니다.

TCP 포트 80은 HTTP 기본 포트 번호입니다. 기본 포트가 아닌 포트(포트 80이 아닌 포트)를 구성하려는 경우, 다른 디바이스에서 이 특정 포트에 액세스할 수 있도록 **cdp-url** 컨피그레이션에 새 포트 번호를 포함해야 합니다.

CRL 배포 지점(CDP)은 로컬 CA ASA에 있는 CRL의 위치입니다. **cdp-url** 명령으로 구성하는 URL은 발급된 인증서에 포함됩니다. CDP에 대해 구체적인 위치를 구성하지 않을 경우 기본 CDP URL은 http://hostname.domain/+CSCOCA+/asa_ca.crl입니다.

클라이언트리스 SSL VPN이 동일한 인터페이스에서 활성화된 경우, HTTP 리디렉션 및 CRL 다운로드 요청은 동일한 HTTP 리스너에서 처리됩니다. 리스너는 들어오는 URL을 점검하며, **cdp-url** 명령으로 구성한 것과 일치하는 경우 CRL 파일이 다운로드됩니다. URL이 **cdp-url** 명령과 일치하지 않으면 연결이 HTTPS로 리디렉션됩니다(HTTP 리디렉션이 활성화된 경우).

예

ca-server 컨피그레이션 모드에서 입력하는 다음 **publish-crl** 명령의 예에서는 CRL 다운로드를 위해 외부 인터페이스의 포트 70이 활성화됩니다.

```
ciscoasa(config)# crypto ca server
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
cdp-url	자동으로 생성된 CRL을 위한 특정 위치를 지정합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

pwd

현재 작업 디렉토리를 표시하려면 특별 권한 EXEC 모드에서 **pwd** 명령을 사용합니다.

pwd

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

루트 디렉토리(*/*)가 기본값입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0	이 명령이 추가되었습니다.

사용 지침

이 명령은 **dir** 명령과 기능이 유사합니다.

예

다음 예는 현재 작업 디렉토리를 표시하는 방법을 보여줍니다.

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

관련 명령

명령	설명
cd	현재의 작업 디렉토리를 지정한 디렉토리로 변경합니다.
dir	디렉토리 내용을 표시합니다.
more	파일의 내용을 표시합니다.

18 장

queue-limit through reset 명령

queue-limit(priority-queue)

우선순위 큐의 깊이를 지정하려면 우선순위 큐 컨피그레이션 모드에서 **queue-limit** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

참고 ASA 5580 Ten Gigabit Ethernet 인터페이스에서는 이 명령이 지원되지 않습니다. (Ten Gigabit Ethernet 인터페이스는 ASA 5585-X의 우선순위 큐에 지원됩니다.) ASA 5512-X~ASA 5555-X 관리 인터페이스에서는 이 명령이 지원되지 않습니다.

ASA Services Module에서는 이 명령이 지원되지 않습니다.

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

구문 설명

number-of-packets	인터페이스에서 패킷 삭제를 시작하기 전에 큐에 추가(즉, 버퍼링)할 수 있는 저지연(low-latency) 또는 일반 우선순위 패킷의 최대 수를 지정합니다. 값 범위의 상한은 런타임에 동적으로 결정됩니다. 이 제한을 보려면 명령줄에 **help** 또는 **?**를 입력하십시오. 주요 결정 요인은 큐 지원에 필요한 메모리 및 디바이스에서 사용 가능한 메모리입니다. 큐는 사용 가능한 메모리를 초과하지 않아야 합니다. 이론상 최대 패킷 수는 2147483647입니다.

기본값

queue-limit 기본값은 1024패킷입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
우선순위 큐 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA에서는 두 개의 트래픽 클래스를 허용합니다. 우선순위가 더 높고 레이턴시에 민감한 트래픽(예: 음성과 비디오)에는 LLQ(Low-Latency Queuing), 나머지 모든 트래픽에는 기본값인 BE(Best Effort)를 허용합니다. ASA에서는 우선순위 트래픽을 인식하고 적절한 QoS(Quality of Service) 정책을 적용합니다. 트래픽 흐름을 정밀하게 조정하기 위해 우선순위 큐의 크기와 깊이를 구성할 수 있습니다.

참고 인터페이스에 대해 우선순위 큐잉을 활성화하려면 **priority-queue** 명령을 *반드시* 구성해야 합니다.

nameif 명령으로 정의할 수 있는 인터페이스에는 **priority-queue** 명령을 한 번 적용할 수 있습니다.

프롬프트에서 알 수 있듯이 **priority-queue** 명령을 실행하면 우선순위 큐 컨피그레이션 모드로 들어갑니다. 우선순위 큐 컨피그레이션 모드에서는 특정 시간에 전송 큐에서 허용되는 최대 패킷 수(**tx-ring-limit** 명령) 및 패킷이 삭제되기까지 버퍼링할 수 있는 각 유형(priority 또는 best-effort)의 패킷 수(**queue-limit** 명령)를 구성할 수 있습니다.

지정하는 tx-ring-limit 및 queue-limit은 우선순위가 더 높은 LLQ 및 BE 큐 모두에 영향을 미칩니다. tx-ring-limit은 혼잡이 해소될 때까지 패킷을 버퍼링할 수 있도록 드라이버가 인터페이스 앞에 있는 큐로 다시 보내기까지 드라이버에 대해 허용되는 각 유형의 패킷 수입니다. 일반적으로 이러한 두 매개변수를 조정하여 저지연 트래픽의 흐름을 최적화할 수 있습니다.

큐의 크기는 무한하지 않으므로 가득 차서 오버플로될 수 있습니다. 큐가 가득 차면 해당 큐로 추가 패킷이 들어갈 수 없어 삭제됩니다. 이를 *tail drop*이라고 합니다. 큐가 가득 차는 것을 막으려면 **queue-limit** 명령을 사용하여 큐 버퍼 크기를 늘릴 수 있습니다.

예

다음 예는 test라는 인터페이스에 대해 우선순위 큐를 구성하면서, 큐 제한은 패킷 234개로 지정하고 전송 큐 제한은 패킷 3개로 지정합니다.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 234
ciscoasa(priority-queue)# tx-ring-limit 3
```

관련 명령

명령	설명
clear configure priority-queue	명명된 인터페이스에서 현재의 우선순위 큐 컨피그레이션을 제거합니다.
priority-queue	인터페이스에서 우선순위 큐잉을 구성합니다.
show priority-queue statistics	명명된 인터페이스의 우선순위 큐 통계를 보여줍니다.
show running-config [all] priority-queue	현재의 우선순위 큐 컨피그레이션을 표시합니다. **all** 키워드를 지정하면 현재의 우선순위 큐, queue-limit 및 tx-ring-limit 컨피그레이션 값이 모두 표시됩니다.
tx-ring-limit	이더넷 전송 드라이버에서 특정 시간에 큐에 추가할 수 있는 최대 패킷 수를 설정합니다.

queue-limit(tcp-map)

TCP 연결을 위해 순서를 지정할 수 있고 버퍼링 가능한 무순서 패킷의 최대 수를 구성하려면 tcp-map 컨피그레이션 모드에서 **queue-limit** 명령을 사용합니다. 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 **set connection advanced-options** 명령을 사용하여 활성화되는 TCP 정규화 정책의 일부입니다.

queue-limit *pkt_num* [**timeout** *seconds*]

no queue-limit

구문 설명

pkt_num	TCP 연결을 위해 순서를 지정하고 버퍼링할 수 있는 무순서 패킷의 최대 수(1~250)를 지정합니다. 기본값은 0입니다. 즉, 트래픽의 유형에 따라 이 설정이 비활성화되고 기본 시스템 큐 제한이 사용될 수 있음을 의미합니다. 자세한 내용은 "사용 지침" 섹션을 참조하십시오.
timeout *seconds*	(선택 사항) 무순서 패킷이 버퍼에 머물 수 있는 최대 시간(1~20초)을 설정합니다. 기본값은 4초입니다. 시간 내에 순서가 정해져 전달되지 않으면 해당 패킷은 삭제됩니다. *pkt_num* 인수를 0으로 설정하면 트래픽의 시간 제한을 변경할 수 없습니다. **timeout** 키워드가 작동하도록 하려면 제한을 1 이상으로 설정해야 합니다.

기본값

기본값은 0입니다. 즉, 이 명령이 비활성화되어 있습니다.

기본 시간 제한은 4초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(4)/8.0(4)	**timeout** 키워드가 추가되었습니다.

사용 지침

TCP 정규화를 활성화하려면 Modular Policy Framework를 사용하십시오.

1. **tcp-map** - TCP 정규화 작업을 식별합니다.
   a. **queue-limit** - tcp-map 컨피그레이션 모드에서는 **queue-limit** 명령 및 기타 많은 명령을 입력할 수 있습니다.
2. **class-map** - TCP 정규화를 수행할 트래픽을 식별합니다.
3. **policy-map** - 각 클래스 맵과 관련된 작업을 식별합니다.
   a. **class** - 작업을 수행할 클래스 맵을 식별합니다.
   b. **set connection advanced-options** - 생성한 tcp-map을 식별합니다.
4. **service-policy** - 정책 맵을 한 인터페이스에 또는 전체적으로 할당합니다.

TCP 정규화를 활성화하지 않거나 **queue-limit** 명령을 기본값 0으로 설정하면(즉, 비활성화되면), 트래픽 유형에 따라 기본 시스템 큐 제한이 사용됩니다.

- 애플리케이션 검사(**inspect** 명령), IPS(**ips** 명령), TCP 확인 재전송(TCP map **check-retransmission** 명령)에 대한 연결에서는 큐 제한이 패킷 3개입니다. ASA에서 다른 윈도우 크기의 TCP 패킷을 수신하면 광고된 설정과 일치하도록 큐 제한이 동적으로 변경됩니다.
- 다른 TCP 연결의 경우 무순서 패킷은 원래의 상태대로 전달됩니다.

queue-limit 명령을 1 이상으로 설정한 경우, 모든 TCP 트래픽에 허용되는 무순서 패킷의 수는 이 설정과 일치합니다. 예를 들어 애플리케이션 검사, IPS 및 TCP 확인 재전송 트래픽의 경우 TCP 패킷의 알려진 설정은 **queue-limit** 설정으로 무시됩니다. 다른 TCP 트래픽의 경우 무순서 패킷은 이제 버퍼링되며, 원래대로 전달되는 대신 순서가 지정됩니다.

예

다음 예는 모든 텔넷 연결에 대해 큐 제한을 8 패킷으로, 버퍼 시간 제한을 6초로 설정합니다.

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# queue-limit 8 timeout 6
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq telnet
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 정책에 대한 트래픽을 식별합니다.
policy-map	서비스 정책에서 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.

quit

현재의 컨피그레이션 모드를 종료하거나 특별 권한 또는 사용자 EXEC 모드에서 로그아웃하려면 **quit** 명령을 사용합니다.

quit

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

키 시퀀스 **Ctrl Z**를 사용하여 글로벌 컨피그레이션(및 그 이상) 모드를 종료할 수도 있습니다. 이 키 시퀀스는 특별 권한 또는 사용자 EXEC 모드와 작동하지 않습니다.

특별 권한 또는 사용자 EXEC 모드에서 **quit** 명령을 입력하면 ASA에서 로그아웃됩니다. 특별 권한 EXEC 모드에서 사용자 EXEC 모드로 돌아가려면 **disable** 명령을 사용합니다.

예

다음 예는 **quit** 명령을 사용하여 글로벌 컨피그레이션 모드를 종료한 다음 세션에서 로그아웃하는 방법을 보여줍니다.

```
ciscoasa(config)# quit
ciscoasa# quit

Logoff
```

다음 예는 **quit** 명령을 사용하여 글로벌 컨피그레이션 모드를 종료한 다음, **disable** 명령을 사용하여 특별 권한 EXEC 모드를 종료하는 방법을 보여줍니다.

```
ciscoasa(config)# quit
ciscoasa# disable
ciscoasa>
```

관련 명령

명령	설명
exit	컨피그레이션 모드를 종료하거나 특별 권한 또는 사용자 EXEC 모드에서 로그아웃합니다.

quota management-session

ASA에서 허용하는 동시 ASDM, SSH 및 텔넷 세션의 최대 개수를 설정하려면 글로벌 컨피그레이션 모드에서 **quota management-session** 명령을 사용합니다. 할당량을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

quota management-session *number*

no quota management-session *number*

구문 설명

number	허용되는 동시 ASDM, SSH, 텔넷 세션의 최대 개수를 지정합니다. 유효한 값은 0~10,000입니다.

기본값

기본값은 0입니다. 즉, 세션 제한이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.1(2)	이 명령이 추가되었습니다.

사용 지침

할당량에 도달하면 후속 관리 세션 요청이 거부되고 syslog 메시지가 생성됩니다. 관리 세션 할당량 메커니즘은 디바이스 잠금을 방지하기 위해 콘솔 세션을 차단하지 않습니다.

예

다음 예는 관리 세션 할당량을 100으로 구성합니다.

```
ciscoasa(config)# quota management-session 100
```

관련 명령

명령	설명
show run quota management-session	관리 세션 할당량의 현재 값을 표시합니다.
show quota management-session	관리 세션의 통계를 표시합니다.

radius-common-pw

ASA를 통해 RADIUS 인증 서버에 액세스하는 모든 사용자가 사용할 공통 비밀번호를 지정하려면 aaa-server host 컨피그레이션 모드에서 **radius-common-pw** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

radius-common-pw *string*

no radius-common-pw

구문 설명

string	대/소문자를 구분하는 최대 127자의 영숫자 키워드로 RADIUS 서버와의 모든 권한 부여 트랜잭션에 대한 공통 비밀번호로 사용됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
aaa-server host	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 RADIUS 인증 서버에 대해서만 유효합니다.

RADIUS 인증 서버에서는 각 연결 사용자에게 비밀번호와 사용자 이름을 요구합니다. ASA는 자동으로 사용자 이름을 제공합니다. 여기서 사용자 이름을 입력합니다. RADIUS 서버 관리자는 이 ASA를 통해 서버에 대해 각 사용자를 인증하도록 RADIUS 서버를 구성해야 합니다. 이 정보를 RADIUS 서버 관리자에게 이 정보를 제공해야 합니다.

공통 사용자 비밀번호를 지정하지 않으면 각 사용자 비밀번호는 사용자 이름입니다. 공통 사용자 비밀번호에 사용자 이름을 사용하는 경우, 보안 예방 조치로서 네트워크의 다른 곳에서는 RADIUS 서버를 권한 부여에 사용하지 마십시오.

참고 *string* 인수는 기본적으로 공간을 채우는 역할을 합니다. RADIUS 서버는 이를 기대하고 요구하지만 사용하지는 않습니다. 사용자는 이에 대해 알 필요가 없습니다.

예

다음 예는 호스트 "1.2.3.4"에서 "svrgrp1"이라는 RADIUS AAA 서버 그룹을 구성하고, 시간 제한 간격을 9초로 설정하고, 재시도 간격을 7초로 설정하며, RADIUS 공통 비밀번호를 "allauthpw"로 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# radius-common-pw allauthpw
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
clear configure aaa-server	컨피그레이션에서 모든 AAA 명령문을 제거합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

radius-reject-message

인증이 거부될 때 로그인 화면에서 RADIUS 거부 메시지의 표시를 활성화하려면 tunnel-group webvpn attributes 컨피그레이션 모드에서 **radius-eject-message** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

radius-reject-message

no radius-reject-message

기본값

기본값은 disabled입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

원격 사용자에게 인증 실패에 대한 RADIUS 메시지를 표시하려면 이 명령을 활성화합니다.

예

다음 예는 engineering이라는 연결 프로필에 대해 RADIUS 거부 메시지의 표시를 활성화합니다.

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry(removed)

인증 중에 ASA가 MS-CHAPv2를 사용하여 사용자와 비밀번호 업데이트를 협상하도록 하려면 tunnel-group ipsec-attributes 컨피그레이션 모드에서 **radius-with-expiry** 명령을 사용합니다. 기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

radius-with-expiry

no radius-with-expiry

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

이 명령의 기본 설정은 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tunnel-group ipsec-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.1(1)	이 명령은 사용이 중단되었습니다. 대신 **password-management** 명령이 사용됩니다. **radius-with-expiry** 명령의 **no** 형식은 더 이상 지원되지 않습니다.
8.0(2)	이 명령은 사용이 중단되었습니다.

사용 지침

이 특성은 IPSec remote-access tunnel-group 유형에만 적용할 수 있습니다. RADIUS 인증이 구성되어 있지 않으면 ASA는 이 명령을 무시합니다.

예

config-ipsec 컨피그레이션 모드에서 입력할 수 있는 다음 예는 remotegrp라는 원격 액세스 터널 그룹에 대해 Radius with Expiry를 구성합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# radius-with-expiry
```

관련 명령

명령	설명
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
password-management	비밀번호 관리를 활성화합니다. tunnel-group general-attributes 컨피그레이션 모드의 이 명령은 **radius-with-expiry** 명령을 교체합니다.
show running-config tunnel-group	표시된 인증서 맵 엔트리를 보여줍니다.
tunnel-group ipsec-attributes	이 그룹에 대한 터널 그룹 IPsec 특성을 구성합니다.

range

네트워크 객체에 대해 주소의 범위를 구성하려면 객체 컨피그레이션 모드에서 **range** 명령을 사용합니다. 컨피그레이션에서 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

range *ip_addr_1 ip_addr2*

no range *ip_addr_1 ip_addr2*

구문 설명

ip_addr_1	범위에서 첫 번째 IP 주소를 식별합니다(IPv4 또는 IPv6).
ip_addr_2	범위에서 마지막 IP 주소를 식별합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
객체 네트워크 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.3(1)	이 명령이 추가되었습니다.
9.0(1)	IPv6 주소에 대한 지원을 추가했습니다.

사용 지침

기존 네트워크 객체를 다른 IP 주소로 구성하면 새 컨피그레이션이 기존 컨피그레이션을 교체합니다.

예

다음 예는 범위 네트워크 객체를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# object network OBJECT_RANGE
ciscoasa (config-network-object)# range 10.1.1.1 10.1.1.8
```

관련 명령

명령	설명
clear configure object	생성된 모든 객체를 지웁니다.
description	네트워크 객체에 설명을 추가합니다.
fqdn	정규화된 도메인 이름 네트워크 객체를 지정합니다.
host	호스트 네트워크 객체를 지정합니다.
nat	네트워크 객체에 대해 NAT를 활성화합니다.
object network	네트워크 객체를 만듭니다.
object-group network	네트워크 객체 그룹을 만듭니다.
show running-config object network	네트워크 객체 컨피그레이션을 보여줍니다.
subnet	서브넷 네트워크 객체를 지정합니다.

ras-rcf-pinholes

게이트키퍼가 네트워크 내부에 있을 때 H.323 엔드포인트 간 통화 설정을 활성화하려면 매개변수 컨피그레이션 모드에서 **ras-rcf-pinholes** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ras-rcf-pinholes enable

no ras-rcf-pinholes enable

구문 설명

enable	H.323 엔드포인트 간 통화 설정을 활성화합니다.

기본값

기본적으로 이 옵션은 사용되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(5)	이 명령이 추가되었습니다.

사용 지침

ASA에는 RRQ/RCF(RegistrationRequest/RegistrationConfirm) 메시지를 기반으로 통화에 대한 핀홀을 열기 위한 옵션이 포함되어 있습니다. 이러한 RRQ/RCF 메시지는 게이트키퍼에서 보내고 받으므로, 통화 엔드포인트의 IP 주소는 알 수 없으며 ASA에서는 소스 IP 주소/포트 0/0을 통해 핀홀을 엽니다.

예

다음 예는 정책 맵에서 작업을 설정하여 이러한 통화용 핀홀을 여는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ras-rcf-pinholes enable
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

rate-limit

Modular Policy Framework를 사용할 때, 일치 또는 클래스 컨피그레이션 모드에서 **rate-limit** 명령을 사용하여 **match** 명령 또는 클래스 맵과 일치하는 패킷에 대해 메시지의 속도를 제한합니다. 이 속도 제한 작업은 검사 정책 맵에서 애플리케이션 트래픽에 대해 사용 가능하지만(**policy-map type inspect** 명령), 모든 애플리케이션에서 이 작업을 허용하는 것은 아닙니다. 이 작업을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

rate-limit *messages_per_second*

no rate-limit *messages_per_second*

구문 설명

messages_per_second	초당 메시지 수를 제한합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
일치 및 클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

검사 정책 맵은 **match** 및 **class** 명령으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 명령은 애플리케이션에 따라 다릅니다. **match** 또는 **class** 명령을 입력하여 애플리케이션 트래픽을 식별한 후(**class** 명령은 기존의 **class-map type inspect** 명령을 참조하며, 여기에 **match** 명령이 포함됨), **rate-limit** 명령을 입력하여 메시지의 속도를 제한할 수 있습니다.

Layer 3/4 정책 맵에서(**policy-map** 명령) **inspect** 명령을 사용하여 애플리케이션 검사를 활성화할 경우 이 작업을 포함하는 검사 정책 맵을 활성화할 수 있습니다. 예를 들어 **inspect dns dns_policy_map** 명령(dns_policy_map은 검사 정책 맵의 이름)을 입력할 수 있습니다.

