Cisco ASA Series 명령 참조 , A ~ H 명령

업데이트 : 2014 년 11 월 5 일

Cisco Systems, Inc.
www.cisco.com

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

텍스트 파트 번호 : 해당 없음 , 온라인 전용

Cisco ASA Series 명령 참조 , A ~ H 명령

파 트 **1**

A ~ B 명령

1 장

aaa accounting command ~ accounting-server-group 명령

aaa accounting command

CLI에서 **show** 명령이 아닌 임의의 명령을 입력할 때 TACACS+ 어카운팅 서버에 어카운팅 메시지를 보내려면 글로벌 컨피그레이션 모드에서 **aaa accounting command** 명령을 사용합니다. 명령 어카운팅에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa accounting command [privilege *level***]** *tacacs+-server-tag*

no aaa accounting command [privilege *level***]** *tacacs+-server-tag*

구문 설명

privilege *level*	**privilege** 명령을 사용하여 명령 권한 레벨을 사용자 지정할 경우, 최소 권한 레벨을 지정함으로써 ASA에서 어떤 명령을 어카운팅할지 제한할 수 있습니다. ASA는 최소 권한 레벨보다 낮은 명령에 대해서는 어카운팅을 수행하지 않습니다. **참고** **privilege** 키워드를 활성화한 상태에서 사용 중단된 명령을 입력하면 ASA에서는 그 명령에 대한 어카운팅 정보를 보내지 않습니다. 사용 중단된 명령에 대해 어카운팅하려는 경우 반드시 **privilege** 키워드를 비활성화하십시오. 사용 중단된 명령 중 상당수가 여전히 CLI에서 사용 가능하며 대개는 CLI에서 현재 허용되는 명령으로 변환됩니다. CLI 도움말 또는 이 설명서에는 포함되어 있지 않습니다.
tacacs+-server-tag	**aaa-server protocol** 명령으로 지정되는 대로 어카운팅 레코드가 보내지는 TACACS+ 서버 또는 서버 그룹을 지정합니다.

기본값

기본 권한 레벨은 0입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

aaa accounting command 명령을 구성할 때, 관리자가 입력한 **show** 명령을 제외한 각 명령이 기록되어 어카운팅 서버에 보내집니다.

예

다음 예에서는 지원되는 모든 명령에 대해 어카운팅 레코드가 생성되고 adminserver라는 이름의 그룹에서 서버에 이 레코드를 전송하도록 지정합니다.

```
ciscoasa(config)# aaa accounting command adminserver
```

관련 명령

명령	설명
aaa accounting	(**aaa-server** 명령으로 지정된 서버에서) TACACS+ 또는 RADIUS 사용자 어카운팅을 활성화하거나 비활성화합니다.
clear configure aaa	구성된 AAA 어카운팅 값을 제거하거나 재설정합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa accounting console

관리 액세스에 대해 AAA 어카운팅 지원을 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa accounting console** 명령을 사용합니다. 관리 액세스에 대해 AAA 어카운팅 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa accounting {serial | telnet | ssh | enable} console *server-tag*

no aaa accounting {serial | telnet | ssh | enable} console *server-tag*

구문 설명

enable	특별 권한 EXEC 모드를 시작하거나 종료하는 항목을 나타내기 위해 어카운팅 레코드의 생성을 활성화합니다.
serial	직렬 콘솔 인터페이스를 통해 이루어지는 관리 세션의 설정과 종료를 나타내기 위해 어카운팅 레코드의 생성을 활성화합니다.
server-tag	**aaa-server protocol** 명령으로 정의된 대로 어카운팅 레코드가 보내지는 서버 그룹을 지정합니다. 유효한 서버 그룹 프로토콜은 RADIUS와 TACACS+입니다.
ssh	SSH를 통해 생성된 관리 세션의 설정과 종료를 나타내기 위해 어카운팅 레코드의 생성을 활성화합니다.
telnet	텔넷을 통해 생성된 관리 세션의 설정과 종료를 나타내기 위해 어카운팅 레코드의 생성을 활성화합니다.

기본값

기본적으로 관리 액세스에 대한 AAA 어카운팅은 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이전에 **aaa-server** 명령에서 지정되었던 서버 그룹의 이름을 지정해야 합니다.