예

다음 예는 초대 요청을 초당 메시지 수 100개로 제한합니다.

```
ciscoasa(config-cmap)# policy-map type inspect sip sip-map1
ciscoasa(config-pmap-c)# match request-method invite
ciscoasa(config-pmap-c)# rate-limit 100
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
policy-map type inspect	애플리케이션 검사를 위한 특수 작업을 정의합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

reactivation-mode

그룹에서 실패한 서버의 재활성화 방법을 지정하려면 aaa-server protocol 모드에서 **reactivation-mode** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

no reactivation-mode [**depletion** [**deadtime** *minutes*] | **timed**]

구문 설명

deadtime *minutes*	(선택 사항) 그룹의 마지막 서버를 비활성화한 시점부터 나중에 모든 서버를 다시 활성화한 시점까지 경과한 시간(분)을 0~1440 범위에서 지정합니다. 기본값은 10분입니다.
depletion	그룹의 모든 서버가 비활성화된 이후에야 실패한 서버를 재활성화합니다.
timed	가동 중단되고 30초가 지나면 실패한 서버를 재활성화합니다.

기본값

기본 재활성화 모드는 depletion이고 기본 deadtime 값은 10입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Aaa-server 프로토콜 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

각 서버 그룹에는 서버에 대한 재활성화 정책을 지정하는 특성이 있습니다.

depletion 모드에서 특정 서버가 비활성화되면 그룹의 다른 모든 서버가 비활성화될 때까지 비활성 상태가 유지됩니다. 이러한 상황이 발생하면 그룹의 모든 서버가 재활성화됩니다. 이 접근 방식은 실패한 서버로 인한 연결 지연 발생을 최소화합니다. **depletion** 모드가 사용 중일 경우 **deadtime** 매개변수도 지정할 수 있습니다. **deadtime** 매개변수는 그룹의 마지막 서버가 비활성화되는 시점부터 나중에 모든 서버가 다시 활성화되는 시점까지의 경과 시간(분)을 지정합니다. 이 매개변수는 서버 그룹을 로컬 대안 기능과 함께 사용 중인 경우에만 의미가 있습니다.

Timed 모드에서는 가동 중단 후 30초가 지나면 실패한 서버가 재활성화됩니다. 이 기능은 고객이 서버 목록의 첫 번째 서버를 기본 서버로 사용하면서 가능한 한 온라인 상태로 유지하려는 경우 유용합니다. UDP 서버의 경우에는 이 정책이 불필요합니다. UDP 서버에 대한 연결은 실패하지 않으므로(서버가 없는 경우에도) UDP 서버는 맹목적으로 온라인 상태로 되돌아가게 됩니다. 따라서 서버 목록에 여러 도달할 수 없는 서버가 있는 경우에는 연결 시간이 느려지거나 연결이 실패할 수 있습니다.

동시 어카운팅이 활성화된 어카운팅 서버 그룹은 강제로 **timed** 모드를 사용하게 됩니다. 이는 지정된 목록의 모든 서버가 동등함을 의미합니다.

예

다음 예는 deadtime 15분, depletion 재활성화 모드를 사용하여 "srvgrp1"이라는 TACACS+ AAA 서버를 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
ciscoasa(config-aaa-server)# exit
ciscoasa(config)#
```

다음 예는 timed 재활성화 모드를 사용하여 "srvgrp1"이라는 TACACS+ AAA 서버를 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp2 protocol tacacs+
ciscoasa(config-aaa-server)# reactivation-mode timed
ciscoasa(config-aaa-server)#
```

관련 명령

accounting-mode	어카운팅 메시지를 단일 서버로 전송할지 아니면 그룹의 모든 서버로 전송할지를 나타냅니다.
aaa-server protocol	그룹과 관련되고 그룹 내 모든 호스트에 공통된 AAA 서버 매개변수를 구성할 수 있도록 aaa-server group 컨피그레이션 모드로 들어갑니다.
max-failed-attempts	서버가 비활성화되기까지 서버 그룹의 특정 서버에 대해 허용되는 실패 횟수를 지정합니다.
clear configure aaa-server	모든 AAA server 컨피그레이션을 제거합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.

record-entry

CTL 파일 생성에 사용할 신뢰 지점을 지정하려면 ctl-file 컨피그레이션 모드에서 record-entry 명령을 사용합니다. CTL에서 레코드 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

no record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trust_point* **address** *ip_address* [**domain-name** *domain_name*]

구문 설명

capf	이 신뢰 지점의 역할을 CAPF로 지정합니다. CAPF 신뢰 지점을 하나만 구성할 수 있습니다.
cucm	이 신뢰 지점의 역할을 CCM으로 지정합니다. 여러 CCM 신뢰 지점을 구성할 수 있습니다.
cucm-tftp	이 신뢰 지점의 역할을 CCM+TFTP로 지정합니다. 여러 CCM+TFTP 신뢰 지점을 구성할 수 있습니다.
domain-name *domain_name*	(선택 사항) 신뢰 지점에 대한 DNS 필드 생성에 사용할 신뢰 지점의 도메인 이름을 지정합니다. Subject DN의 Common Name 필드에 추가되어 DNS Name을 생성합니다. 신뢰 지점에 대해 FQDN이 구성되지 않은 경우 도메인 이름을 구성해야 합니다.
address *ip_address*	신뢰 지점의 IP 주소를 지정합니다.
tftp	이 신뢰 지점의 역할을 TFTP로 지정합니다. 여러 TFTP 신뢰 지점을 구성할 수 있습니다.
trustpoint *trust_point*	설치된 신뢰 지점의 이름을 설정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
CTL-file 구성	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(4)	이 명령이 추가되었습니다.

사용 지침

도메인 이름을 하나만 지정할 수 있습니다. CTL 파일이 없으면 CUCM에서 ASA로 이 인증서를 수동으로 내보내십시오.

Phone Proxy에 대해 CTL 파일을 구성하지 않은 경우에만 이 명령을 사용하고, 이미 CTL 파일을 구성한 경우에는 이 명령을 사용하지 마십시오.

ip_address 인수에서 지정하는 IP 주소는 신뢰 지점의 CTL 레코드에 사용되는 IP 주소이므로 전역 주소이거나 IP Phone에서 볼 수 있는 주소여야 합니다.

CTL 파일에 필요한 각 엔티티에 대해 record-entry 구성을 추가합니다.

예

다음 예는 **record-entry** 명령을 사용하여 CTL 파일 생성에 사용할 신뢰 지점을 지정하는 방법을 보여줍니다.

```
ciscoasa(config-ctl-file)# record-entry cucm-tftp trustpoint cucm1 address 192.168.1.2
```

관련 명령

명령	설명
ctl-file (global)	전화 프록시 컨피그레이션을 만들기 위한 CTL 파일 또는 플래시 메모리에서 구문 분석하기 위한 CTL 파일을 지정합니다.
ctl-file (phone-proxy)	전화 프록시 컨피그레이션에 사용할 CTL 파일을 지정합니다.
phone-proxy	Phone Proxy 인스턴스를 구성합니다.

redirect-fqdn

vpn 로드 밸런싱 모드에서 정규화된 도메인 이름을 사용하여 리디렉션을 활성화 또는 비활성화하려면 글로벌 컨피그레이션 모드에서 **redirect-fqdn enable** 명령을 사용합니다.

redirect-fqdn {enable | disable}

no redirect-fqdn {enable | disable}

참고 VPN 로드 밸런싱을 사용하려면 Plus 라이센스의 ASA Model 5510 또는 ASA Model 5520 이상이 필요합니다. VPN 로드 밸런싱에는 활성 3DES/AES 라이센스도 필요합니다. 보안 어플라이언스는 로드 밸런싱을 활성화하기 전에 이 암호화 라이센스의 존재 여부를 확인합니다. 활성 3DES 또는 AES 라이센스가 감지되지 않으면 라이센스에서 허용하지 않는 한, 보안 어플라이언스는 로드 밸런싱의 활성화를 차단하고 로드 밸런싱에 의한 3DES의 내부 구성도 차단합니다.

구문 설명

disable	정규화된 도메인 이름을 이용한 리디렉션을 비활성화합니다.
enable	정규화된 도메인 이름을 이용한 리디렉션을 활성화합니다.

기본값

이 동작은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
VPN 로드 밸런싱 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

기본적으로 ASA는 로드 밸런싱 리디렉션에서 IP 주소만 클라이언트로 전송합니다. DNS 이름 기반의 인증서가 사용 중인 경우 보조 디바이스로 리디렉션된 인증서는 무효화됩니다.

VPN 클러스터 마스터로서 ASA는 VPN 클라이언트 연결을 해당 클러스터 디바이스로 리디렉션할 경우, 역방향 DNS 조회를 사용하여 클러스터 디바이스(클러스터의 또 다른 ASA)의 외부 IP 주소 대신 FQDN(정규화된 도메인 이름)을 전송할 수 있습니다.

클러스터 내 로드 밸런싱 디바이스의 모든 외부 및 내부 네트워크 인터페이스는 동일한 IP 네트워크에 있어야 합니다.

IP 주소 대신 FQDN을 사용하여 WebVPN 로드 밸런싱을 수행하려면 다음의 컨피그레이션 단계를 따라야 합니다.

1 단계 **redirect-fqdn enable** 명령으로 로드 밸런싱에 대한 FQDN 의 사용을 활성화합니다 .

2단계 ASA 외부 인터페이스 각각에 대한 엔트리를 DNS 서버에 추가합니다(해당 엔트리가 아직 없는 경우). 각 ASA 외부 IP 주소에는 조회를 위한 관련 DNS 엔트리가 있어야 합니다. 역방향 조회에 대해서도 이러한 DNS 엔트리를 활성화해야 합니다.

3단계 "dns domain-lookup inside" 명령으로 ASA(또는 DNS 서버에 대한 경로가 있는 인터페이스)에서 DNS 조회를 활성화합니다.

4단계 ASA에서 DNS 서버 IP 주소를 정의합니다(예: `dns name-server 10.2.3.4`)(DNS 서버의 IP 주소).

예

다음은 리디렉션을 비활성화하는 **redirect-fqdn** 명령의 예입니다.

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# redirect-fqdn disable
ciscoasa(config-load-balancing)#
```

다음은 정규화된 도메인 이름의 리디렉션을 활성화하는 인터페이스 명령이 포함된 VPN 로드 밸런싱 명령 시퀀스의 예로서, 클러스터의 공개 인터페이스를 "test"로 지정하고 클러스터의 비공개 인터페이스를 "foo"로 지정합니다.

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# redirect-fqdn enable
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
clear configure vpn load-balancing	로드 밸런싱 런타임 컨피그레이션을 제거하고 로드 밸런싱을 비활성화합니다.
show running-config vpn load-balancing	현재의 VPN 로드 밸런싱 가상 클러스터 컨피그레이션을 표시합니다.
show vpn load-balancing	VPN 로드 밸런싱 런타임 통계를 표시합니다.
vpn load-balancing	VPN 로드 밸런싱 모드로 들어갑니다.

redistribute

한 라우팅 도메인에서 다른 라우팅 도메인으로 경로를 재배포하려면 적절한 컨피그레이션 모드에서 **redistribute** 명령을 사용합니다. 재배포를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

redistribute *protocol* [*process-id*] [*autonomous-system-number*][**metric** {*metric-value* | **transparent**}][**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

no redistribute *protocol* [*process-id*] [*autonomous-system-number*][**metric** {*metric-value* | **transparent**}][**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

구문 설명

protocol	경로가 재배포되는 소스 프로토콜로서, 다음 키워드 중 하나일 수 있습니다. **bgp**, **connected**, **eigrp**, ,**ospf**, **static** 또는 **rip**. **static** 키워드는 IP 고정 경로를 재배포하는 데 사용됩니다. **connected** 키워드는 인터페이스에서 IP를 활성화함으로써 자동으로 설정되는 경로를 참조합니다. OSPF(Open Shortest Path First) 같은 라우팅 프로토콜의 경우 이러한 경로는 외부(external)로서 자동 시스템에 재배포됩니다.
process-id	(선택 사항) **bgp** 또는 **eigrp** 키워드의 경우에는 16비트 십진수의 자동 시스템 번호입니다. **ospf** 키워드의 경우에는 경로가 재배포되는 적절한 OSPF 프로세스 ID입니다. 이것은 라우팅 프로세스를 식별합니다. 이 값은 0이 아닌 10진수 형태를 취합니다. **rip** 키워드의 경우 *process-id* 값이 필요하지 않습니다. 기본적으로 프로세스 ID는 정의되지 않습니다.
autonomous-system-number	(선택 사항) 재배포된 경로의 자동 시스템 번호입니다. 범위는 1~65535입니다. • Cisco IOS 릴리스 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE 릴리스 2.4 및 그 이후의 릴리스에서는 asplain 표기법의 경우 65536~4294967295 범위, asdot 표기법의 경우 1.0~65535.65535 범위의 4바이트 자동 시스템 번호가 지원됩니다. • Cisco IOS 릴리스 12.0(32)S12, 12.4(24)T 및 Cisco IOS XE 릴리스 2.3에서는 asdot 표기법으로만 1.0~65535.65535 범위의 자동 시스템 번호가 지원됩니다. 자동 시스템 번호 형식에 대한 자세한 내용은 **router bgp** 명령을 참조하십시오.
metric *metric-value*	(선택 사항) 하나의 OSPF 프로세스에서 동일한 라우터의 다른 OSPF 프로세스로 재배포할 경우, 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재배포할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다. 기본값은 0입니다.

metric transparent	(선택 사항) 재배포된 경로에 대한 라우팅 테이블 메트릭을 RIP에서 RIP 메트릭으로 사용하도록 지정합니다.
metric-type *type-value*	(선택 사항) OSPF의 경우, OSPF 라우팅 도메인으로 광고된 기본 경로와 연결된 외부 링크 유형을 지정합니다. 다음 두 값 중 하나일 수 있습니다. • **1** - Type 1 외부 경로 • **2** - Type 2 외부 경로 **metric-type**이 지정되지 않은 경우 Cisco IOS 소프트웨어는 Type 2 외부 경로를 채택합니다.
match {internal | external 1 | external 2}	(선택 사항) OSPF 경로가 다른 라우팅 도메인으로 재배포되는 기준. 다음 중 하나일 수 있습니다. • **internal -** 특정 자동 시스템에 대해 내부인 경로. • **external 1** - 자동 시스템에 대해 외부이지만, OSPF에 Type 1 외부 경로로서 가져오는 경로입니다. • **external 2** - 자동 시스템에 대해 외부이지만, OSPF에 Type 2 외부 경로로서 가져오는 경로입니다. 기본값은 internal 및 external 1입니다.
tag *tag-value*	(선택 사항) 각 외부 경로에 연결되는 32비트 십진수 값을 지정합니다. OSPF 자체에서는 이 값을 사용하지 않습니다. ASBR(Autonomous System Boundary Router) 간에 정보를 교환하는 데 사용될 수 있습니다. 아무것도 지정하지 않으면 BGP(Border Gateway Protocol) 및 EGP(Exterior Gateway Protocol)의 경로에 원격 자동 시스템 번호가 사용됩니다. 다른 프로토콜에는 영(0)이 사용됩니다.
route-map	(선택 사항) 이 소스 라우팅 프로토콜에서 현재의 라우팅 프로토콜로의 경로 가져오기를 필터링하기 위해 검증해야 할 경로 맵을 지정합니다. 지정하지 않으면 모든 경로가 재배포됩니다. 이 키워드를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다.
map-tag	(선택 사항) 구성된 경로 맵의 식별자.
subnets	(선택 사항) OSPF로 경로를 재배포할 경우 지정된 프로토콜에 대한 재배포의 범위. 기본적으로 서브넷이 정의되지 않습니다.
nssa-only	(선택 사항) OSPF로 재배포된 모든 경로에 대해 nssa-only 특성을 설정합니다.

기본값

경로 재배포가 비활성화됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

키워드의 변경 또는 비활성화는 다른 키워드의 상태에 영향을 미치지 않습니다.

내부 메트릭으로 link-state 프로토콜을 수신하는 라우터는 자체에서 재배포하는 라우터까지의 경로 비용은 물론 목적지에 도달하기 위한 광고 비용도 고려하게 됩니다. 외부 메트릭은 목적지에 도달하기 위한 광고 메트릭만 고려합니다.

재배포된 라우팅 정보는 **distribute-list out** 라우터 컨피그레이션 명령으로 필터링해야 합니다. 이 지침은 관리자가 의도하는 경로만 수신 라우팅 프로토콜로 전달되도록 보장합니다.

redistribute 또는 **default-information** 라우터 컨피그레이션 명령을 사용하여 OSPF 라우팅 도메인으로 경로를 재배포할 때마다 라우터는 자동으로 ASBR이 됩니다. 그러나 ASBR은 기본적으로 OSPF 라우팅 도메인에 *기본 경로*를 생성하지 않습니다.

OSPF 또는 BGP 이외의 프로토콜에서 OSPF로 경로가 재배포되고 **metric-type** 키워드 및 *type-value* 인수로 메트릭을 지정하지 않은 경우, OSPF는 20을 기본 메트릭으로 사용합니다. BGP에서 OSPF로 경로가 재배포되는 경우 OSPF는 1을 기본 메트릭으로 사용합니다. 한 OSPF 프로세스에서 다른 OSPF 프로세스로 경로가 재배포되는 경우, AS(자동 시스템) 외부 및 NSSA(not-so-stubby-area) 경로는 20을 기본 메트릭으로 사용합니다. OSPF 프로세스 간에 intra-area 및 inter-area 경로가 재배포되는 경우, 재배포 소스 프로세스의 내부 OSPF 메트릭은 재배포 대상 프로세스에서 외부 메트릭으로서 광고됩니다. (이것이 OSPF로 경로가 재배포될 때 라우팅 테이블 메트릭이 유지되는 유일한 경우입니다.)

경로를 OSPF로 재배포할 경우 **subnets** 키워드를 지정하지 않으면 서브넷으로 지정되지 않은 경로만 재배포됩니다.

NSSA 영역에 대해 내부인 라우터에서 **nssa-only** 키워드를 사용하면 원래의 type-7 NSSA LSA에서 P(propagate) 비트가 0으로 설정되는데, 이 경우 ABR(영역 경계선 라우터)은 이러한 LSA를 type-5 외부 LSA로 변환하지 못합니다. NSSA 및 일반 영역에 연결된 ABR에서 **nssa-only** 키워드를 사용하면 경로가 NSSA 영역으로만 재배포됩니다.

이 **redistribute** 명령의 영향을 받는 **connected** 키워드로 구성된 경로는 **network** 라우터 컨피그레이션 명령으로 지정되지 않은 경로입니다.

default-metric 명령으로는 연결된 경로를 광고하는 데 사용되는 메트릭에 영향을 미칠 수 없습니다.

참고 **redistribute** 명령으로 지정한 **metric** 값은 **default-metric** 명령으로 지정한 **metric** 값을 대체합니다.

default-information originate 라우터 컨피그레이션 명령을 지정하지 않는 한, IGP 또는 EGP에서 BGP로의 기본 재배포는 허용되지 않습니다.

redistribute 명령의 no 형식 사용

redistribute 명령에 대해 구성한 옵션을 제거하려는 경우 원하는 결과를 얻으려면 **redistribute** 명령의 **no** 형식을 신중하게 사용해야 합니다. 자세한 내용은 "예" 섹션을 참조하십시오.

4바이트 자동 시스템 번호 지원

Cisco의 4바이트 자동 시스템 번호 구현에서는 자동 시스템 번호에 대한 기본 정규식 일치 및 출력 표시 형식으로서 asplain(예: 65538)을 사용합니다. 그러나 RFC 5396에 설명된 대로 asplain 형식 및 asdot 형식 모두로 4바이트 자동 시스템 번호를 구성할 수 있습니다. 4바이트 자동 시스템 번호의 기본 정규식 일치 및 출력 표시를 asdot 형식으로 변경하려면 **bgp asnotation dot** 명령을 사용합니다.

EIGRP 컨피그레이션에 **default-metric** 명령이 없는 경우 redistribute 명령으로 **metric**을 지정해야 합니다.

예

다음 예는 OSPF 경로를 BGP 도메인으로 재배포하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# redistribute ospf
```

다음 예에서는 EIGRP 경로가 OSPF 도메인으로 재배포됩니다.

```
ciscoasa(config)# router ospf 110
ciscoasa(config-router)# redistribute eigrp
```

다음 예에서는 지정된 EIGRP 프로세스 경로가 OSPF 도메인으로 재배포됩니다. EIGRP에서 파생된 메트릭은 100으로 리맵되고 RIP 경로는 200으로 리맵됩니다.

```
ciscoasa(config)# router ospf 109
ciscoasa(config-router)# redistribute eigrp 108 metric 100 subnets
ciscoasa(config-router)# redistribute rip metric 200 subnets
```

다음 예에서 네트워크 172.16.0.0은 OSPF 1에서 비용(cost) 100과 함께 외부 LSA(link-state advertisement)로 나타납니다(비용은 유지됨).

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ip address 172.16.0.1 255.0.0.0
ciscoasa(config)#  ospf cost 100
ciscoasa(config)# interface ethernet 1
ciscoasa(config-if)#ip address 10.0.0.1 255.0.0.0
!
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0 0.255.255.255 area 0
ciscoasa(config-router)# redistribute ospf 2 subnet
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

다음 예는 BGP 경로를 OSPF에 재배포하고 로컬 4바이트 자동 시스템 번호를 asplain 형식으로 할당하는 방법을 보여줍니다.

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# redistribute bgp 65538
```

다음 예는 **redistribute connected metric 1000 subnets** 명령에서 **connected metric 1000 subnets** 옵션을 제거하고 컨피그레이션에 **redistribute connected** 명령을 남겨둡니다.

```
ciscoasa(config-router)# no redistribute connected metric 1000 subnets
```

다음 예는 **redistribute connected metric 1000 subnets** 명령에서 **metric 1000** 옵션을 제거하고 컨피그레이션에 **redistribute connected subnets** 명령을 남겨둡니다.

```
ciscoasa(config-router)# no redistribute connected metric 1000
```

다음 예는 **redistribute connected metric 1000 subnets** 명령에서 **subnets** 옵션을 제거하고 컨피그레이션에 **redistribute connected metric 1000** 명령을 남겨둡니다.

```
ciscoasa(config-router)# no redistribute connected subnets
```

다음 예는 **redistribute connected** 명령, 그리고 **redistribute connected** 명령에 대해 구성되었던 모든 옵션을 컨피그레이션에서 제거합니다.

```
ciscoasa(config-router)# no redistribute connected
```

redistribute(EIGRP)

한 라우팅 도메인에서 EIGRP 라우팅 프로세스로 경로를 재배포하려면 라우터 컨피그레이션 모드에서 **redistribute** 명령을 사용합니다. 재배포를 제거하려면 이 명령의 **no** 형식을 사용합니다.

redistribute {{**eigrp** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

no redistribute {{**eigrp** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

구문 설명

bandwidth	초당 킬로비트 단위의 EIGRP 대역폭 메트릭. 유효한 값은 1~4294967295입니다.
connected	인터페이스에 연결된 네트워크를 EIGRP 라우팅 프로세스로 재배포함을 지정합니다.
delay	10밀리초 단위의 EIGRP 지연 메트릭. 유효한 값은 0~4294967295입니다.
external *type*	지정된 자동 시스템에 대해 외부인 EIGRP 메트릭 경로를 지정합니다. 유효한 값은 **1** 또는 **2**입니다.
internal *type*	지정된 자동 시스템에 대해 내부인 EIGRP 메트릭 경로를 지정합니다.
load	EIGRP 유효 대역폭(로딩) 메트릭. 유효한 값은 1~255입니다. 255는 100% 로드되었음을 나타냅니다.
match	(선택 사항) OSPF에서 EIGRP로의 경로 재배포 조건을 지정합니다.
metric	(선택 사항) EIGRP 라우팅 프로세스에 재배포된 경로의 EIGRP 메트릭에 대한 값을 지정합니다.
mtu	경로의 MTU. 유효한 값은 1~65535입니다.
nssa-external *type*	NSSA에 대해 외부인 경로의 EIGRP 메트릭 유형을 지정합니다. 유효한 값은 **1** 또는 **2**입니다.
eigrp *pid*	EIGRP 라우팅 프로세스의 경로를 EIGRP 라우팅 프로세스에 재배포하는 데 사용됩니다. *pid*는 EIGRP 라우팅 프로세스에 대해 내부적으로 사용되는 식별 매개변수를 지정하며, 유효한 값은 1~65535입니다.
reliability	EIGRP 신뢰성 메트릭. 유효한 값은 0~255입니다. 255는 100% 신뢰성을 나타냅니다.
rip	RIP 라우팅 프로세스에서 EIGRP 라우팅 프로세스로의 네트워크 재배포를 지정합니다.
route-map *map_name*	(선택 사항) 소스 라우팅 프로토콜에서 EIGRP 라우팅 프로세스로 가져온 경로를 필터링하는 데 사용되는 경로 맵의 이름입니다. 지정하지 않으면 모든 경로가 재배포됩니다.
static	고정 경로를 EIGRP 라우팅 프로세스에 재배포하는 데 사용됩니다.

기본값

다음은 명령 기본값입니다.

- **match**: **Internal**, **external 1**, **external 2**

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

명령 모드	방화벽 모드		보안 컨텍스트		
	라우팅	투명성	단일	다중	
				컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

EIGRP 컨피그레이션에 **default-metric** 명령이 없는 경우 redistribute 명령으로 **metric**을 지정해야 합니다.

예

다음 예는 고정 및 연결된 경로를 EIGRP 라우팅 프로세스에 재배포합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# redistribute static
ciscoasa(config-router)# redistribute connected
```

관련 명령

명령	설명
router eigrp	EIGRP 라우팅 프로세스를 생성하고 이 프로세스에 대한 컨피그레이션 모드로 들어갑니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

redistribute(OSPF)

한 라우팅 도메인에서 OSPF 라우팅 프로세스로 경로를 재배포하려면 라우터 컨피그레이션 모드에서 **redistribute** 명령을 사용합니다. 포함된 옵션이 없을 때 재배포를 제거하려면 이 명령의 **no** 형식을 사용합니다. 옵션이 하나 포함된 상태에서 이 명령의 **no** 형식을 사용하면 해당 옵션에 대한 컨피그레이션만 제거됩니다.

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected** | **eigrp** *as-number*} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

구문 설명

connected	인터페이스에 연결된 네트워크를 OSPF 라우팅 프로세스로 재배포함을 지정합니다.
eigrp *as-number*	EIGRP 경로를 OSPF 라우팅 프로세스에 재배포하는 데 사용됩니다. *as-number*는 EIGRP 라우팅 프로세스의 자동 시스템 번호를 지정합니다. 유효한 값은 1~65535입니다.
external *type*	지정된 자동 시스템에 대해 외부인 OSPF 메트릭 경로를 지정합니다. 유효한 값은 **1** 또는 **2**입니다.
internal *type*	지정된 자동 시스템에 대해 내부인 OSPF 메트릭 경로를 지정합니다.
match	(선택 사항) 하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 지정합니다.
metric *metric_value*	(선택 사항) 0~16777214 범위에서 OSPF 기본 메트릭 값을 지정합니다.
metric-type *metric_type*	(선택 사항) OSPF 라우팅 도메인으로 광고된 기본 경로와 연결된 외부 링크 유형. 값은 **1**(Type 1 외부 경로) 또는 **2**(Type 2 외부 경로)가 될 수 있습니다.
nssa-external *type*	NSSA에 대해 외부인 경로의 OSPF 메트릭 유형을 지정합니다. 유효한 값은 **1** 또는 **2**입니다.
ospf *pid*	OSPF 라우팅 프로세스를 현재의 OSPF 라우팅 프로세스에 재배포하는 데 사용됩니다. *pid*는 OSPF 라우팅 프로세스에 대해 내부적으로 사용되는 식별 매개변수를 지정하며, 유효한 값은 1~65535입니다.
rip	RIP 라우팅 프로세스에서 현재의 OSPF 라우팅 프로세스로의 네트워크 재배포를 지정합니다.
route-map *map_name*	(선택 사항) 소스 라우팅 프로토콜에서 현재의 OSPF 라우팅 프로세스로 가져온 경로를 필터링하는 데 사용되는 경로 맵의 이름입니다. 지정하지 않으면 모든 경로가 재배포됩니다.
static	고정 경로를 OSPF 프로세스에 재배포하는 데 사용됩니다.
subnets	(선택 사항) OSPF로 경로를 재배포할 경우 지정된 프로토콜에 대한 재배포의 범위. 사용하지 않으면 classful 경로만 재배포됩니다.
tag *tag_value*	(선택 사항) 각 외부 경로에 연결되는 32비트 십진수 값. 이 값은 OSPF 자체에서는 사용되지 않지만, ASBR 간에 정보를 교환하는 데 사용될 수 있습니다. 아무것도 지정하지 않으면 BGP 및 EGP의 경로에 원격 자동 시스템 번호가 사용됩니다. 다른 프로토콜에는 영(0)이 사용됩니다. 유효한 값의 범위는 0~4294967295입니다.

기본값

다음은 명령 기본값입니다.

- **metric** *metric-value*: 0
- **metric-type** *type-value*: **2**
- **match**: **Internal**, **external 1**, **external 2**
- **tag** *tag-value*: 0

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	이 명령이 **rip** 키워드를 포함하도록 수정되었습니다.
8.0(2)	이 명령이 **eigrp** 키워드를 포함하도록 수정되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

예

다음 예는 고정 경로를 현재의 OSPF 프로세스로 재배포하는 방법을 보여줍니다.

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# redistribute static
```

관련 명령

명령	설명
redistribute (RIP)	RIP 라우팅 프로세스에 경로를 재배포합니다.
router ospf	라우터 컨피그레이션 모드로 들어갑니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

redistribute(OSPFv3)

한 OSPFv3 라우팅 도메인에서 다른 OSPFv3 라우팅 도메인으로 IPv6 경로를 재배포하려면 IPv6 라우터 컨피그레이션 모드에서 **redistribute** 명령을 사용합니다. 재배포를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

redistribute *source-protocol* [*process-id*] [**include-connected** {**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected** {**level-1** | **level-1-2** | **level-2**}] [*as-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

구문 설명

as-number	라우팅 프로세스의 자동 시스템 번호를 지정합니다. 유효한 값의 범위는 1~65535입니다.
external	지정된 자동 시스템에 대해 외부이지만 type 1 또는 type 2 외부 경로로서 OSPFv3으로 가져오는 OSPFv3 메트릭 경로를 지정합니다. 유효한 값은 1 또는 2입니다.
include-connected	(선택 사항) 대상 프로토콜에서는 소스 프로토콜 및 연결된 접두사를 통해 학습한 경로를 소스 프로토콜이 실행 중인 해당 인터페이스에 재배포할 수 있습니다.
internal	지정된 자동 시스템에 대해 내부인 OSPFv3 메트릭 경로를 지정합니다.
level-1	IS-IS(Intermediate System-to-Intermediate System)의 경우, Level 1 경로가 다른 IP 라우팅 프로토콜에 독립적으로 재배포되도록 지정합니다.
level-1-2	IS-IS의 경우, Level 1 및 Level 2 경로가 모두 다른 IP 라우팅 프로토콜에 독립적으로 재배포되도록 지정합니다.
level-2	IS-IS의 경우, Level 2 경로가 다른 IP 라우팅 프로토콜에 독립적으로 재배포되도록 지정합니다.
map-tag	(선택 사항) 구성된 경로 맵의 식별자를 지정합니다.
match	(선택 사항) 다른 라우팅 도메인에 경로를 재배포합니다.
metric *metric_value*	(선택 사항) 0~16777214 범위에서 OSPFv3 기본 메트릭 값을 지정합니다.
metric-type *metric_type*	(선택 사항) OSPFv3 라우팅 도메인으로 광고된 기본 경로와 연결된 외부 링크 유형을 지정합니다. 값은 1(Type 1 외부 경로) 또는 2(Type 2 외부 경로)가 될 수 있습니다.
nssa-external	자동 시스템의 외부에 있지만 IPv6용 NSSA(not so stubby area)의 OSPFv3에 Type 1 또는 Type 2 외부 경로로서 가져오는 경로를 지정합니다.
process-id	(선택 사항) OSPFv3 라우팅 프로세스가 활성화될 때 관리를 위해 할당되는 번호를 지정합니다.
route-map *map_name*	(선택 사항) 소스 라우팅 프로토콜에서 현재의 OSPFv3 라우팅 프로토콜로 가져온 경로를 필터링하는 데 사용되는 경로 맵의 이름을 지정합니다. 이 키워드를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다. 지정하지 않으면 모든 경로가 재배포됩니다.
source-protocol	경로가 재배포되는 소스 프로토콜을 지정합니다. connected, ospf 또는 static 중 하나가 될 수 있습니다.

tag *tag_value*	(선택 사항) 각 외부 경로에 연결되는 32비트 십진수 값을 지정합니다. 이 값은 OSPFv3에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있습니다. 아무것도 지정하지 않으면 BGP 및 EGP의 경로에 원격 자동 시스템 번호가 사용됩니다. 다른 프로토콜에는 영(0)이 사용됩니다. 유효한 값의 범위는 0~4294967295입니다.
transparent	(선택 사항) 재배포된 경로에 대한 라우팅 테이블 메트릭을 RIP에서 RIP 메트릭으로 사용하도록 지정합니다.

기본값

다음은 명령 기본값입니다.

- **metric** *metric-value*: **0**
- **metric-type** *type-value*: **2**
- **match**: **internal**, **external 1**, **external 2**
- **tag** *tag-value*: **0**

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
IPv6 라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

예

다음 예는 고정 경로를 현재의 OSPFv3 프로세스로 재배포하는 방법을 보여줍니다.

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# redistribute static
```

관련 명령

명령	설명
ipv6 router ospf	OSPFv3용 라우터 컨피그레이션 모드로 들어갑니다.
show running-config ipv6 router	OSPFv3용 라우터 컨피그레이션에서 명령을 표시합니다.

redistribute(RIP)

또 다른 라우팅 도메인에서 RIP 라우팅 프로세스로 경로를 재배포하려면 라우터 컨피그레이션 모드에서 **redistribute** 명령을 사용합니다. 재배포를 제거하려면 이 명령의 **no** 형식을 사용합니다.

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

구문 설명

connected	인터페이스에 연결된 네트워크를 RIP 라우팅 프로세스로 재배포함을 지정합니다.
eigrp *as-number*	EIGRP 경로를 RIP 라우팅 프로세스에 재배포하는 데 사용됩니다. *as-number*는 EIGRP 라우팅 프로세스의 자동 시스템 번호를 지정합니다. 유효한 값은 1~65535입니다.
external *type*	지정된 자동 시스템에 대해 외부인 OSPF 메트릭 경로를 지정합니다. 유효한 값은 **1** 또는 **2**입니다.
internal *type*	지정된 자동 시스템에 대해 내부인 OSPF 메트릭 경로를 지정합니다.
match	(선택 사항) OSPF에서 RIP로의 경로 재배포 조건을 지정합니다.
metric {*metric_value* | **transparent**}	(선택 사항) 재배포할 경로에 대한 RIP 메트릭 값을 지정합니다. *metric_value* 범위의 유효한 값은 0~16입니다. 메트릭을 **transparent**로 설정하면 현재 경로 메트릭이 사용됩니다.
nssa-external *type*	NSSA(not-so-stubby area)에 대해 외부인 경로의 OSPF 메트릭 유형을 지정합니다. 유효한 값은 **1** 또는 **2**입니다.
ospf *pid*	OSPF 라우팅 프로세스의 경로를 RIP 라우팅 프로세스에 재배포하는 데 사용됩니다. *pid*는 OSPF 라우팅 프로세스에 대해 내부적으로 사용되는 식별 매개변수를 지정하며, 유효한 값은 1~65535입니다.
route-map *map_name*	(선택 사항) 소스 라우팅 프로토콜에서 RIP 라우팅 프로세스로 가져온 경로를 필터링하는 데 사용되는 경로 맵의 이름입니다. 지정하지 않으면 모든 경로가 재배포됩니다.
static	고정 경로를 OSPF 프로세스에 재배포하는 데 사용됩니다.

기본값

다음은 명령 기본값입니다.

- **metric** *metric-value*: 0
- **match**: **Internal**, **external 1**, **external 2**

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.
8.0(2)	이 명령이 **eigrp** 키워드를 포함하도록 수정되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

예

다음 예는 고정 경로를 현재의 RIP 프로세스로 재배포하는 방법을 보여줍니다.

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# redistribute static metric 2
```

관련 명령

명령	설명
redistribute (EIGRP)	다른 라우팅 도메인에서 EIGRP로 경로를 재배포합니다.
redistribute (OSPF)	다른 라우팅 도메인에서 OSPF로 경로를 재배포합니다.
router rip	RIP 라우팅 프로세스를 활성화하고 해당 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

redundant-interface

이중화 인터페이스의 어떤 멤버 인터페이스를 액티브 상태로 만들 것인지를 설정하려면 특별 권한 EXEC 모드에서 **redundant-interface** 명령을 사용합니다.

redundant-interface redundant*number* **active-member** *physical_interface*

구문 설명

active-member *physical_interface*	액티브 멤버를 설정합니다. 허용되는 값은 **interface** 명령을 참조하십시오. 두 멤버 인터페이스 모두 물리적 유형이 같아야 합니다.
redundant *number*	이중화 인터페이스 ID(예: **redundant1**)를 지정합니다.

기본값

기본적으로, 액티브 인터페이스는 컨피그레이션에 나열된 사용 가능한 첫 번째 멤버 인터페이스입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

어떤 인터페이스가 액티브 인터페이스인지 확인하려면 다음 명령을 입력합니다.

```
ciscoasa# show interface redundantnumber detail | grep Member
```

예:

```
ciscoasa# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

예

다음 예는 이중화 인터페이스를 생성합니다. 기본적으로 gigabitethernet 0/0이 컨피그레이션에서 첫 번째 멤버이므로 액티브 인터페이스가 됩니다. redundant-interface 명령은 gigabitethernet 0/1을 액티브 인터페이스로 설정합니다.

```
ciscoasa(config-if)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1

ciscoasa(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

관련 명령

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
debug redundant-interface	이중화 인터페이스 이벤트 또는 오류와 관련된 디버그 메시지를 표시합니다.
interface redundant	이중화 인터페이스를 만듭니다.
member-interface	멤버 인터페이스를 이중화 인터페이스 쌍에 할당합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

regex

텍스트 확인을 위한 정규식을 만들려면 글로벌 컨피그레이션 모드에서 **regex** 명령을 사용합니다. 정규식을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

regex *name regular_expression*

no regex *name* [*regular_expression*]

구문 설명

name	정규식 이름을 최대 40자로 지정합니다.
regular_expression	정규식을 최대 100자로 지정합니다. 정규식에서 사용할 수 있는 메타 문자 목록은 "사용 지침" 섹션을 참조하십시오.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

regex 명령은 텍스트 매칭이 필요한 다양한 기능에 대해 사용할 수 있습니다. 예를 들면 *검사 정책 맵*을 사용하는 Modular Policy Framework를 사용하여 애플리케이션 검사에 대한 특별 작업을 구성할 수 있습니다(**policy map type inspect** 명령 참조). 검사 정책 맵에서, 하나 이상의 **match** 명령을 포함하는 검사 클래스 맵을 만들어 작업을 수행할 트래픽을 식별할 수 있습니다. 또는 검사 정책 맵에서 **match** 명령을 직접 사용할 수도 있습니다. 일부 **match** 명령을 사용하면 정규식을 사용하여 패킷에서 텍스트를 식별할 수 있습니다. 예를 들어, HTTP 패킷 내부에서 URL 문자열을 확인할 수 있습니다. 정규식 클래스 맵에서 정규식을 그룹화합니다(**class-map type regex** 명령 참조).

정규식은 있는 그대로의 정확한 문자열로서 텍스트 문자열을 확인하거나, *메타 문자*를 사용하여 텍스트 문자열의 다양한 변형을 확인합니다. 특정 애플리케이션 트래픽의 내용을 확인하기 위해 정규식을 사용할 수 있습니다. 예를 들면 HTTP 패킷 내에서 본문 텍스트를 확인할 수 있습니다.

참고 최적화를 위해 ASA는 애매함이 제거된(deobfuscated) URL에서 검색합니다. 애매함 제거 방식(Deobfuscation)에서는 여러 슬래시(/)를 단일 슬래시로 압축합니다. "http://"와 같이 일반적으로 이중 슬래시를 사용하는 문자열의 경우 "http:/"를 대신 검색해야 합니다.

표 18-1에는 특별한 의미가 있는 메타 문자가 나열되어 있습니다.

표 18-1 regex 메타 문자

문자	설명	참고
.	점	단일 문자와 일치합니다. 예를 들어 **d.g**는 dog, dag, dtg 및 그러한 문자가 포함된 단어(예: doggonnit)와 일치합니다.
(*exp*)	하위 식	하위 식은 문자를 주변 문자와 분리하므로, 하위 식에서 기타 메타 문자를 사용할 수 있습니다. 예를 들어, **d(ola)g**는 dog 및 dag와 일치하지만, **dolag**는 do 및 ag와 일치합니다. 하위 식을 반복 한정자와 함께 사용하면 반복을 의미하는 문자를 구분할 수 있습니다. 예를 들어 **ab(xy){3}z**는 abxyxyxyz와 같습니다.
|	대안	구분하는 두 가지 식 중 하나와 일치합니다. 예를 들어 **doglcat**은 dog 또는 cat과 일치합니다.
?	물음표	이전 식이 0 또는 1회 반복됨을 나타내는 한정자입니다. 예를 들어 **lo?se**는 lse 또는 lose와 일치합니다. **참고** **Ctrl+V**를 입력한 후 물음표를 입력해야 합니다. 그렇게 하지 않으면 도움말 기능이 호출됩니다.
*	별표	이전 식이 0, 1 또는 임의의 숫자만큼 반복됨을 나타내는 한정자입니다. 예를 들어 **lo*se**는 lse, lose, loose 등과 일치합니다.
+	Plus	이전 식이 1회 이상 반복됨을 나타내는 한정자입니다. 예를 들어 **lo+se**는 lose 및 loose와 일치하지만 lse와는 일치하지 않습니다.
{*x*} 또는 {*x*,}	최소 반복 한정자	최소 *x*회 반복됩니다. 예를 들어 **ab(xy){2,}z**는 abxyxyz, abxyxyxyz 등과 일치합니다.
[*abc*]	문자 클래스	괄호 안에 있는 모든 문자와 일치합니다. 예를 들어 **[abc]**는 a, b 또는 c와 일치합니다.
[^*abc*]	부정 문자 클래스	괄호에 포함되지 않은 단일 문자와 일치합니다. 예를 들어 **[^abc]**는 a, b 또는 c 이외의 모든 문자와 일치합니다. **[^A-Z]**는 대문자가 아닌 모든 단일 문자와 일치합니다.
[*a-c*]	문자 범위 클래스	범위에 있는 모든 문자와 일치합니다. **[a-z]**는 모든 소문자와 일치합니다. 문자 및 범위를 혼합할 수 있습니다. **[abcq-z]**는 a, b, c, q, r, s, t, u, v, w, x, y, z와 일치하며 **[a-cq-z]**도 마찬가지입니다. 대시(-) 문자는 괄호 안의 마지막 문자 또는 첫 번째 문자인 경우에만 리터럴입니다(예: **[abc-]** 또는 **[-abc]**).
" "	따옴표	문자열에 있는 선행 또는 후행 공백을 유지합니다. 예를 들어 **" test"**는 일치 항목을 찾을 때 선행 공백을 유지합니다.
^	캐럿	줄의 시작을 지정합니다.
\	이스케이프 문자	메타 문자와 함께 사용할 경우 리터럴 문자와 일치합니다. 예를 들어 **\[**는 왼쪽 각괄호와 일치합니다.

표 18-1 regex 메타 문자(계속)

문자	설명	참고
char	문자	문자가 메타 문자가 아닐 경우 리터럴 문자와 일치합니다.
\r	캐리지 리턴	캐리지 리턴 0x0d와 일치합니다.
\n	새 줄	새 줄 0x0a와 일치합니다.
\t	탭	탭 0x09와 일치합니다.
\f	폼피드	폼피드 0x0c와 일치합니다.
\x*NN*	이스케이프된 16진수 숫자	16진수(정확히 두 자릿수)를 사용하는 ASCII 문자와 일치합니다.
*****NNN*	이스케이프된 8진수 숫자	8진수(정확히 세 자릿수)를 사용하는 ASCII 문자와 일치합니다. 예를 들어, 문자 040은 공백을 나타냅니다.

정규식을 테스트하여 원하는 내용과 일치하는지 확인하려면 **test regex** 명령을 입력합니다.

정규식 성능 효과는 두 가지 요인에 의해 결정됩니다.

- 정규식 일치 확인을 위해 검색해야 할 텍스트의 길이.

  검색 길이가 짧으면 정규식 엔진이 ASA 성능에 미치는 영향이 크지 않습니다.
- 정규식 일치 확인을 위해 검색해야 할 정규식 체인 테이블의 수.

검색 길이가 성능에 미치는 영향

정규식 검색을 구성하면 일반적으로 정규식 데이터베이스에서 일치 항목을 찾기 위해 검색할 텍스트의 모든 바이트가 검토됩니다. 검색할 텍스트의 길이가 길수록 검색 시간도 더 걸립니다. 다음은 이러한 현상을 설명하는 성능 테스트 사례입니다.

- HTTP 트랜잭션에 300바이트 길이의 GET 요청 및 3250바이트 길이의 응답이 각각 하나씩 포함되어 있습니다.
- URI 검색을 위한 445개 정규식, 요청 본문 검색을 위한 34개 정규식.
- 응답 본문 검색을 위한 55개 정규식.

HTTP GET 요청에서만 URI와 본문을 검색하도록 정책을 구성하는 경우 처리량은 다음과 같습니다.

- 해당 정규식 데이터베이스를 검색하지 않을 경우 420mbps.
- 해당 정규식 데이터베이스를 검색할 경우 413mbps(정규식 사용의 오버헤드가 비교적 미미함을 나타냄).

그러나 전체 HTTP 응답 본문을 검색하도록 정책을 구성하는 경우 응답 본문이 길기 때문에(3250바이트) 처리량은 145mbps로 떨어집니다.

다음은 정규식 검색을 위한 텍스트 길이가 늘어나게 하는 요소입니다.

- 서로 다른 여러 프로토콜 필드에 대해 정규식 검색이 구성되어 있는 경우. 예를 들어 HTTP 검사에서 정규식 일치에 대해 URI만 구성된 경우, 정규식 일치에서 URI 필드만 검색되며 검색 길이는 URI 길이로 제한됩니다. 그러나 정규식 일치에 대해 헤더, 본문 등 추가 프로토콜 필드도 구성된 경우, 헤더 길이와 본문 길이도 포함하도록 검색 길이가 늘어납니다.
- 검색할 필드가 긴 경우. 예를 들어 정규식 검색을 위해 URI가 구성된 경우 GET 요청의 URI가 길면 검색 시간도 더 오래 걸리게 됩니다. 또한 현재 HTTP 본문 검색 길이는 기본적으로 200바이트로 제한됩니다. 그러나 본문을 검색하도록 정책을 구성하고 본문 검색 길이를 5000바이트로 변경하면, 긴 본문 검색 때문에 성능에 심각한 영향을 미치게 됩니다.

정규식 체인 테이블의 수가 성능에 미치는 영향

현재 동일한 프로토콜 필드에 대해 구성된 모든 정규식(예: 모든 URI용 정규식)은 하나 이상의 정규식 체인 테이블로 구성된 데이터베이스에 내장됩니다. 테이블의 수는 필요한 전체 메모리 및 테이블 구축 시점의 메모리 가용성에 의해 결정됩니다. 정규식 데이터베이스는 다음과 같은 조건에서 여러 테이블로 분할됩니다.

- 최대 테이블 크기가 32MB로 제한되는데 총 필수 메모리가 32MB보다 큰 경우.
- 최대 연속 메모리의 크기가 완전한 정규식 데이터베이스를 구축할 만큼 충분하지 않은 경우 모든 정규식을 수용할 수 있도록 더 작은 여러 개의 테이블이 구축됩니다. 메모리 조각화의 정도는 상호 관련된 많은 요소에 의해 결정되며, 조각화의 수준을 예측하는 것은 거의 불가능합니다.

여러 체인 테이블이 있는 경우 각 테이블에서 정규식 일치를 검색해야 하므로, 검색할 테이블의 수에 비례하여 검색 시간도 증가합니다.

특정 정규식 유형은 테이블 크기를 대폭 증가시키는 경향이 있습니다. 가능하면 와일드카드와 반복 요소를 피하는 방식으로 정규식을 디자인하는 것이 좋습니다. 다음 메타 문자에 대한 설명은 표 18-1을 참조하십시오.

- 와일드카드 유형의 사양이 있는 정규식:
  - 점 (.)
- 클래스에 있는 임의의 문자와 일치하는 다양한 문자 클래스:
  - [^a-z]
  - [a-z]
  - [abc]]
- 반복 유형의 사양이 있는 정규식:
  - *
  - +
  - {n,}
- 와일드카드와 반복 유형의 정규식이 결합되어 있어 테이블 크기를 대폭 증가시킬 수 있는 예:
  - 123.*xyz
  - 123.+xyz
  - [^a-z]+
  - [^a-z]*
  - .*123.*(이것은 "123" 일치와 동등하기 때문에 사용해서는 안 됨).

다음 예는 와일드카드와 반복이 있는 정규식과 없는 정규식이 메모리 소비에서 어떤 차이를 보이는가를 설명합니다.

- 다음 4개 정규식의 데이터베이스 크기는 958,464바이트입니다.

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- 다음 4개 정규식의 데이터베이스 크기는 10,240바이트에 불과합니다.

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

정규식의 수가 많으면 정규식 데이터베이스에 필요한 총 메모리도 늘어나므로, 메모리가 조각화되면 테이블 수가 많아질 확률이 높아집니다. 다음은 정규식에 따른 메모리 소비를 보여주는 예입니다.

- 샘플 URI 100개: 3,079,168바이트
- 샘플 URI 200개: 7,156,224바이트
- 샘플 URI 500개: 11,198,971바이트

참고 컨텍스트당 최대 정규식 수는 2048입니다.

debug menu regex 40 10 명령은 각 regex 데이터베이스에 있는 체인 테이블의 수를 표시하는 데 사용할 수 있습니다.

예

다음 예에서는 검사 정책 맵에서 사용할 정규식 2개를 만듭니다.

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
```

관련 명령

명령	설명
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	트래픽 클래스를 하나 이상의 작업과 연결하여 정책 맵을 만듭니다.
policy-map type inspect	애플리케이션 검사를 위한 특수 작업을 정의합니다.
class-map type regex	정규식 클래스 맵을 만듭니다.
test regex	정규식을 테스트합니다.

reload

컨피그레이션을 재부팅하여 다시 로드하려면 특별 권한 EXEC 모드에서 **reload** 명령을 사용합니다.

reload [**at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh*:]*mm*] [**max-hold-time** [*hh*:]*mm*] [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

구문 설명

at *hh*:*mm*	(선택 사항) 지정된 시간에 소프트웨어 다시 로드가 발생하도록 예약합니다(24시간 클록 사용). 월과 날짜를 지정하지 않으면 현재 날짜의 지정된 시간(지정된 시간이 현재 시간 이후인 경우)에 또는 다음날(지정된 시간이 현재 시간 이전인 경우)에 다시 로드가 발생합니다. 00:00을 지정하면 다시 로드가 자정으로 예약됩니다. 다시 로드는 24시간 내에 발생해야 합니다.
cancel	(선택 사항) 예약된 다시 로드를 취소합니다.
day	(선택 사항) 1~31 범위의 날짜.
in [*hh*:]*mm*	(선택 사항) 지정된 분/시간 및 분에 소프트웨어 다시 로드가 발생하도록 예약합니다. 다시 로드는 24시간 내에 발생해야 합니다.
max-hold-time [*hh*:]*mm*	(선택 사항) 종료 또는 재부팅 전에 ASA가 다른 하위 시스템에 알리기 위해 대기하는 최대 보류 시간을 지정합니다. 이 시간이 경과하면 빠른(강제) 종료/재부팅이 발생합니다.
month	(선택 사항) 월의 이름을 지정합니다. 월 이름에 대한 고유한 문자열을 만들 수 있도록 충분한 문자를 입력합니다. 예를 들어 "Ju"는 June과 July를 모두 나타낼 수 있으므로 고유하지 않지만, "Jul"은 이 세 글자로 시작하는 다른 달이 없기 때문에 고유합니다.
noconfirm	(선택 사항) 사용자 확인 없이 ASA를 다시 로드하도록 허용합니다.
quick	(선택 사항) 알리거나 모든 하위 시스템을 올바르게 종료하지 않은 채 강제로 빠르게 다시 로드합니다.
reason *text*	(선택 사항) 다시 로드의 이유를 1~255자로 지정합니다. 이유 텍스트는 모든 열린 IPsec VPN 클라이언트, 터미널, 콘솔, 텔넷, SSH 및 ASDM 연결/세션으로 전송됩니다. **참고** ISAKMP 같은 일부 애플리케이션은 IPsec VPN 클라이언트에 이유 텍스트를 전송하려면 추가 컨피그레이션이 필요합니다. 자세한 내용은 VPN CLI 컨피그레이션 가이드를 참조하십시오.
save-config	(선택 사항) 종료 전에 실행 중인 컨피그레이션을 메모리에 저장합니다. **save-config** 키워드를 입력하지 않으면, 다시 로드한 후 저장하지 않은 컨피그레이션 변경 사항이 손실됩니다.
save-show-tech	(선택 사항) 다시 로드가 발생하기 전 **show tech** 명령의 출력을 파일에 저장합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	*day*, *hh*, *mm*, *month*, **quick**, **save-config**, *text* 등의 새 인수 및 키워드를 추가할 수 있도록 이 명령이 수정되었습니다.
9.1(3)	**save-show-tech** 키워드가 추가되었습니다.

사용 지침

이 명령을 사용하면 ASA를 재부팅하고 컨피그레이션을 플래시 메모리에서 다시 로드할 수 있습니다.

기본적으로 **reload** 명령은 대화형입니다. ASA는 우선 컨피그레이션이 수정되었지만 저장되지 않았는지 확인합니다. 그런 다음 ASA는 컨피그레이션을 저장하라는 프롬프트를 표시합니다. 다중 컨텍스트 모드에서 ASA는 저장되지 않은 컨피그레이션이 있는 각 컨텍스트에 대해 프롬프트를 표시합니다. **save-config** 키워드를 지정하면 프롬프트 없이 컨피그레이션이 저장됩니다. 그러면 ASA는 시스템을 다시 로드할 것인지를 확인하는 프롬프트를 표시합니다. **y**를 입력하거나 **Enter** 키를 누르는 경우에만 다시 로드가 발생합니다. 확인 후 ASA는 지연 키워드(**in** 또는 **at**)의 지정 여부에 따라 다시 로드 프로세스를 시작 또는 예약합니다.

기본적으로 다시 로드 프로세스는 "정상적(graceful)" 모드에서 운영됩니다. 재부팅 전에 모든 등록된 하위 시스템이 올바르게 종료될 수 있도록, 재부팅이 발생하려고 할 때 하위 시스템에 알림이 제공됩니다. 그러한 종료가 발생할 때까지의 대기 시간을 피하려면 **max-hold-time** 키워드로 최대 대기 시간을 지정합니다. 또는, 영향을 받는 하위 시스템에 알리지 않거나 정상적인 종료를 기다리지 않고 다시 로드 프로세스가 즉시 시작되도록 **quick** 키워드를 사용할 수 있습니다.

noconfirm 키워드를 지정하여 비대화형으로 작동하는 **reload** 명령을 강제로 적용할 수 있습니다. 이 경우 **save-config** 키워드가 지정되지 않았다면 ASA는 저장되지 않은 컨피그레이션을 확인하지 않습니다. ASA는 시스템 재부팅 전에 확인 프롬프트를 표시하지 않습니다. **max-hold-time** 또는 **quick** 키워드를 사용하여 동작 또는 다시 로드 프로세스를 제어할 수는 있지만, delay 키워드가 지정되지 않았다면 다시 로드 프로세스를 즉시 시작 또는 예약합니다.

예약된 다시 로드를 취소하려면 **reload cancel** 명령을 사용합니다. 이미 진행 중인 다시 로드는 취소할 수 없습니다.

참고 플래시 파티션에 기록되지 않은 컨피그레이션 변경 사항은 다시 로드 이후에 손실됩니다. 현재의 컨피그레이션을 플래시 파티션에 저장하려면 재부팅 전에 **write memory** 명령을 입력합니다.

예

다음 예는 컨피그레이션을 재부팅 및 다시 로드하는 방법을 보여줍니다.

```
ciscoasa# reload
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

관련 명령

명령	설명
show reload	ASA의 다시 로드 상태를 표시합니다.

remote-access threshold session-threshold-exceeded

임계값을 설정하려면 글로벌 컨피그레이션 모드에서 **remote-access threshold** 명령을 사용합니다. 임계값을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 ASA가 트랩을 전송하는 지점인 활성 원격 액세스 세션의 수를 지정합니다.

remote-access threshold session-threshold-exceeded {*threshold-value*}

no **remote-access threshold session-threshold-exceeded**

구문 설명

threshold-value	ASA가 지원하는 세션 제한과 같거나 작은 정수를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0 (1)	이 명령이 추가되었습니다.

예

다음 예는 임계값을 1500으로 설정하는 방법을 보여줍니다.

```
ciscoasa# remote-access threshold session-threshold-exceeded 1500
```

관련 명령

명령	설명
snmp-server enable trap remote-access	임계값 트래픽을 활성화합니다.

rename

소스 파일 이름에서 대상 파일 이름으로 파일 또는 디렉토리의 이름을 변경하려면 특별 권한 EXEC 모드에서 **rename** 명령을 사용합니다.

rename [**/noconfirm**] [**disk0**: | **disk1**: | **flash:**] *source-path* [**disk0**: | **disk1**: | **flash:**] *destination-path*

구문 설명

/noconfirm	(선택 사항) 확인 프롬프트를 억제합니다.
destination-path	대상 파일의 경로를 지정합니다.
disk0*:*	(선택 사항) 내장 플래시 메모리 및 그 뒤에 콜론을 지정합니다.
disk1:	(선택 사항) 외장 플래시 메모리 카드 및 그 뒤에 콜론을 지정합니다.
flash:	(선택 사항) 내장 플래시 메모리 및 그 뒤에 콜론을 지정합니다.
source-path	소스 파일의 경로를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

rename flash: flash: 명령을 입력하면 소스 및 대상 파일 이름을 입력하라는 프롬프트가 표시됩니다.

파일 시스템 전체에서 파일 또는 디렉토리의 이름을 변경할 수 없습니다.

예:

```
ciscoasa# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

예

다음 예는 파일 이름을 "test"에서 "test1"로 변경하는 방법을 보여줍니다.

```
ciscoasa# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

관련 명령

명령	설명
mkdir	새 디렉토리를 만듭니다.
rmdir	디렉토리를 제거합니다.
show file	파일 시스템에 대한 정보를 표시합니다.

rename(class-map)

클래스 맵의 이름을 변경하려면 클래스 맵 컨피그레이션 모드에서 **rename** 명령을 입력합니다.

rename *new_name*

구문 설명

new_name	클래스 맵의 새 이름을 지정합니다(길이 최대 40자). "class-default"는 예약된 이름입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
클래스 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

예

다음 예는 클래스 맵 이름을 test에서 test2로 변경하는 방법을 보여줍니다.

```
ciscoasa(config)# class-map test
ciscoasa(config-cmap)# rename test2
```

관련 명령

명령	설명
class-map	클래스 맵을 만듭니다.

renewal-reminder

인증서 소유자에게 재등록 초기 알림을 보내야 하는, 사용자 인증서가 만료되기까지 남은 일수를 지정하려면 ca 서버 컨피그레이션 모드에서 **renewal-reminder** 명령을 사용합니다. 기간을 기본값 14일로 복원하려면 이 명령의 **no** 형식을 사용합니다.

renewal-reminder *days*

no renewal-reminder

구문 설명

days	인증서 소유자에게 재등록 초기 알림을 보내야 하는, 발급된 인증서가 만료되기까지 남은 일수를 지정합니다. 유효한 값의 범위는 1~90일입니다.

기본값

기본값은 14일입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

알림은 총 3번 발송됩니다. 이메일 주소가 사용자 데이터베이스에 지정된 경우, 3번의 알림이 각각 인증서 소유자에게 이메일로 자동 발송됩니다. 이메일 주소가 없는 경우 관리자에게 갱신을 경고하는 syslog 메시지가 생성됩니다.

기본적으로 CA 서버는 인증서 만료 전에 다음의 이메일 메시지 3개를 지정된 순서로 전송합니다.

1. Certification Enrollment Invitation
2. Reminder: Certification Enrollment Invitation
3. Last Reminder: Certification Enrollment Invitation

첫 번째 이메일은 초대, 두 번째는 알림, 세 번째는 최종 알림입니다. 이 알림의 기본 설정은 14일입니다. 즉, 초기 초대는 인증서 만료 14일 전에 전송되고, 알림 이메일은 7일 전, 최종 알림 이메일은 3일 전에 전송됩니다.

renewal-reminder *days* 명령을 사용하여 갱신 알림 간격을 원하는 대로 조정할 수 있습니다.

예

다음 예는 ASA에서 인증서 만료 7일 전에 만료 알림을 전송하도록 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# renewal-reminder 7
ciscoasa(config-ca-server)#
```

다음 예는 만료 알림 시간을 기본값인 인증서 만료 14일 전으로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no renewal-reminder
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	로컬 CA를 구성 및 관리할 수 있는 ca 서버 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다.
lifetime	CA 인증서, 발급된 모든 인증서 및 CRL의 수명을 지정합니다.
show crypto ca server	로컬 CA 서버의 컨피그레이션 세부사항을 표시합니다.

replication http

장애 조치 그룹에 대해 HTTP 연결 복제를 활성화하려면 장애 조치 그룹 컨피그레이션 모드에서 **replication http** 명령을 사용합니다. HTTP 연결 복제를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

replication http

no replication http

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

없다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
장애 조치 그룹 컨피그레이션	• 예	• 예	—	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

기본적으로 ASA는 스테이트풀 장애 조치가 활성화된 경우 HTTP 세션 정보를 복제하지 않습니다. 보통 HTTP 클라이언트에서는 오류가 발생한 연결을 다시 수행하려고 시도하기 때문에 HTTP 세션은 짧은 것이 일반적입니다. 따라서 HTTP 세션을 복제하지 않을 경우 중요한 데이터 또는 연결이 손실되지 않으면서 시스템 성능이 향상됩니다. **replication http** 명령은 스테이트풀 장애 조치 환경에서 HTTP 세션의 스테이트풀 복제를 활성화하지만 시스템 성능에는 부정적인 영향을 미칠 수 있습니다.

이 명령은 액티브/액티브 장애 조치에서만 이용할 수 있습니다. 또한 액티브/스탠바이 장애 조치에 대한 **failover replication http** 명령과 동일한 기능을 제공합니다(액티브/액티브 장애 조치 컨피그레이션의 장애 조치 그룹 제외).

예

다음 예는 장애 조치 그룹에 대해 가능한 컨피그레이션을 보여줍니다.

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
```

관련 명령

명령	설명
failover group	액티브/액티브 장애 조치에 대한 장애 조치 그룹을 정의합니다.
failover replication http	HTTP 연결을 복제하도록 스테이트풀 장애 조치를 구성합니다.

request-command deny

FTP 요청 내에서 특정 명령을 허용하지 않으려면 **ftp-map** 명령을 사용하여 액세스할 수 있는 FTP 맵 컨피그레이션 모드에서 **request-command deny** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }

no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

구문 설명

appe	파일에 추가되는 명령을 허용하지 않습니다.
cdup	현재 작업 디렉토리의 상위 디렉토리로 변경하는 명령을 허용하지 않습니다.
dele	서버에서 파일을 삭제하는 명령을 허용하지 않습니다.
get	서버에서 파일을 검색하기 위한 클라이언트 명령을 허용하지 않습니다.
help	도움말 정보를 제공하는 명령을 허용하지 않습니다.
mkd	서버에 디렉토리를 만드는 명령을 허용하지 않습니다.
put	서버에 파일을 보내기 위한 클라이언트 명령을 허용하지 않습니다.
rmd	서버에서 디렉토리를 삭제하는 명령을 허용하지 않습니다.
rnfr	rename-from 파일 이름을 지정하는 명령을 허용하지 않습니다.
rnto	rename-to 파일 이름을 지정하는 명령을 허용하지 않습니다.
site	서버 시스템에 해당하는 명령을 허용하지 않습니다. 주로 원격 관리에 사용됩니다.
stou	고유한 파일 이름을 사용해 파일을 저장하는 명령을 허용하지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
FTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 엄격한 FTP 검사를 사용할 때 ASA를 통과하는 FTP 요청 내에서 허용되는 명령을 제어하는 데 사용됩니다.

예

다음 예는 ASA에서 **stor**, **stou** 또는 **appe** 명령을 포함하는 FTP 요청을 삭제하도록 지정합니다.

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# request-command deny put stou appe
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
ftp-map	FTP 맵을 정의하고 FTP 맵 컨피그레이션 모드를 활성화합니다.
inspect ftp	애플리케이션 검사에 사용할 특정 FTP 맵을 적용합니다.
mask-syst-reply	클라이언트에서 오는 FTP 서버 응답을 숨깁니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.

request-data-size

SLA 작업 요청 패킷에서 페이로드의 크기를 설정하려면 sla 모니터 프로토콜 컨피그레이션 모드에서 **request-data-size** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

request-data-size *bytes*

no request-data-size

구문 설명

bytes	요청 패킷 페이로드의 크기(바이트 단위). 유효한 값은 0~16384입니다. 최소값은 사용하는 프로토콜에 따라 다릅니다. 에코 유형의 경우 최소값은 28바이트입니다. 이 값을 프로토콜 또는 PMTU에서 허용하는 최대값보다 크게 설정하지 마십시오. **참고** ASA는 8바이트 타임스탬프를 페이로드에 추가하므로 실제 페이로드는 *바이트* + 8입니다.

기본값

기본 *바이트*는 28입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
sla 모니터 프로토콜 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

도달 범위를 확장하기 위해 소스와 대상 사이의 PMTU 변경 사항을 감지하도록 기본 데이터 크기를 늘려야 할 수 있습니다. 낮은 PMTU는 세션 성능에 영향을 미칠 수 있으며, 감지되는 경우 보조 경로가 사용되고 있음을 나타낼 수 있습니다.

예

다음 예는 ICMP 에코 요청/응답 시간 프로브 작업을 사용하는 ID 123으로 SLA 작업을 구성합니다. 에코 요청 패킷의 페이로드 크기를 48바이트로 설정하고 SLA 작업 중 전송되는 에코 요청의 수를 5로 설정합니다.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
```

```
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

명령	설명
num-packets	SLA 작업 중에 전송할 요청 패킷의 수를 지정합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.
type echo	SLA 작업을 에코 응답 시간 프로브 작업으로서 구성합니다.

request-queue

응답을 기다리는 큐에 추가할 최대 GTP 요청 수를 지정하려면 **gtp-map** 명령을 사용하여 액세스할 수 있는 GTP 맵 컨피그레이션 모드에서 **request-queue** 명령을 사용합니다. 이 숫자를 기본값 200으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

request-queue *max_requests*

no request-queue *max_requests*

구문 설명

max_requests	응답을 대기하도록 큐에 추가할 최대 GTP 요청 수를 설정합니다. 값의 범위는 1~4294967295입니다.

기본값

max_requests 기본값은 200입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
GTP 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

gtp request-queue 명령은 응답을 대기하도록 큐에 추가할 최대 GTP 요청 수를 설정합니다. 제한에 도달한 상태에서 새 요청이 도착하면 큐에 있는 가장 오래된 요청이 제거됩니다. Error Indication, Version Not Supported 및 SGSN Context Acknowledge 메시지는 요청으로 간주되지 않으며 응답 대기를 위해 요청 큐에 추가되지 않습니다.

예

다음 예는 최대 요청 큐 크기를 300바이트로 지정합니다.

```
ciscoasa(config)# gtp-map qtp-policy
ciscoasa(config-gtpmap)# request-queue-size 300
```

관련 명령

명령	설명
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
debug gtp	GTP 검사에 대한 상세 정보를 표시합니다.
gtp-map	GTP 맵을 정의하고 GTP 맵 컨피그레이션 모드를 활성화합니다.
inspect gtp	애플리케이션 검사에 사용할 특정 GTP 맵을 적용합니다.
show service-policy inspect gtp	GTP 컨피그레이션을 표시합니다.

request-timeout

실패한 SSO 인증 시도의 시간 제한 값(초 단위)을 구성하려면 webvpn 컨피그레이션 모드에서 **request-timeout** 명령을 사용합니다.

기본값으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

request-timeout *seconds*

no request-timeout

구문 설명

seconds	실패한 SSO 인증 시도의 시간 제한 값(초 단위)을 지정합니다. 범위는 1~30초입니다. 소수는 지원되지 않습니다.

기본값

이 명령의 기본값은 5초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1.1	이 명령이 추가되었습니다.

사용 지침

WebVPN에서만 사용 가능한 단일 로그인이 지원되므로, 사용자는 사용자 이름과 비밀번호를 한 번만 입력하여 다양한 서버의 서로 다른 보안 서비스에 안전하게 액세스할 수 있습니다. ASA는 현재 SiteMinder 및 SAML POST 유형 SSO 서버를 지원합니다.

이 명령은 두 SSO 서버 유형에 모두 적용됩니다.

SSO 인증을 지원하도록 ASA를 구성했으면 두 가지 시간 제한 매개변수를 조정할 수 있습니다.

- **request-timeout** 명령으로 지정하는 실패한 SSO 인증 시도의 시간 제한 값(초 단위)
- 실패한 SSO 인증 시도에 대해 ASA에서 재시도할 횟수. (**max-retry-attempts** 명령 참조.)

예

webvpn-config-sso-siteminder 모드에서 입력하는 다음 예는 SiteMinder 유형 SSO 서버 "example"에 대한 인증 시간 제한을 10초로 구성합니다.

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# request-timeout 10
```

관련 명령

명령	설명
max-retry-attempts	실패한 SSO 인증 시도에 대해 ASA에서 재시도할 횟수를 구성합니다.
policy-server-secret	SiteMinder SSO 서버에 대한 인증 요청을 암호화하기 위해 사용되는 비밀 키를 만듭니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso-server	단일 로그인 서버를 만듭니다.
test sso-server	SSO 서버를 평가 인증 요청으로 테스트합니다.
web-agent-url	ASA에서 SiteMinder SSO 인증 요청을 수행하는 SSO 서버 URL을 지정합니다.

reserve-port-protect

미디어 협상 중에 예약 포트의 사용을 제한하려면 매개변수 컨피그레이션 모드에서 **reserve-port-protect** 명령을 사용합니다. 매개변수 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

reserve-port-protect

no reserve-port-protect

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

예

다음 예는 RTSP 검사 정책 맵에서 예약 포트를 보호하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# reserve-port-protect
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

reserved-bits

TCP 헤더에서 예약된 비트를 지우거나 예약된 비트 세트로 패킷을 삭제하려면 tcp-map 컨피그레이션 모드에서 **reserved-bits** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits {**allow** | **clear** | **drop**}

구문 설명

allow	TCP 헤더에 예약된 비트가 포함된 패킷을 허용합니다.
clear	TCP 헤더에서 예약된 비트를 지우고 패킷을 허용합니다.
drop	TCP 헤더에 예약된 비트가 포함된 패킷을 삭제합니다.

기본값

기본적으로 예약된 비트는 허용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용됩니다. **class-map** 명령을 사용하여 트래픽의 클래스를 정의하고 **tcp-map** 명령으로 TCP 검사를 사용자 지정합니다. **policy-map** 명령을 사용하여 새 TCP 맵을 적용합니다. **service-policy** 명령으로 TCP 검사를 활성화합니다.

tcp-map 컨피그레이션 모드로 들어가려면 **tcp-map** 명령을 사용합니다. 엔드 호스트에서 예약된 비트가 포함된 패킷을 처리하는 방법에 대한 모호성을 제거하려면 tcp-map 컨피그레이션 모드에서 **reserved-bits** 명령을 사용합니다. 이 경우 ASA의 동기화가 해제될 수 있습니다. 예약된 비트를 TCP 헤더에서 지울 수도 있고, 예약된 비트 세트가 포함된 패킷을 삭제할 수도 있습니다.

예

다음 예는 예약된 비트 세트가 포함된 모든 TCP 흐름에서 패킷을 지우는 방법을 보여줍니다.

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# reserved-bits clear
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
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
policy-map	트래픽 클래스 및 하나 이상의 작업을 결합한 정책을 구성합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 컨피그레이션 모드에 대한 액세스를 허용합니다.

reset

Modular Policy Framework를 사용하는 경우, 일치 또는 클래스 컨피그레이션 모드에서 **reset** 명령을 사용하여 **match** 명령 또는 클래스 맵과 일치하는 트래픽에 대해 패킷을 삭제하고, 연결을 닫고, TCP 재설정을 전송합니다. 이 재설정 작업은 검사 정책 맵에서 애플리케이션 트래픽에 대해 사용 가능하지만(**policy-map type inspect** 명령), 모든 애플리케이션에서 이 작업을 허용하는 것은 아닙니다. 이 작업을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

reset [**log**]

no reset [**log**]

구문 설명

log	일치를 기록합니다. 시스템 로그 메시지 번호는 애플리케이션에 따라 다릅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
일치 및 클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

검사 정책 맵은 **match** 및 **class** 명령으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 명령은 애플리케이션에 따라 다릅니다. **match** 또는 **class** 명령을 입력하여 애플리케이션 트래픽을 식별한 후(**class** 명령은 기존의 **class-map type inspect** 명령을 참조하며, 여기에 **match** 명령이 포함됨), **reset** 명령을 입력하여 패킷을 삭제하고 **match** 명령 또는 **class** 명령과 일치하는 트래픽에 대해 연결을 닫을 수 있습니다.

연결을 재설정하는 경우 검사 정책 맵에서 추가 작업이 수행되지 않습니다. 예를 들어, 첫 번째 작업에서 연결을 재설정하면 추가 **match** 또는 **class** 명령이 적용되지 않습니다. 첫 번째 작업에서 패킷을 기록하면, 두 번째 작업(예: 연결 재설정)이 발생할 수 있습니다. 동일한 **match** 또는 **class** 명령에 대해 **reset** 및 **log** 작업을 모두 구성할 수 있습니다. 이 경우 지정된 일치에 대해 재설정되기 전에 패킷이 기록됩니다.

Layer 3/4 정책 맵에서(**policy-map** 명령) **inspect** 명령을 사용하여 애플리케이션 검사를 활성화할 경우 이 작업을 포함하는 검사 정책 맵을 활성화할 수 있습니다. 예를 들어 **inspect http http_policy_map** 명령(http_policy_map은 검사 정책 맵의 이름)을 입력할 수 있습니다.

예

다음 예는 연결을 재설정하고 http-traffic 클래스 맵과 일치할 경우 로그를 전송합니다. 동일한 패킷이 두 번째 **match** 명령도 확인하는 경우, 이미 삭제되었기 때문에 처리되지 않습니다.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
policy-map type inspect	애플리케이션 검사를 위한 특수 작업을 정의합니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

19 장

retries through rtp-min-port rtp-max-port 명령

retries

ASA에서 응답을 받지 못할 때 DNS 서버 목록을 재시도할 횟수를 지정하려면 글로벌 컨피그레이션 모드에서 **dns retries** 명령을 사용합니다. 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

retries *number*

no retries [*number*]

구문 설명

number	재시도 횟수를 지정합니다(0~10). 기본값은 2입니다.

기본값

기본 재시도 횟수는 2입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

name-server 명령을 사용하여 DNS 서버를 추가합니다.

이 명령이 **dns name-server** 명령을 교체합니다.

예

다음 예는 재시도 횟수를 0으로 설정합니다. ASA는 각 서버에 대해 한 번만 시도합니다.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# dns retries 0
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns server-group 모드로 들어갑니다.
show running-config dns server-group	하나 또는 기존의 모든 dns-server-group 컨피그레이션을 보여줍니다.

retry-count

서버가 도달 불가능한 상태임을 확인할 때까지 Cloud Web Security 프록시 서버에 대한 연속 폴링 실패 횟수의 값을 설정하려면 scansafe general-options 컨피그레이션 모드에서 **retry-count** 명령을 입력합니다. 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

retry-count *value*

no retry-count [*value*]

구문 설명

value	재시도 카운터 값을 입력합니다(2~100). 기본값은 5입니다.

명령 기본값

기본값은 5입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Scansafe general-options 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

Cisco Cloud Web Security 서비스를 구독하는 사용자에게는 기본 Cloud Web Security 프록시 서버 및 백업 프록시 서버가 할당됩니다.

클라이언트가 기본 서버에 도달할 수 없는 경우 ASA에서는 가용성 확인을 위해 타워의 폴링을 시작합니다. 클라이언트 활동이 없으면 ASA는 15분마다 폴링합니다. 구성된 재시도 횟수(기본 5회이며 구성 가능) 이후에도 프록시 서버를 사용할 수 없는 경우, 해당 서버는 도달할 수 없는 상태로 선언되고 백업 프록시 서버가 활성화됩니다.

클라이언트 또는 ASA가 재시도 횟수에 도달하기 전 2회 이상 연속적으로 서버에 도달할 수 있으면 폴링이 멈추고 타워는 도달 가능한 것으로 확인됩니다.

백업 서버로의 장애 조치 이후에도 ASA는 계속해서 기본 서버를 폴링합니다. 기본 서버에 도달할 수 있게 되면 ASA는 다시 기본 서버를 사용합니다.

예

다음 예는 재시도 값을 7로 구성합니다.

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 7
```

관련 명령

명령	설명
class-map type inspect scansafe	화이트리스트에 있는 사용자 및 그룹에 대한 검사 클래스 맵을 만듭니다.
default user group	ASA에서 ASA로 들어오는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**] (parameters)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스에서 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청이 어느 조직에서 오는지를 나타내기 위해 ASA가 Cloud Web Security 프록시 서버에 전송하는 인증 키를 구성합니다.
match user group	화이트리스트를 기준으로 사용자 또는 그룹을 확인합니다.
policy-map type inspect scansafe	규칙에 대한 필수 매개변수를 구성하고 선택적으로 화이트리스트를 식별할 수 있도록 검사 정책 맵을 만듭니다.
scansafe	다중 컨텍스트 모드에서는 컨텍스트 단위로 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 정규화된 도메인 이름 또는 IP 주소를 구성합니다.
show conn scansafe	모든 Cloud Web Security 연결을 보여줍니다(대문자 Z 플래그로 표시됨).
show scansafe server	서버의 상태, 즉 현재 활성 서버인지, 백업 서버인지 또는 도달할 수 없는 서버인지를 보여줍니다.
show scansafe statistics	전체 및 현재 http 연결을 보여줍니다.
user-identity monitor	지정된 사용자 또는 그룹 정보를 AD 에이전트에서 다운로드합니다.
whitelist	트래픽의 클래스에 대해 화이트리스트 작업을 수행합니다.

retry-interval

이전 **aaa-server host** 명령으로 지정한 특정 AAA 서버에 대한 재시도 간격을 구성하려면 aaa-server host 모드에서 **retry-interval** 명령을 사용합니다. 재시도 간격을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

retry-interval *seconds*

no retry-interval

구문 설명

seconds	요청의 재시도 간격(1~10초)을 지정합니다. 연결 요청을 재시도하기 전에 ASA가 대기하는 시간입니다.

기본값

기본 재시도 간격은 10초입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
AAA-server 호스트	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령은 CLI 지침에 따라 수정되었습니다.

사용 지침

ASA에서 연결 시도 간에 대기할 시간(초)을 지정하거나 재설정하려면 **retry-interval** 명령을 사용합니다. ASA에서 AAA 서버에 연결하기 위해 시도하는 시간을 지정하려면 **timeout** 명령을 사용합니다.

참고 다음 재시도까지의 간격은 입력한 재시도 간격 설정과 무관하게 항상 50 또는 100밀리초입니다. 이것은 의도된 것입니다.

예

다음 예는 **retry-interval** 명령의 컨텍스트를 보여줍니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 7
ciscoasa(config-aaa-server-host)# retry-interval 9
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
aaa-server host	호스트와 관련된 AAA 서버 매개변수를 구성할 수 있는 aaa-server host 컨피그레이션 모드로 들어갑니다.
clear configure aaa-server	컨피그레이션에서 모든 AAA 명령문을 제거합니다.
show running-config aaa-server	모든 AAA 서버, 특정 서버 그룹, 특정 그룹 내 특정 서버 또는 특정 프로토콜에 대한 AAA 서버 통계를 표시합니다.
timeout	ASA에서 AAA 서버에 연결하기 위해 시도하는 시간을 지정합니다.

reval-period

NAC Framework 세션에서 성공적인 각 PV(posture validation) 사이의 간격을 지정하려면 nac-policy-nac-framework 컨피그레이션 모드에서 **reval-period** 명령을 사용합니다. NAC Framework 정책에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

reval-period *seconds*

no reval-period [*seconds*]

구문 설명

seconds	성공적인 각 PV(posture validation) 사이의 시간(초)입니다. 범위는 300~86400입니다.

기본값

기본값은 36000입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
nac-policy-nac-framework 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.3(0)	명령 이름에서 "nac-"가 제거되었습니다. 그룹 정책 컨피그레이션 모드에서 nac-policy-nac-framework 컨피그레이션 모드로 명령이 이동했습니다.
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ASA는 성공적인 각 PV(posture validation) 이후 재검증 타이머를 시작합니다. 이 타이머가 만료되면 조건 없이 다음번 PV가 트리거됩니다. ASA는 재검증 중에 PV를 유지합니다. PV 또는 재검증 중에 Access Control Server를 사용할 수 없는 경우 기본 그룹 정책이 사용됩니다.

예

다음 예는 재검증 타이머를 86400초로 변경합니다.

```
ciscoasa(config-nac-policy-nac-framework)# reval-period 86400
ciscoasa(config-nac-policy-nac-framework)
```

다음 예는 NAC 정책에서 재검증 타이머를 제거합니다.

```
ciscoasa(config-nac-policy-nac-framework)# no reval-period
ciscoasa(config-nac-policy-nac-framework)
```

관련 명령

명령	설명
eou timeout	NAC Framework 컨피그레이션의 원격 호스트로 EAP over UDP 메시지를 전송한 이후 대기해야 할 시간(초)을 변경합니다.
sq-period	NAC Framework 세션의 성공적인 각 PV와 호스트 상태의 변경 사항에 대한 다음 쿼리 사이의 간격을 지정합니다.
nac-policy	Cisco NAC 정책을 만들고 액세스하며, 해당 유형을 지정합니다.
debug nac	NAC Framework 이벤트의 로깅을 활성화합니다.
eou revalidate	하나 이상의 NAC Framework 세션에 즉각적인 상태 재검증을 적용합니다.

revert webvpn all

ASA 플래시 메모리에서 모든 웹 관련 데이터(사용자 지정, 플러그인, 변환 테이블, URL 목록, 웹 콘텐츠)를 제거하려면 특별 권한 EXEC 모드에서 **revert webvpn all** 명령을 입력합니다.

revert webvpn all

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

ASA의 플래시 메모리에서 모든 웹 관련 정보(사용자 지정, 플러그인, 변환 테이블, URL 목록, 웹 콘텐츠)를 비활성화 및 제거하려면 **revert webvpn all** 명령을 사용합니다. 웹 관련 데이터를 모두 제거하면 해당되는 경우 기본 설정으로 돌아가게 됩니다.

예

다음 명령은 ASA에서 웹 관련 컨피그레이션 데이터를 모두 제거합니다.

```
ciscoasa# revert webvpn all
ciscoasa
```

관련 명령

명령	설명
show import webvpn (*option*)	가져온 각종 WebVPN 데이터 및 플러그인(현재 ASA의 플래시 메모리에 있는)을 표시합니다.

revert webvpn AnyConnect-customization

AnyConnect 클라이언트 GUI를 사용자 지정하는 ASA에서 파일을 제거하려면 특별 권한 EXEC 모드에서 **revert webvpn AnyConnect-customization** 명령을 사용합니다.

revert webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

구문 설명

type	사용자 지정 파일 유형: • binary - AnyConnect GUI를 대신하는 실행 파일 • resource - 회사 로고 등의 리소스 파일 • transform - MSI를 사용자 지정하는 변환
platform	AnyConnect 클라이언트를 실행하는 엔드포인트 디바이스의 OS. 다음 중 하나 지정: **linux**, **mac-intel**, **mac-powerpc**, **win**, **win-mobile**.
name	제거할 파일을 식별하는 이름(최대 64자).

기본값

이 명령에는 기본 동작이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

AnyConnect 클라이언트 GUI 사용자 지정에 대한 자세한 절차는 *AnyConnect VPN Client Administrator Guide*를 참조하십시오.

예

다음 예는 AnyConnect GUI를 사용자 지정하기 위해 전에 리소스 파일로서 가져온 Cisco 로고를 제거합니다.

```
ciscoasa# revert webvpn AnyConnect-customization type resource platform win name
cisco_logo.gif
```

관련 명령

명령	설명
customization	tunnel-group, group 또는 user에 대해 사용할 사용자 지정 객체를 지정합니다.
export customization	사용자 지정 객체를 내보냅니다.
import customization	사용자 지정 객체를 설치합니다.
revert webvpn all	모든 webvpn 관련 데이터(사용자 지정, 플러그인, 변환 테이블, URL 목록 및 웹 콘텐츠)를 제거합니다.
show webvpn customization	ASA의 플래시 디바이스에 있는 현재 사용자 지정 객체를 표시합니다.

revert webvpn customization

ASA 캐시 메모리에서 사용자 지정 객체를 제거하려면 특별 권한 EXEC 모드에서 **revert webvpn customization** 명령을 입력합니다.

revert webvpn customization *name*

구문 설명

name	삭제할 사용자 지정 객체의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

특정 사용자 지정에 대한 클라이언트리스 SSL VPN 지원을 제거하고 이를 ASA의 캐시 메모리에서도 제거하려면 **revert webvpn customization** 명령을 사용합니다. 사용자 지정 객체를 제거하면 해당되는 경우 기본 설정으로 돌아가게 됩니다. 사용자 지정 객체에는 명명된 특정 포털 페이지에 대한 컨피그레이션 매개변수가 포함되어 있습니다.

버전 8.0 소프트웨어에서는 사용자 지정 구성에 대한 기능이 확장되며, 새 프로세스는 이전 버전과 호환되지 않습니다. 8.0 소프트웨어로 업그레이드하는 동안 보안 어플라이언스는 이전 설정을 사용하여 새 사용자 지정 객체를 생성함으로써 현재 컨피그레이션을 유지합니다. 이 프로세스는 한 번만 발생하며, 이전 형식에서 새 형식으로의 간단한 변환 이상의 의미를 갖습니다. 이전 값은 새 값의 일부 부분 집합에 불과하기 때문입니다.

참고 버전 8.0으로 업그레이드하기 전에 클라이언트리스 SSL VPN(WebVPN)이 버전 7.2(x) 컨피그레이션 파일의 해당 인터페이스에서 활성화된 경우에만, 버전 7.2 포털 사용자 지정 및 URL 목록이 베타 8.0 컨피그레이션에서 작동합니다.

예

다음 명령은 GroupB라는 사용자 지정 객체를 제거합니다.

```
ciscoasa# revert webvpn customization groupb
ciscoasa
```

관련 명령

명령	설명
customization	tunnel-group, group 또는 user에 대해 사용할 사용자 지정 객체를 지정합니다.
export customization	사용자 지정 객체를 내보냅니다.
import customization	사용자 지정 객체를 설치합니다.
revert webvpn all	모든 webvpn 관련 데이터(사용자 지정, 플러그인, 변환 테이블, URL 목록 및 웹 콘텐츠)를 제거합니다.
show webvpn customization	ASA의 플래시 디바이스에 있는 현재 사용자 지정 객체를 표시합니다.

revert webvpn plug-in protocol

ASA의 플래시 디바이스에 플러그인을 제거하려면 특별 권한 EXEC 모드에서 **revert webvpn plug-in protocol** 명령을 입력합니다.

revert plug-in protocol *protocol*

구문 설명

protocol	다음 문자열 중 하나를 입력합니다. • **rdp** Remote Desktop Protocol 플러그인은 원격 사용자가 Microsoft Terminal Services를 실행하는 컴퓨터에 연결하도록 허용합니다. • **SSH** Secure Shell 플러그인은 원격 사용자가 원격 컴퓨터에 대해 안전한 채널을 설정하도록 허용하거나, 원격 사용자가 텔넷을 사용하여 원격 컴퓨터에 연결하도록 허용합니다. • **vnc** Virtual Network Computing 플러그인은 원격 사용자가 모니터, 키보드 및 마우스를 사용하여 원격 데스크톱 공유가 켜진 컴퓨터를 보고 제어할 수 있도록 허용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

지정한 Java 기반 클라이언트 애플리케이션에 대한 클라이언트리스 SSL VPN 지원을 비활성화 및 제거하고 ASA의 플래시 드라이브에서도 제거하려면 **revert webvpn plug-in protocol** 명령을 사용합니다.

예

다음 명령은 RDP에 대한 지원을 제거합니다.

```
ciscoasa# revert webvpn plug-in protocol rdp
ciscoasa
```

관련 명령

명령	설명
import webvpn plug-in protocol	지정된 플러그인을 URL에서 ASA의 플래시 디바이스로 복사합니다. 이 명령을 실행하면 클라이언트리스 SSL VPN은 향후 세션을 위한 Java 기반 클라이언트 애플리케이션 사용을 자동으로 지원합니다.
show import webvpn plug-in	ASA의 플래시 디바이스에 있는 플러그인을 나열합니다.

revert webvpn translation-table

ASA 플래시 메모리에서 변환 테이블을 제거하려면 특별 권한 EXEC 모드에서 **revert webvpn translation-table** 명령을 입력합니다.

revert webvpn translation-table *translationdomain language*

구문 설명

translationdomain	사용 가능한 변환 도메인: • AnyConnect • PortForwarder • 배너 • CSD • 사용자 지정 • URL 목록 • (RDP, SSH 및 VNC 플러그인에서 메시지 변환)
language	삭제할 문자 인코딩 방법을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

가져온 변환 테이블을 비활성화 및 제거하고 ASA의 플래시 메모리에서도 제거하려면 **revert webvpn translation-table** 명령을 사용합니다. 변환 테이블을 제거하면 해당되는 경우 기본 설정으로 돌아가게 됩니다.

예

다음 명령은 AnyConnect 변환 테이블, Dutch를 제거합니다.

```
ciscoasa# revert webvpn translation-table anyconnect dutch
ciscoasa
```

관련 명령

명령	설명
revert webvpn all	모든 webvpn 관련 데이터(사용자 지정, 플러그인, 변환 테이블, URL 목록 및 웹 콘텐츠)를 제거합니다.
show webvpn translation-table	Displays the current 변환 테이블은 현재 ASA의 플래시 디바이스에 있습니다.

revert webvpn url-list

ASA에서 URL 목록을 제거하려면 특별 권한 EXEC 모드에서 **revert webvpn url-list** 명령을 입력합니다.

revert webvpn url-list template *name*

구문 설명

template *name*	URL 목록의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

ASA의 플래시 드라이브에서 현재의 URL 목록을 비활성화 및 제거하려면 **revert webvpn url-list** 명령을 사용합니다. url-list를 제거하면 해당되는 경우 기본 설정으로 돌아가게 됩니다.

revert webvpn url-list 명령에 사용된 템플릿 인수는 전에 구성된 URL 목록의 이름을 지정합니다. 그러한 목록을 구성하려면 글로벌 컨피그레이션 모드에서 **url-list** 명령을 사용합니다.

예

다음 명령은 URL 리스트, servers2를 제거합니다.

```
ciscoasa# revert webvpn url-list servers2
ciscoasa
```

관련 명령

명령	설명
revert webvpn all	모든 webvpn 관련 데이터(사용자 지정, 플러그인, 변환 테이블, URL 목록 및 웹 콘텐츠)를 제거합니다.
show running-configuration url-list	구성된 URL 목록 명령의 현재 집합을 표시합니다.
url-list (WebVPN mode)	WebVPN 서버 및 URL의 목록을 특정 사용자 또는 그룹 정책에 적용합니다.

revert webvpn webcontent

ASA 플래시 메모리의 위치에서 특정 웹 객체를 제거하려면 특별 권한 EXEC 모드에서 **revert webvpn webcontent** 명령을 입력합니다.

revert webvpn webcontent *filename*

구문 설명

filename	삭제할 웹 콘텐츠가 있는 플래시 메모리 파일의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특권 실행 모드	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

웹 콘텐츠가 포함된 파일을 비활성화 및 제거하고 ASA의 플래시 메모리에서도 제거하려면 **revert webvpn content** 명령을 사용합니다. 웹 콘텐츠를 제거하면 해당되는 경우 기본 설정으로 돌아가게 됩니다.

예

다음 명령은 웹 콘텐츠 파일, ABCLogo를 ASA 플래시 메모리에서 제거합니다.

```
ciscoasa# revert webvpn webcontent abclogo
ciscoasa
```

관련 명령

명령	설명
revert webvpn all	모든 webvpn 관련 데이터(사용자 지정, 플러그인, 변환 테이블, URL 목록 및 웹 콘텐츠)를 제거합니다.
show webvpn webcontent	현재 ASA의 플래시 메모리에 있는 웹 콘텐츠를 표시합니다.

revocation-check

trustpool 정책에 폐기 검사가 필요한지 여부를 정의하려면 crypto ca trustpool 컨피그레이션 모드에서 **revocation-check** 명령을 사용합니다. 기본 폐기 검사 방법을 복원하려면*(none)* 이 명령의 **no** 형식을 사용합니다.

revocation-check {[**crl**] [**ocsp**] [**none**] }

no revocation-check {[**crl**] [**ocsp**] [**none**]}

구문 설명

crl	ASA에서 폐기 검사 방법으로 CRL을 사용하도록 지정합니다.
none	모든 방법이 오류를 반환하더라도 ASA에서 인증서 상태를 유효한 것으로 해석하도록 지정합니다.
ocsp	ASA에서 폐기 검사 방법으로 OCSP를 사용하도록 지정합니다.

기본값

기본값은 *none*입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Crypto ca trustpool 컨피그레이션 모드	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

OCSP 응답의 서명자는 대개 OCSP 서버(responder) 인증서입니다. 디바이스에서는 응답을 받은 후 responder 인증서의 확인을 시도합니다.

일반적으로 CA는 OCSP responder 인증서의 수명을 비교적 짧게 설정하여 보안 문제의 발생 가능성을 최소화합니다. CA는 폐기 상태 검사가 필요하지 않음을 나타내는 ocsp-no-check 확장을 responder 인증서에 포함합니다. 그러나 이 확장이 없으면 디바이스에서는 **revocation-check** 명령으로 신뢰 지점에 대해 구성한 폐기 방법을 사용하여 인증서 폐기 상태를 확인하려고 시도합니다. 상태 확인을 무시하도록 *none* 옵션을 설정하지 않는 한 OCSP 폐기 검사가 실패하므로 ocsp-no-check 확장이 없는 경우 OCSP responder 인증서를 확인할 수 있어야 합니다.

참고 선택적 인수가 어떤 순서이든 *none*을 반드시 마지막 키워드로 사용해야 합니다.

ASA는 사용자가 구성한 순서대로 방법을 시도하며, 이전 방법에서 오류를 반환하는 경우에만(예: 서버 다운) 상태가 폐기되었는지 확인하는 대신 두 번째와 세 번째 방법을 시도합니다.

클라이언트 인증서의 유효성을 검사하는 신뢰 지점에서 폐기 검사 방법을 설정하고 responder 인증서의 유효성을 검사하는 신뢰 지점에서 폐기 검사를 구성하지 않을 수 있습니다 (**revocation-check none**). 컨피그레이션 예는 **match certificate** 명령을 참조하십시오.

revocation-check crl none 명령으로 ASA를 구성한 경우 클라이언트는 ASA에 연결하면 자동으로 CRL 다운로드를 시작하고(캐시되지 않았기 때문에), 인증서의 유효성을 검사하고, CRL 다운로드를 마무리합니다. 이 경우 CRL이 캐시되지 않았으면 ASA는 CRL을 다운로드하기 전에 인증서의 유효성을 검사합니다.

예

```
ciscoasa(config-ca-trustpoint)# revocation-check ?

crypto-ca-trustpoint mode commands/options:
  crl   Revocation check by CRL
  none  Ignore revocation check
  ocsp  Revocation check by OCSP
(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpool policy	trustpool 정책 정의를 위한 명령을 제공하는 하위 모드로 들어갑니다.
match certificate allow expired-certificate	관리자가 특정 인증서에 대해 만료 검사를 생략하도록 허용합니다.
match certificate skip revocation-check	관리자가 특정 인증서에 대해 폐기 검사를 생략하도록 허용합니다.

rewrite

WebVPN 연결을 통한 특정 애플리케이션 또는 트래픽 유형의 콘텐츠 재작성을 비활성화하려면 webvpn 모드에서 **rewrite** 명령을 사용합니다. 재작성 규칙을 제거하려면 규칙을 고유하게 식별하는 규칙 번호와 함께 이 명령의 **no** 형식을 사용합니다. 모든 재작성 규칙을 제거하려면 번호 없이 명령의 **no** 형식을 사용합니다.

기본적으로 ASA는 모든 WebVPN 트래픽을 재작성 또는 변환합니다.

rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

no rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

구문 설명

disable	특정 트래픽에 대한 콘텐츠 재작성을 비활성화하는 규칙으로서 이 재작성 규칙을 정의합니다. 콘텐츠 재작성을 비활성화하면 트래픽이 보안 어플라이언스를 통과하지 못합니다.
enable	특정 트래픽에 대한 콘텐츠 재작성을 활성화하는 규칙으로서 이 재작성 규칙을 정의합니다.
integer	구성된 모든 규칙 가운데에서 규칙의 순서를 설정합니다. 범위는 1-65534입니다.
name	(선택 사항) 규칙을 적용할 애플리케이션 또는 리소스의 이름을 식별합니다.
order	ASA에서 규칙을 적용할 순서를 정의합니다.
resource-mask	규칙에 대한 애플리케이션 또는 리소스를 식별합니다.
resource name	(선택 사항) 규칙을 적용할 애플리케이션 또는 리소스를 지정합니다. 최대 128바이트.
string	정규식을 포함할 수 있는, 확인할 애플리케이션 또는 리소스의 이름을 지정합니다. 다음 와일드카드를 사용할 수 있습니다. 정규식을 포함할 수 있는, 확인할 패턴을 지정합니다. 다음 와일드카드를 사용할 수 있습니다. * - 모든 것이 일치합니다 . 이 와일드카드는 단독으로 사용할 수 없습니다 . 영숫자 문자열과 함께 사용해야 합니다 . ? - 단일 문자와 일치합니다 . [!seq] - 시퀀스에 없는 문자와 일치합니다 . [seq] - 시퀀스에 있는 문자와 일치합니다 . 최대 300바이트.

기본값

기본값은 모든 것을 재작성하는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.1(1)	이 명령이 추가되었습니다.

사용 지침

ASA는 애플리케이션에 대해 콘텐츠 재작성을 수행하여 WebVPN 연결을 통해 올바르게 작동하도록 보장합니다. 외부 공개 웹사이트 등 일부 애플리케이션에는 이 프로세싱이 필요하지 않습니다. 이러한 애플리케이션에 대해서는 콘텐츠 재작성을 꺼둘 수 있습니다.

사용자가 ASA를 통하지 않고 특정 사이트를 직접 탐색하도록 하려면 rewrite 명령과 disable 옵션을 사용하여 콘텐츠 재작성을 선택적으로 끌 수 있습니다. 이것은 IPsec VPN 연결의 split-tunneling과 유사합니다.

이 명령을 여러 번 사용할 수 있습니다. ASA에서는 순서 번호로 재작성 규칙을 검색한 다음 일치하는 첫 번째 규칙을 적용하므로 엔트리를 구성하는 순서는 중요합니다.

예

다음 예는 cisco.com 도메인의 URL에 대한 콘텐츠 재작성을 끄는 재작성 규칙(순서 번호 1)의 구성 방법을 보여줍니다.

```
ciscoasa(config-webpn)# rewrite order 2 disable resource-mask *cisco.com/*
```

관련 명령

명령	설명
apcf	특정 애플리케이션에 사용할 비표준 규칙을 지정합니다.
proxy-bypass	특정 애플리케이션에 대해 최소 콘텐츠 재작성을 구성합니다.

re-xauth

IPsec 사용자가 IKE rekey를 재인증하도록 하려면 그룹 정책 컨피그레이션 모드에서 **re-xauth enable** 명령을 사용합니다. IKE rekey에 대한 사용자 재인증을 비활성화하려면 **re-xauth disable** 명령을 사용합니다.

실행 중인 컨피그레이션에서 re-xauth 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 그러면 다른 그룹 정책으로부터 IKE rekey에 대한 재인증 값을 상속할 수 있게 됩니다.

re-xauth {**enable** [**extended**] | **disable**}

no re-xauth

구문 설명

disable	IKE rekey에 대한 재인증을 비활성화합니다.
enable	IKE rekey에 대한 재인증을 활성화합니다.
extended	구성된 SA의 최대 수명까지 인증 자격 증명의 재입력에 허용되는 시간을 확장합니다.

기본값

IKE rekey에 대한 재인증이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
그룹 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.0.4	**extended** 키워드가 추가되었습니다.

사용 지침

IKE rekey에 대한 재인증은 IPsec 연결에만 적용됩니다.

IKE rekey에 대한 재인증을 활성화하면 ASA는 초기 Phase 1 IKE 협상 중에 사용자에게 사용자 이름과 비밀번호를 입력하라는 프롬프트를 표시하고, IKE rekey가 발생할 때마다 사용자 인증 프롬프트를 표시합니다. 재인증은 추가 보안을 제공합니다.

자격 증명을 입력할 시간으로 30초가 제공되며, 약 2분이 되어 SA가 만료되고 터널이 종료되기까지 최대 세 번 재시도할 수 있습니다. 구성된 SA의 최대 수명까지 인증 자격 증명을 다시 입력하도록 허용하려면 **extended** 키워드를 사용합니다.

구성된 rekey 간격을 확인하려면 모니터링 모드에서 **show crypto ipsec sa** 명령을 사용하여 보안 관련 수명을 초 단위 및 데이터의 킬로바이트로 확인합니다.

참고 연결의 다른 쪽 끝에 사용자가 없으면 재인증이 실패합니다.

예 다음 예는 그룹 정책 FirstGroup에 대해 rekey의 재인증을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config) #group-policy FirstGroup attributes
ciscoasa(config-group-policy)# re-xauth enable
```

rip send version

인터페이스에서 RIP 업데이트를 전송하는 데 사용할 RIP 버전을 지정하려면 인터페이스 컨피그레이션 모드에서 **rip send version** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

rip send version {[**1**] [**2**]}

no rip send version

구문 설명

1	RIP 버전 1을 지정합니다.
2	RIP 버전 2를 지정합니다.

기본값

ASA는 RIP 버전 1 패킷을 전송합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 **rip send version** 명령을 입력하여 인터페이스 단위로 전역 RIP 전송 버전 설정을 재지정할 수 있습니다.

RIP 버전 2를 지정하면 인접 디바이스 인증을 활성화하고 MD5 기반 암호화를 사용하여 RIP 업데이트를 인증할 수 있습니다.

예

다음 예는 지정된 인터페이스에서 RIP 버전 1 및 2 패킷을 보내고 받도록 ASA를 구성합니다.

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

관련 명령

명령	설명
rip receive version	특정 인터페이스에서 업데이트를 수신할 때 허용할 RIP 버전을 지정합니다.
router rip	RIP 라우팅 프로세스를 활성화하고 해당 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.
version	ASA에서 전체적으로 사용되는 RIP의 버전을 지정합니다.

rip receive version

인터페이스에서 허용되는 RIP의 버전을 지정하려면 인터페이스 컨피그레이션 모드에서 **rip receive version** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

version {[**1**] [**2**]}

no version

구문 설명

1	RIP 버전 1을 지정합니다.
2	RIP 버전 2를 지정합니다.

기본값

ASA는 버전 1 및 버전 2 패킷을 허용합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 **rip receive version** 명령을 입력하여 인터페이스 단위로 전역 설정을 재지정할 수 있습니다.

RIP 버전 2를 지정하면 인접 디바이스 인증을 활성화하고 MD5 기반 암호화를 사용하여 RIP 업데이트를 인증할 수 있습니다.

예

다음 예는 지정된 인터페이스에서 RIP 버전 1 및 2 패킷을 받도록 ASA를 구성합니다.

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

관련 명령

명령	설명
rip send version	특정 인터페이스에서 업데이트를 전송할 때 사용할 RIP 버전을 지정합니다.
router rip	RIP 라우팅 프로세스를 활성화하고 해당 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.
version	ASA에서 전체적으로 사용되는 RIP의 버전을 지정합니다.

rip authentication mode

RIP 버전 2 패킷에 사용할 인증 유형을 지정하려면 인터페이스 컨피그레이션 모드에서 **rip authentication mode** 명령을 사용합니다. 기본 인증 방법을 복원하려면 이 명령의 **no** 형식을 사용합니다.

rip authentication mode {**text** | **md5**}

no rip authentication mode

구문 설명

md5	RIP 메시지 인증에 MD5를 사용합니다.
text	RIP 메시지 인증에 일반 텍스트를 사용합니다(권장하지 않음).

기본값

기본적으로 일반 텍스트 인증이 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

RIP 버전 2를 지정하면 인접 디바이스 인증을 활성화하고 MD5 기반 암호화를 사용하여 RIP 업데이트를 인증할 수 있습니다.

인터페이스에서 **rip authentication** 명령을 보려면 **show interface** 명령을 사용합니다.

예

다음 예는 GigabitEthernet0/3 인터페이스에 구성된 RIP 인증을 보여줍니다.

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key thisismykey key_id 5
```

관련 명령

명령	설명
rip authentication key	RIP 버전 2 인증을 활성화하고 인증 키를 지정합니다.
rip receive version	특정 인터페이스에서 업데이트를 수신할 때 허용할 RIP 버전을 지정합니다.
rip send version	특정 인터페이스에서 업데이트를 전송할 때 사용할 RIP 버전을 지정합니다.
show running-config interface	지정된 인터페이스의 컨피그레이션 명령을 표시합니다.
version	ASA에서 전체적으로 사용되는 RIP의 버전을 지정합니다.

rip authentication key

RIP 버전 2 패킷의 인증을 활성화하고 인증 키를 지정하려면 인터페이스 컨피그레이션 모드에서 **rip authentication key** 명령을 사용합니다. RIP 버전 2 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

rip authentication key [0 | 8] *string* **key_id** *id*

no rip authentication key

구문 설명

0	암호화되지 않은 비밀번호가 이어짐을 지정합니다.
8	암호화된 비밀번호가 이어짐을 지정합니다.
ID	키 인증 값을 지정합니다. 유효한 값의 범위는 1~255입니다.
key	인증 키 문자열에 사용할 공유 키를 지정합니다. 키는 최대 16자를 포함할 수 있습니다.
string	암호화되지 않은(cleartext) 사용자 비밀번호를 지정합니다.

기본값

RIP 인증이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

RIP 버전 2를 지정하면 인접 디바이스 인증을 활성화하고 MD5 기반 암호화를 사용하여 RIP 업데이트를 인증할 수 있습니다. 인접 디바이스 인증을 활성화할 경우, *key* 및 *key_id* 인수가 RIP 버전 2 업데이트를 제공하는 인접 디바이스에서 사용된 것과 동일한지 확인해야 합니다. *key*는 최대 16자의 텍스트 문자열이어야 합니다.

인터페이스에서 **rip authentication** 명령을 보려면 **show interface** 명령을 사용합니다.

예

다음 예는 GigabitEthernet0/3 인터페이스에 구성된 RIP 인증을 보여줍니다.

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb 5
```

관련 명령

명령	설명
rip authentication mode	RIP 버전 2 패키지에 사용할 인증의 유형을 지정합니다.
rip receive version	특정 인터페이스에서 업데이트를 수신할 때 허용할 RIP 버전을 지정합니다.
rip send version	특정 인터페이스에서 업데이트를 전송할 때 사용할 RIP 버전을 지정합니다.
show running-config interface	지정된 인터페이스의 컨피그레이션 명령을 표시합니다.
version	ASA에서 전체적으로 사용되는 RIP의 버전을 지정합니다.

rip receive version

인터페이스에서 허용되는 RIP의 버전을 지정하려면 인터페이스 컨피그레이션 모드에서 **rip receive version** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

version {[**1**] [**2**]}

no version

구문 설명

1	RIP 버전 1을 지정합니다.
2	RIP 버전 2를 지정합니다.

기본값

ASA는 버전 1 및 버전 2 패킷을 허용합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 **rip receive version** 명령을 입력하여 인터페이스 단위로 전역 설정을 재지정할 수 있습니다.

RIP 버전 2를 지정하면 인접 디바이스 인증을 활성화하고 MD5 기반 암호화를 사용하여 RIP 업데이트를 인증할 수 있습니다.

예

다음 예는 지정된 인터페이스에서 RIP 버전 1 및 2 패킷을 받도록 ASA를 구성합니다.

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

관련 명령

명령	설명
rip send version	특정 인터페이스에서 업데이트를 전송할 때 사용할 RIP 버전을 지정합니다.
router rip	RIP 라우팅 프로세스를 활성화하고 해당 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.
version	ASA에서 전체적으로 사용되는 RIP의 버전을 지정합니다.

rip send version

인터페이스에서 RIP 업데이트를 전송하는 데 사용할 RIP 버전을 지정하려면 인터페이스 컨피그레이션 모드에서 **rip send version** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

rip send version {[**1**] [**2**]}

no rip send version

구문 설명

1	RIP 버전 1을 지정합니다.
2	RIP 버전 2를 지정합니다.

기본값

ASA는 RIP 버전 1 패킷을 전송합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
인터페이스 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 **rip send version** 명령을 입력하여 인터페이스 단위로 전역 RIP 전송 버전 설정을 재지정할 수 있습니다.

RIP 버전 2를 지정하면 인접 디바이스 인증을 활성화하고 MD5 기반 암호화를 사용하여 RIP 업데이트를 인증할 수 있습니다.

예

다음 예는 지정된 인터페이스에서 RIP 버전 1 및 2 패킷을 보내고 받도록 ASA를 구성합니다.

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

관련 명령

명령	설명
rip receive version	특정 인터페이스에서 업데이트를 수신할 때 허용할 RIP 버전을 지정합니다.
router rip	RIP 라우팅 프로세스를 활성화하고 해당 프로세스의 라우터 컨피그레이션 모드로 들어갑니다.
version	ASA에서 전체적으로 사용되는 RIP의 버전을 지정합니다.

rmdir

기존 디렉토리를 제거하려면 특별 권한 EXEC 모드에서 **rmdir** 명령을 사용합니다.

rmdir [/noconfirm] [disk0: | disk1: | flash:]*path*

구문 설명

/noconfirm	(선택 사항) 확인 프롬프트를 억제합니다.
disk0*:*	(선택 사항) 비이동식 내장 플래시 메모리 및 그 뒤에 콜론을 지정합니다.
disk1:	(선택 사항) 이동식 외장 플래시 메모리 카드 및 그 뒤에 콜론을 지정합니다.
flash:	(선택 사항) 비이동식 내부 플래시 및 그 뒤에 콜론을 지정합니다. ASA 5500 Series Adaptive Security 어플라이언스에서 **flash** 키워드는 **disk0**의 별칭을 갖게 됩니다.
path	(선택 사항) 제거할 디렉토리의 절대 또는 상대 경로.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

디렉토리가 비어 있지 않으면 **rmdir** 명령이 실패합니다.

예

다음 예는 "test"라는 기존 디렉토리를 제거하는 방법을 보여줍니다.

```
ciscoasa# rmdir test
```

관련 명령

명령	설명
dir	디렉토리 내용을 표시합니다.
mkdir	새 디렉토리를 만듭니다.
pwd	현재의 작업 디렉토리를 표시합니다.
show file	파일 시스템에 대한 정보를 표시합니다.

route

지정한 인터페이스에 대한 고정 또는 기본 경로를 입력하려면 글로벌 컨피그레이션 모드에서 **route** 명령을 사용합니다. 지정된 인터페이스에서 경로를 제거하려면 이 명령의 **no** 형식을 사용합니다.

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

구문 설명

gateway_ip	게이트웨이 라우터의 IP 주소를 지정합니다(이 경로의 next-hop 주소). **참고** 투명 모드에서 *gateway_ip* 인수는 선택 사항입니다.
interface_name	트래픽을 라우팅할 내부 또는 외부 네트워크 인터페이스 이름을 지정합니다.
ip_address	내부 또는 외부 IP 주소를 지정합니다.
metric	(선택 사항) 이 경로의 관리 거리를 지정합니다. 유효한 값의 범위는 1~255입니다. 기본값은 1입니다.
netmask	*ip_address*에 적용할 네트워크 마스크를 지정합니다.
track *number*	(선택 사항) 추적 엔트리를 이 경로와 연결합니다. 유효한 값은 1~500입니다. **참고** **track** 옵션은 라우팅된 단일 모드에서만 사용할 수 있습니다.
tunneled	VPN 트래픽에 대한 기본 터널 게이트웨이로 경로를 지정합니다.

기본값

metric 기본값은 1입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	**track** *number* 값이 추가되었습니다.

사용 지침

인터페이스에 대해 기본 또는 고정 경로를 입력하려면 **route** 명령을 사용합니다. 기본 경로를 입력하려면 *ip_address*와 *netmask*를 **0.0.0.0** 또는 축약된 형태인 **0**으로 설정합니다. **route** 명령을 사용하여 입력하는 모든 경로는 저장 시 컨피그레이션에 보관됩니다.

표준 기본 경로를 가지고 터널링된 트래픽을 위한 별도의 기본 경로를 정의할 수 있습니다. **tunneled** 옵션으로 기본 경로를 생성하면 학습 경로나 고정 경로를 이용하여 라우팅할 수 없는 ASA에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다. 터널에서 발생하는 트래픽에 대해 이 경로는 다른 구성된 또는 학습된 기본 경로를 재지정합니다.

tunneled 옵션을 포함한 기본 경로에는 다음 제한 사항이 적용됩니다.

- 터널링 경로의 이그레스 인터페이스에서 유니캐스트 RPF(**ip verify reverse-path**)를 활성화하지 마십시오. 터널링 경로의 이그레스 인터페이스에서 uRPF를 활성화하면 세션이 실패합니다.
- 세션이 실패할 수 있으므로 터널링 경로의 이그레스 인터페이스에서 TCP 인터셉트를 활성화하지 마십시오.
- VoIP 검사 엔진(CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), DNS 검사 엔진 또는 DCE RPC 검사 엔진을 터널링 경로에 사용하지 마십시오. 이러한 검사 엔진은 터널링 경로를 무시합니다.

tunneled 옵션으로 두 개 이상의 기본 경로를 정의할 수 없습니다. 터널링 트래픽에 대한 ECMP는 지원되지 않습니다.

인터페이스에서 라우터 외부에 연결된 네트워크에 액세스하려면 고정 경로를 만듭니다. 예를 들어 ASA는 192.168.42.0 네트워크로 이동하는 모든 패킷을 다음과 같은 고정 **route** 명령으로 192.168.1.5 라우터를 통해 전송합니다.

```
ciscoasa(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

각 라우터의 IP 주소를 입력하면 ASA는 라우팅 테이블에 CONNECT 경로를 생성합니다. 이 엔트리는 **clear route** 또는 **clear configure route** 명령 사용 시 삭제되지 않습니다.

route 명령에서 ASA의 인터페이스 중 하나의 IP 주소를 게이트웨이 IP 주소로 사용하는 경우, ASA는 게이트웨이 IP 주소 대신 패킷의 수신 IP 주소에 대해 ARP를 사용합니다.

예

다음 예는 외부 인터페이스에 대해 하나의 기본 **route** 명령을 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# route outside 0 0 209.165.201.1 1
```

다음 예는 네트워크에 대한 액세스를 제공하기 위해 이러한 고정 **route** 명령을 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
ciscoasa(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

다음 예는 SLA 작업을 사용하여 외부 인터페이스의 10.1.1.1 게이트웨이에 기본 경로를 설치합니다. SLA 작업은 해당 게이트웨이의 가용성을 모니터링합니다. SLA 작업이 실패하면 DMZ 인터페이스의 백업 경로가 사용됩니다.

```
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
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
ciscoasa(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

관련 명령

명령	설명
clear configure route	고정으로 구성된 **route** 명령을 제거합니다.
clear route	RIP와 같은 동적 라우팅 프로토콜을 통해 학습된 경로를 제거합니다.
show route	경로 정보를 표시합니다.
show running-config route	구성된 경로를 표시합니다.

route-map

한 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의하거나 정책 라우팅을 활성화하려면 글로벌 컨피그레이션 모드에서 **route-map** 명령을 사용하고 경로 맵 컨피그레이션 모드에서 match 및 set 명령을 사용합니다. 엔트리를 삭제하려면 이 명령의 **no** 형식을 사용합니다.

route-map *name* [**permit | deny**] [*sequence number*]

no route-map *name* [**permit | deny**] [*sequence number*]

구문 설명

name	경로 맵에 대해 의미 있는 이름을 정의합니다. 재배포 라우터 컨피그레이션 명령은 이 이름을 사용하여 이 경로 맵을 참조합니다. 여러 경로 맵에서 동일한 이름을 공유할 수 있습니다.
permit	(선택 사항) 이 경로 맵에 대해 일치 기준이 충족되고 **permit** 키워드가 지정되면, 설정된 작업으로 제어되면서 경로가 재배포됩니다. 정책 라우팅의 경우에는 패킷이 정책으로 라우팅됩니다(policy routed). 일치 기준이 충족되지 않고 **permit** 키워드가 지정되면, 동일한 맵 태그의 다음 경로 맵이 테스트됩니다. 동일한 이름을 공유하는 경로 맵 집합에 대한 일치 기준을 하나도 통과하지 못하는 경로는 해당 집합에 의해 재배포되지 않습니다. **permit** 키워드가 기본값입니다.
deny	(선택 사항) 경로 맵에 대해 일치 기준이 충족되고 **deny** 키워드가 지정되면 경로가 재배포되지 않습니다. 정책 라우팅의 경우에는 패킷이 정책으로 라우팅되지 않으며(not policy routed), 동일한 맵 태그 이름을 공유하는 추가 경로 맵이 검토되지 않습니다. 패킷이 정책으로 라우팅되지 않으면 일반적인 전달 알고리즘이 사용됩니다.
sequence-number	(선택 사항) 동일한 이름으로 이미 구성된 경로 맵의 목록에서 새 경로 맵이 갖게 될 위치를 나타내는 번호입니다. 이 명령의 no 형식을 사용하면 경로 맵의 위치가 삭제됩니다.

기본값

기본값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.

사용 지침

경로를 재배포하려면 경로 맵을 사용합니다.

route-map 글로벌 컨피그레이션 명령과 match 및 set route-map 컨피그레이션 명령을 사용하면 하나의 라우팅 프로토콜에서 다른 라우팅 프로토콜로 경로를 재배포하기 위한 조건을 정의할 수 있습니다. 각 **route-map** 명령에는 연결된 match 및 set 명령이 있습니다. match 명령은 일치 기준(현재의 route-map 명령으로 재배포가 허용되는 조건)을 지정합니다. set 명령은 set 작업, 즉 match 명령으로 적용된 기준이 충족되는 경우 수행할 특별한 재배포 작업을 지정합니다. **no route-map** 명령은 경로 맵을 삭제합니다.

match route-map 컨피그레이션 명령에는 여러 형식이 있습니다. match 명령은 어떤 순서로든 사용할 수 있으며, set 명령으로 지정한 set 작업에 따라 경로를 재배포하려면 모든 match 명령을 "통과"해야 합니다. match 명령의 no 형식은 지정된 일치 기준을 제거합니다.

라우팅 프로세스 간에 경로 재배포 방법을 세밀하게 제어하려면 경로 맵을 사용합니다. 대상 라우팅 프로토콜은 라우터 글로벌 컨피그레이션 명령으로 지정합니다. 소스 라우팅 프로토콜은 재배포 라우터 컨피그레이션 명령으로 지정합니다. 경로 맵 구성 방법에 대한 설명은 "예" 섹션을 참조하십시오.

경로 맵을 통해 경로를 전달할 때, 경로 맵은 여러 부분으로 구성될 수 있습니다. route-map 명령과 관련된 match 구문과 하나 이상 일치하지 않는 경로는 무시됩니다. 즉, 경로가 아웃바운드 경로 맵에 대해 광고되지 않으며 인바운드 경로 맵에 대해 허용되지 않습니다. 일부 데이터만 수정하려는 경우 두 번째 경로 맵 섹션을 구성하고 정확한 일치를 지정해야 합니다.

sequence-number 인수는 다음과 같이 작동합니다.

1. route-map 이름으로 정의한 엔트리가 없으면, sequence-number 인수가 10으로 설정된 엔트리가 생성됩니다.
2. route-map 이름으로 정의한 엔트리가 하나뿐인 경우 이 엔트리는 다음 route-map 명령의 기본 엔트리가 됩니다. 이 엔트리의 sequence-number 인수는 변경되지 않습니다.
3. route-map 이름으로 정의된 엔트리가 둘 이상인 경우 sequence-number 인수가 필요하다는 내용의 오류 메시지가 표시됩니다.
4. sequence-number 인수 없이 **no route-map name** 명령을 지정하는 경우 전체 경로 맵이 삭제됩니다.

예

다음 예는 합 개수가 1과 같은 경로를 OSPF로 재배포하는 방법을 보여줍니다. ASA에서는 이러한 경로를 메트릭이 5이고 메트릭 유형이 Type 1인 외부 LSA로서 재배포합니다.

```
ciscoasa(config)# route-map 1-to-2 permit

ciscoasa(config-route-map)# match metric 11
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

다음 예는 10.1.1.0 고정 경로를 다음의 구성된 메트릭 값의 eigrp 프로세스 1로 재배포하는 방법을 설명합니다.

```
ciscoasa (config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config)# redistribute static metric 250 250 1 1 1 route-map
```

관련 명령

명령	설명
redistribute	하나의 라우팅 도메인에서 다른 라우팅 도메인으로 경로를 재배포합니다.
route	인터페이스에 대한 고정 또는 기본 경로를 생성합니다.
router	지정된 프로토콜에 대해 라우터 컨피그레이션 모드로 들어갑니다.

route null0

고정 null0 경로는 black hole로 원하지 않거나 바람직하지 않은 트래픽을 전달하는 데 사용됩니다. null 인터페이스 null0은 black hole 생성에 사용됩니다. 바람직하지 않은 대상에 대해 고정 경로를 생성하려면 글로벌 컨피그레이션 모드에서 **route null0** 명령을 사용합니다. 이 고정 경로 컨피그레이션은 null 인터페이스를 가리킵니다.

고정 null0 경로를 제거하려면 이 명령의 **no** 형식을 사용합니다.

route null0 *ip_address*

no route null0 *ip_address*

구문 설명

ip_address	내부 또는 외부 IP 주소를 지정합니다.

기본값

고정 null 0 경로는 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

고정 경로는 바람직하지 않은 대상에 대해 생성되며 고정 경로 컨피그레이션은 null 인터페이스를 향합니다. black hole 고정 경로와의 최적의 일치를 포함한 대상 주소의 트래픽은 자동으로 삭제됩니다. ACL과는 달리 고정 null0 경로는 성능 저하를 일으키지 않습니다.

고정 null0 경로 컨피그레이션은 라우팅 루프를 방지하는 데 사용됩니다. BGP는 Remotely Triggered Black Hole 라우팅을 위해 고정 null0 컨피그레이션을 활용합니다.

예

다음 예는 고정 null0 경로 구성 방법을 보여줍니다.

```
ciscoasa(config)# route null0 192.168.2.0 255.255.255.0
```

router-alert

IP Options 검사의 패킷에 Router Alert IP 옵션이 있는 경우 수행할 작업을 정의하려면 매개변수 컨피그레이션 모드에서 **router-alert** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

router-alert action {allow | clear}

no router-alert action {allow | clear}

구문 설명

allow	Router Alert IP 옵션이 포함된 패킷의 통과를 허용하도록 ASA에 지시합니다.
clear	패킷에서 Router Alert IPP 옵션을 지우고 패킷의 통과를 허용하도록 ASA에 지시합니다.

기본값

기본적으로 IP Options 검사는 Router Alert IP 옵션이 포함된 패킷을 삭제합니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
8.2(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IP Options 검사 정책 맵에서 구성할 수 있습니다.

ASA를 통과하도록 허용할 특정 IP 옵션의 IP 패킷을 제어하려면 IP Options 검사를 구성할 수 있습니다. 이 검사를 구성하면 ASA는 패킷이 통과하도록 허용하거나, 지정된 IP 옵션을 지운 다음 패킷이 통과하도록 허용합니다.

RTRALT(Router Alert) 또는 IP Option 20은 트랜싯 라우터에 패킷의 내용을 검사하도록 알립니다(패킷의 목적지가 해당 라우터가 아닌 경우에도). 이 검사는 RSVP 및 패킷의 배달 경로에 있는 라우터에서 비교적 복잡한 프로세싱을 수행하도록 요구하는 유사 프로토콜을 구현할 때 매우 유용합니다.

예

다음 예는 정책 맵에서 프로토콜 위반에 대한 작업을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

router-id

고정 라우터 ID를 사용하려면 OSPFv2용 라우터 컨피그레이션 모드 또는 IPv6용 라우터 컨피그레이션 모드에서 **router-id** 명령을 사용합니다. 이전 라우터 ID 동작을 사용하도록 OSPF를 재설정하려면 이 명령의 **no** 형식을 사용합니다.

router-id *id*

no router-id [*id*]

구문 설명

id	IP 주소 형식으로 라우터 ID를 지정합니다.

기본값

지정하지 않는 경우 ASA에서 최상위 수준의 IP 주소가 라우터 ID로 사용됩니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—
IPv6 라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
8.0(2)	이 명령의 처리 순서가 변경되었습니다. 이 명령은 이제 OSPFv2 컨피그레이션의 **network** 명령 이전에 처리됩니다.
9.0(1)	다중 컨텍스트 모드 및 OSPFv3이 지원됩니다.

사용 지침

기본적으로 ASA는 OSPF 컨피그레이션의 **network** 명령이 적용되는 인터페이스에서 최상위 수준의 IP 주소를 사용합니다. 최상위 수준의 IP 주소가 사설 주소이면 해당 주소는 hello 패킷 및 데이터베이스 정의에서 전송됩니다. 특정 라우터 ID를 사용하려면 **router-id** 명령을 사용하여 라우터 ID용 전역 주소를 지정합니다.

라우터 ID는 OSPF 라우팅 도메인 내에서 고유해야 합니다. 동일한 OSPF 도메인에서 두 라우터가 동일한 라우터 ID를 사용하면 라우팅이 제대로 작동하지 않을 수 있습니다.

OSPF 컨피그레이션에서 **network** 명령을 입력하기 전에 **router-id** 명령을 입력해야 합니다. 이렇게 하면 ASA에서 생성하는 기본 라우터 ID와 충돌할 가능성이 차단됩니다. 충돌이 발생하면 다음 메시지가 수신됩니다.

```
ERROR: router-id id in use by ospf process pid
```

충돌 ID를 입력하려면 충돌을 일으키는 IP 주소가 포함된 **network** 명령을 제거하고, **router-id** 명령을 입력한 다음, **network** 명령을 다시 입력합니다.

클러스터링

모든 유닛이 동일한 라우터 ID를 수신하는 경우 Layer 2 클러스터링에서 **router-id** *id* 명령을 구성하거나 라우터 ID를 공백으로 유지해야 합니다.

예

다음 예는 라우터 ID를 192.168.1.1로 설정합니다.

```
ciscoasa(config-rtr)# router-id 192.168.1.1
ciscoasa(config-rtr)#
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드로 들어갑니다.
show ospf	OSPFv2 라우팅 프로세스에 대한 일반 정보가 표시됩니다.

router-id cluster-pool

Layer 3 클러스터링 구축을 위한 라우터 ID 클러스터 풀을 지정하려면 OSPFv2용 라우터 컨피그레이션 모드 또는 OSPFv3용 라우터 컨피그레이션 모드에서 **router-id cluster-pool** 명령을 사용합니다.

router-id cluster-pool hostname | A.B.C.D *ip_pool*

구문 설명

cluster-pool	Layer 3 클러스터링이 구성된 경우 IP 주소 풀의 컨피그레이션을 활성화합니다.
hostname | A.B.C.D	이 OSPF 프로세스에 대한 OSPF 라우터 ID를 지정합니다.
ip_pool	IP 주소 풀의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—
IPv6 라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
9.0(1)	이 명령이 추가되었습니다.

사용 지침

라우터 ID는 클러스터링의 OSPFv2 또는 OSPFv3 라우팅 도메인 내에서 고유해야 합니다. 동일한 OSPFv2 또는 OSPFv3 도메인에서 두 라우터가 동일한 라우터 ID를 사용하면 클러스터링의 라우팅이 제대로 작동하지 않을 수 있습니다.

모든 유닛이 동일한 라우터 ID를 수신하는 경우 Layer 2 클러스터링에서 **router-id** *id* 명령을 구성하거나 라우터 ID를 공백으로 유지해야 합니다.

Layer 3 클러스터 인터페이스가 구성된 경우 각 유닛은 고유한 인터페이스 IP 주소를 가져야 합니다. 각 유닛이 고유한 인터페이스 IP 주소를 갖도록 하려면 **router-id cluster-pool** 명령으로 OSPFv2 또는 OSPFv3에 대한 IP 주소의 로컬 풀을 구성할 수 있습니다.

예

다음 예는 OSPFv2에 대해 Layer 3 클러스터링이 구성된 경우 IP 주소 풀을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ip local pool rpool 1.1.1.1-1.1.1.4
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
ciscoasa(config-rtr)# log-adj-changes
```

다음 예는 OSPFv3에 대해 Layer 3 클러스터링이 구성된 경우 IP 주소 풀을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# ipv6 router ospf 2
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# interface gigabitEthernet0/0
ciscoasa(config-rtr)# nameif inside
ciscoasa(config-rtr)# security-level 0
ciscoasa(config-rtr)# ip address 17.5.33.1 255.255.0.0 cluster-pool inside_pool
ciscoasa(config-rtr)# ipv6 address 8888::1/64 cluster-pool p6
ciscoasa(config-rtr)# ipv6 nd suppress-ra
ciscoasa(config-rtr)# ipv6 ospf 2 area 0.0.0.0
```

관련 명령

명령	설명
ipv6 router ospf	IPv6 라우터 컨피그레이션 모드로 들어갑니다.
router ospf	라우터 컨피그레이션 모드로 들어갑니다.
show ipv6 ospf	OSPFv3 라우팅 프로세스에 대한 일반 정보가 표시됩니다.
show ospf	OSPFv2 라우팅 프로세스에 대한 일반 정보가 표시됩니다.

router bgp

BGP(Border Gateway Protocol) 라우팅 프로세스를 구성하려면 글로벌 컨피그레이션 모드에서 **router bgp** 명령을 사용합니다. BGP 라우팅 프로세스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

router bgp *autonomous-system-number*

no router bgp *autonomous-system-number*

구문 설명

autonomous-system-number	다른 BGP 라우터에 대한 라우터를 식별하고 전달되는 라우팅 정보를 태깅하는 자동 시스템의 수. 범위는 1~65535입니다.

기본값

BGP 라우팅 프로세스는 기본적으로 활성화되어 있지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	• 예

명령 기록

릴리스	수정
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 자동 시스템 간 라우팅 정보의 루프 프리(loop-free) 교환을 자동으로 보장하는 배포된 라우팅 코어를 설정할 수 있습니다.

2009년 1월 전에는 회사에 할당된 BGP 자동 시스템 번호가 RFC 4271, *BGP-4(Border Gateway Protocol 4)* 에 설명된 대로 1~65535 범위의 2-옥텟이었습니다.

자동 시스템 번호에 대한 수요가 증가함에 따라 이제 IANA(Internet Assigned Number Authority)에서는 자동 시스템 번호로 65536~4294967295 범위의 4-옥텟을 할당합니다.

RFC 5396(*Textual Representation of Autonomous System(AS) Numbers*)에서는 자동 시스템 번호를 나타내는 세 가지 방법에 대해 설명합니다. Cisco에서는 다음 두 가지 방법을 구현했습니다.

- Asplain - 2바이트 및 4바이트 자동 시스템 번호를 십진수 값으로 나타내는 십진수 값 표기법. 예를 들어 65526은 2바이트 자동 시스템 번호이고 234567은 4바이트 자동 시스템 번호입니다.
- Asdot - 2바이트 자동 시스템 번호는 십진수 값으로 표시되고 4바이트 자동 시스템 번호는 dot 표기법으로 표시되는 자동 시스템 dot 표기법. 예를 들어 65526은 2바이트 자동 시스템 번호이고 1.169031은 4바이트 자동 시스템 번호(234567 십진수의 dot 표기법)입니다.

자동 시스템 번호를 나타내는 세 번째 방법에 대한 자세한 내용은 RFC 5396을 참조하십시오.

예

다음 예는 자동 시스템 번호 100에 대한 BGP 프로세스를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)#
```

관련 명령

명령	설명
show route bgp	라우팅 테이블을 표시합니다.
show bgp summary	모든 BGP(Border Gateway Protocol) 연결 상태를 표시합니다.

router eigrp

EIGRP 라우팅 프로세스를 시작하고 해당 프로세스에 대해 매개변수를 구성하려면 글로벌 컨피그레이션 모드에서 **router eigrp** 명령을 사용합니다. EIGRP 라우팅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

router eigrp *as-number*

no router eigrp *as-number*

구문 설명

as-number	다른 EIGRP 라우터에 대한 경로를 식별하는 자동 시스템 번호. 라우팅 정보를 태깅하는 데에도 사용됩니다. 유효한 값은 1~65535입니다.

기본값

EIGRP 라우팅이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.0(2)	이 명령이 추가되었습니다.

사용 지침

EIGRP 라우팅 프로세스를 만들거나 기존 EIGRP 라우팅 프로세스에 대한 컨피그레이션 모드로 들어가려면 **router eigrp** 명령을 사용합니다. ASA에서는 단일 EIGRP 라우팅 프로세스만 만들 수 있습니다.

다음 라우터 컨피그레이션 모드 명령을 사용하면 EIGRP 라우팅 프로세스를 구성할 수 있습니다.

- **auto-summary** - 자동 경로 요약을 활성화/비활성화합니다.
- **default-information** - 기본 경로 정보의 송신과 수신을 활성화/비활성화합니다.
- **default-metric** - EIGRP 라우팅 프로세스로 재배포되는 경로의 기본 메트릭을 정의합니다.
- **distance eigrp** - 내부 및 외부 EIGRP 경로에 대한 관리 거리를 구성합니다.
- **distribute-list** - 라우팅 업데이트에서 보내고 받는 네트워크를 필터링합니다.
- **eigrp log-neighbor-changes** - 인접 디바이스 상태 변경의 기록을 활성화/비활성화합니다.
- **eigrp log-neighbor-warnings** - 인접 디바이스 경고 메시지의 기록을 활성화/비활성화합니다.
- **eigrp router-id** - 고정 라우터 ID를 생성합니다.
- **eigrp stub** - 스텁 EIGRP 라우팅을 위해 ASA를 구성합니다.
- **neighbor** - EIGRP 인접 디바이스를 고정으로 정의합니다.

- **network** - EIGRP 라우팅 프로세스에 참여하는 네트워크를 구성합니다.
- **passive-interface** - 패시브 인터페이스 역할을 하도록 인터페이스를 구성합니다.
- **redistribute** - 다른 라우팅 프로세스에서 EIGRP로 경로를 재배포합니다.

인터페이스 관련 EIGRP 매개변수를 구성하려면 다음 인터페이스 컨피그레이션 모드 명령을 사용합니다.

- **authentication key eigrp** - EIGRP 메시지 인증에 사용할 인증 키를 정의합니다.
- **authentication mode eigrp** - EIGRP 메시지 인증에 사용할 인증 알고리즘을 정의합니다.
- **delay** - 인터페이스에 대한 지연 메트릭을 구성합니다.
- **hello-interval eigrp** - 인터페이스에서 EIGRP hello 패킷을 전송할 간격을 변경합니다.
- **hold-time eigrp** - ASA에서 광고할 대기 시간을 변경합니다.
- **split-horizon eigrp** - 인터페이스에서 EIGRP split-horizon을 활성화/비활성화합니다.
- **summary-address eigrp** - 요약 주소를 수동으로 정의합니다.

예

다음 예는 자동 시스템 번호 100의 EIGRP 라우팅 프로세스를 위한 컨피그레이션 모드로 들어가는 방법을 보여줍니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-rtr)#
```

관련 명령

명령	설명
clear configure eigrp	실행 중인 컨피그레이션에서 EIGRP 라우터 컨피그레이션 모드 명령을 지웁니다.
show running-config router eigrp	실행 중인 컨피그레이션에서 EIGRP 라우터 컨피그레이션 모드 명령을 표시합니다.

router ospf

OSPF 라우팅 프로세스를 시작하고 해당 프로세스에 대해 매개변수를 구성하려면 글로벌 컨피그레이션 모드에서 **router ospf** 명령을 사용합니다. OSPF 라우팅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

router ospf *pid*

no router ospf *pid*

구문 설명

pid	OSPF 라우팅 프로세스에 대해 내부적으로 사용되는 식별 매개변수로서, 유효한 값은 1~65535입니다. *pid*는 다른 라우터에서 OSPF 프로세스의 ID를 확인할 필요가 없습니다.

기본값

OSPF 라우팅이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

router ospf 명령은 ASA에서 실행 중인 OSPF 라우팅 프로세스를 위한 글로벌 컨피그레이션 명령입니다. **router ospf** 명령을 입력하면 명령 프롬프트가 (config-router)#으로 표시되는데, 이는 라우터 컨피그레이션 모드에 있음을 나타냅니다.

no router ospf 명령을 사용할 경우, 필요한 정보를 제공하지 않는 한 선택적인 인수를 지정할 필요가 없습니다. **no router ospf** 명령은 *pid* 로 지정한 OSPF 라우팅 프로세스를 종료합니다.*pid*는 ASA에서 로컬로 할당합니다. 각 OSPF 라우팅 프로세스에 고유한 값을 할당해야 합니다.

router ospf 명령을 다음과 같은 OSPF 관련 명령과 함께 사용하면 OSPF 라우팅 프로세스를 구성할 수 있습니다.

- **area** - 일반적인 OSPF 영역을 구성합니다.
- **compatible rfc1583** - RFC 1583당 요약 경로 비용을 계산하는 데 사용할 방법을 복원합니다.
- **default-information originate** - OSPF 라우팅 도메인에 기본 외부 경로를 생성합니다.
- **distance** - 경로 유형을 기준으로 OSPF 경로 관리 거리를 정의합니다.

- **ignore** - 라우터에 Type 6 Multicast OSPF(MOSPF)에 대한 링크 상태 광고(LSA)가 수신될 경우, syslog 메시지가 전송되는 것을 억제합니다.
- **log-adj-changes** - OSPF 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다.
- **neighbor** - 인접 라우터를 지정합니다. VPN 터널을 통해 설정되는 근접성을 허용하는 데 사용됩니다.
- **network** - OSPF가 실행되는 주소 및 해당 인터페이스의 영역 ID를 정의합니다.
- **redistribute** - 지정된 매개변수에 따라 하나의 라우팅 도메인에서 다른 도메인으로 경로를 재배포하도록 구성합니다.
- **router-id** - 고정 라우터 ID를 생성합니다.
- **summary-address** - OSPF에 대한 종합 주소를 생성합니다.
- **timer lsa arrival** - OSPF 인접 디바이스에서 동일한 LSA(링크 상태 광고)를 허용하는 최소 간격(msec)을 정의합니다.
- **timer pacing flood** - 플러딩 큐의 LSA가 업데이트되는 최소 간격(msec)을 정의합니다.
- **timer pacing lsa-group** - LSA 그룹의 새로 고침 또는 maxage 간격(msec)을 정의합니다.
- **timer pacing retransmission** - 인접 디바이스 재전송 간 최소 간격(msec)을 정의합니다.
- **timer throttle lsa** - 첫 번째 LSA를 생성하기 위한 지연을 정의합니다(msec).
- **timer throttle spf** - SPF 계산에 대한 변경 수신 간의 지연을 정의합니다(msec).

예

다음 예는 번호 5의 OSPF 라우팅 프로세스를 위한 컨피그레이션 모드로 들어가는 방법을 보여줍니다.

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)#
```

관련 명령

명령	설명
clear configure router	실행 중인 컨피그레이션에서 OSPF 라우터 명령을 지웁니다.
show running-config router ospf	실행 중인 컨피그레이션의 OSPF 라우터 명령을 표시합니다.

router rip

RIP 라우팅 프로세스를 시작하고 해당 프로세스에 대해 매개변수를 구성하려면 글로벌 컨피그레이션 모드에서 **router rip** 명령을 사용합니다. RIP 라우팅 프로세스를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

router rip

no router rip

구문 설명

이 명령에는 인수나 키워드가 없습니다.

기본값

RIP 라우팅이 비활성화되어 있습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
글로벌 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

사용 지침

router rip 명령은 ASA에서 RIP 라우팅 프로세스를 구성하기 위한 글로벌 컨피그레이션 명령입니다. ASA에서 하나의 RIP 프로세스만 구성할 수 있습니다. **no router rip** 명령은 RIP 라우팅 프로세스를 종료하고 해당 프로세스에 대한 모든 라우터 컨피그레이션을 제거합니다.

router rip 명령을 입력하면 명령 프롬프트가 ciscoasa(config-router)#으로 변경되는데, 이는 라우터 컨피그레이션 모드에 있음을 나타냅니다.

router rip 명령을 다음과 같은 라우터 컨피그레이션 명령과 함께 사용하면 RIP 라우팅 프로세스를 구성할 수 있습니다.

- **auto-summary** - 경로의 자동 요약을 활성화/비활성화합니다.
- **default-information originate** - 기본 경로를 배포합니다.
- **distribute-list in** - 들어오는 라우팅 업데이트에서 네트워크를 필터링합니다.
- **distribute-list out** - 나가는 라우팅 업데이트에서 네트워크를 필터링합니다.
- **network** - 라우팅 프로세스에서 인터페이스를 추가/제거합니다.
- **passive-interface** - 특정 인터페이스를 패시브 모드로 설정합니다.
- **redistribute** - 다른 라우팅 프로세스에서 RIP 라우팅 프로세스로 경로를 재배포합니다.
- **version** - ASA에서 사용되는 RIP 프로토콜 버전을 설정합니다.

또한 인터페이스 컨피그레이션 모드에서 다음 명령을 사용하여 인터페이스 기반으로 RIP 속성을 구성할 수 있습니다.

- **rip authentication key** - 인증 키를 설정합니다.
- **rip authentication mode** - RIP 버전 2에서 사용되는 인증 유형을 설정합니다.
- **rip send version** - 인터페이스 외부로 업데이트를 전송하는 데 사용되는 RIP의 버전을 설정합니다. 이 값은 전역 라우터 컨피그레이션 모드에서 설정한 버전(있는 경우)을 재지정합니다.
- **rip receive version** - 인터페이스에서 허용되는 RIP의 버전을 설정합니다. 이 값은 전역 라우터 컨피그레이션 모드에서 설정한 버전(있는 경우)을 재지정합니다.

투명 모드에서는 RIP가 지원되지 않습니다. 기본적으로 ASA는 모든 RIP 브로드캐스트 및 멀티캐스트 패킷을 거부합니다. 이러한 RIP 메시지가 투명 모드에서 운영되는 ASA를 통과하도록 허용하려면 이 트래픽을 허용하는 액세스 목록 엔트리를 정의해야 합니다. 예를 들어 RIP 버전 2 트래픽이 ASA를 통과하도록 허용하려면 다음과 같은 액세스 목록 엔트리를 생성합니다.

```
ciscoasa(config)# access-list myriplist extended permit ip any host 224.0.0.9
```

RIP 버전 1 브로드캐스트를 허용하려면 다음과 같은 액세스 목록 엔트리를 생성합니다.

```
ciscoasa(config)# access-list myriplist extended permit udp any any eq rip
```

access-group 명령을 사용하여 이러한 액세스 목록 엔트리를 적절한 인터페이스에 적용하십시오.

RIP 및 OSPF 라우팅을 동시에 ASA에서 활성화할 수 있습니다.

예

다음 예는 번호 5의 OSPF 라우팅 프로세스를 위한 컨피그레이션 모드로 들어가는 방법을 보여줍니다.

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# version 2
```

관련 명령

명령	설명
clear configure router rip	실행 중인 컨피그레이션에서 RIP 라우터 명령을 지웁니다.
show running-config router rip	실행 중인 컨피그레이션의 RIP 명령을 표시합니다.

rtp-conformance

H.323 및 SIP의 프로토콜 적합성을 위해 핀홀에서 RTP 패킷 흐름을 확인하려면 매개변수 컨피그레이션 모드에서 **rtp-conformance** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

구문 설명

enforce-payloadtype	신호 교환을 기반으로 오디오/비디오에 페이로드 유형을 적용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정
7.2(1)	이 명령이 추가되었습니다.

예

다음 예는 H.323 통화의 프로토콜 적합성을 위해 핀홀에서 RTP 패킷 흐름을 확인하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# rtp-conformance
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션과 관련된 트래픽을 확인하기 위한 검사 클래스 맵을 만듭니다.
debug rtp	H.323 및 SIP 검사와 관련된 RTP 패킷의 디버그 정보 및 오류 메시지를 표시합니다.
policy-map	Layer 3/4 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 컨피그레이션을 표시합니다.

rtp-min-port rtp-max-port

Phone Proxy 기능에 대해 rtp-min-port 및 rtp-max-port 제한을 구성하려면 phone-proxy 컨피그레이션 모드에서 **rtp-min-port** *port1* **rtp-max-port** *port2* 명령을 사용합니다.

phone proxy 컨피그레이션에서 rtp-min-port 및 rtp-max-port 제한을 제거하려면 이 명령의 **no** 형식을 사용합니다.

rtp-min-port *port1* **rtp-maxport** *port2*

no rtp-min-port *port1* **rtp-maxport** *port2*

구문 설명

port1	미디어 종료 지점의 RTP 포트 범위에 대한 최소값을 지정합니다. 여기서 *port1*은 1024~16384 범위로 값을 설정할 수 있습니다.
port2	미디어 종료 지점의 RTP 포트 범위에 대한 최대값을 지정합니다. 여기서 *port2*는 32767~65535 범위로 값을 설정할 수 있습니다.

기본값

기본적으로 **rtp-min-port** 키워드의 *port1* 값은 16384이고 **rtp-max-port** 키워드의 *port2* 값은 32767입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명성	단일	컨텍스트	시스템
Phone-proxy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정
8.2(1)	이 명령이 추가되었습니다.

사용 지침

Phone Proxy에서 지원하는 통화 수를 늘려야 할 경우 미디어 종료 지점에 대한 RTP 포트 범위를 구성합니다.

예

다음 예는 미디어 연결에 사용할 IP 주소를 지정하기 위해 **media-termination address** 명령을 사용하는 방법을 보여줍니다.

```
ciscoasa(config-phone-proxy)# rtp-min-port 2001 rtp-maxport 32770
```

관련 명령

명령	설명
phone-proxy	Phone Proxy 인스턴스를 구성합니다.