예

다음 예에서는 enable 액세스에 대해 어카운팅 레코드가 생성되고 adminserver라는 이름의 서버에 이 레코드를 전송하도록 지정합니다.

```
ciscoasa(config)# aaa accounting enable console adminserver
```

관련 명령

명령	설명
aaa accounting match	(**aaa-server** 명령으로 지정된 서버에서) TACACS+ 또는 RADIUS 사용자 어카운팅을 활성화하거나 비활성화합니다.
aaa accounting command	관리자/사용자가 입력한, 지정된 권한 레벨 이상의 각 명령을 기록하고 어카운팅 서버에 보내도록 지정합니다.
clear configure aaa	구성된 AAA 어카운팅 값을 제거하거나 재설정합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa accounting include, exclude

ASA를 통한 TCP 또는 UDP 연결에 대한 어카운팅을 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa accounting include** 명령을 사용합니다. 어카운팅에서 주소를 제외하려면 **aaa accounting exclude** 명령을 사용합니다. 어카운팅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

구문 설명

exclude	지정된 서비스 및 주소가 **include** 명령으로 이미 지정된 경우 이를 어카운팅에서 제외합니다.
include	어카운팅이 필요한 서비스 및 IP 주소를 지정합니다. **include** 문에서 지정되지 않은 트래픽은 처리되지 않습니다.
inside_ip	상위 보안 인터페이스의 IP 주소를 지정합니다. 이 주소는 이 명령을 적용하는 인터페이스에 따라 소스 주소 또는 수신 주소일 수 있습니다. 하위 보안 인터페이스에 명령을 적용할 경우 이 주소는 수신 주소입니다. 상위 보안 인터페이스에 명령을 적용할 경우 이 주소는 소스 주소입니다. 모든 호스트를 가리키려면 0을 사용합니다.
inside_mask	내부 IP 주소에 대한 네트워크 마스크를 지정합니다. IP 주소가 0이라면 0을 사용합니다. 호스트에는 255.255.255.255를 사용합니다.
interface_name	어떤 인터페이스 이름에서 사용자의 어카운팅이 필요한지 지정합니다.
outside_ip	(선택 사항) 하위 보안 인터페이스의 IP 주소를 지정합니다. 이 주소는 이 명령을 적용하는 인터페이스에 따라 소스 주소 또는 수신 주소일 수 있습니다. 하위 보안 인터페이스에 명령을 적용할 경우 이 주소는 소스 주소입니다. 상위 보안 인터페이스에 명령을 적용할 경우 이 주소는 수신 주소입니다. 모든 호스트를 가리키려면 0을 사용합니다.
outside_mask	(선택 사항) 외부 IP 주소에 대한 네트워크 마스크를 지정합니다. IP 주소가 0이라면 0을 사용합니다. 호스트에는 255.255.255.255를 사용합니다.
server_tag	**aaa-server host** 명령으로 정의된 AAA 서버 그룹을 지정합니다.
service	어카운팅이 필요한 서비스를 지정합니다. 다음 값 중 하나를 지정할 수 있습니다. • **any** 또는 **tcp/0**(모든 TCP 트래픽 지정) • **ftp** • **HTTP** • **https** • **ssh** • **telnet** • **tcp/***port* • **udp/***port*

기본값

기본적으로 관리 액세스에 대한 AAA 어카운팅은 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서는 ASA를 통과하는 어떤 TCP 또는 UDP 트래픽에 대한 어카운팅 정보도 RADIUS 또는 TACACS+ 서버에 보낼 수 있습니다. 또한 이 트래픽이 인증된 경우 AAA 서버는 사용자 이름을 기준으로 어카운팅 정보를 유지 관리할 수 있습니다. 트래픽이 인증되지 않은 경우 AAA 서버는 IP 주소를 기준으로 어카운팅 정보를 유지 관리할 수 있습니다. 어카운팅 정보에는 세션이 시작하고 중지한 시간, 사용자 이름, 해당 세션에서 ASA를 통과한 바이트 수, 사용된 서비스, 각 세션의 기간이 포함됩니다.

이 명령을 사용하려면 먼저 **aaa-server** 명령으로 AAA 서버를 지정해야 합니다.

ACL에 의해 지정된 트래픽에 대한 어카운팅을 활성화하려면 **aaa accounting match** 명령을 사용합니다. **match** 명령은 **include** 및 **exclude** 명령과 동일한 컨피그레이션에서 사용할 수 없습니다. **include** 및 **exclude** 명령 대신 **match** 명령을 사용하는 것이 좋습니다. **include** 및 **exclude** 명령은 ASDM에서 지원하지 않습니다.

동일한 보안 인터페이스 간에 **aaa accounting include** 명령과 **exclude** 명령을 사용할 수 없습니다. 그러한 경우에는 **aaa accounting match** 명령을 사용해야 합니다.

예

다음 예에서는 모든 TCP 연결에서 어카운팅을 활성화합니다.

```
ciscoasa(config)# aaa-server mygroup protocol tacacs+
ciscoasa(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

관련 명령

명령	설명
aaa accounting match	ACL에 의해 지정된 트래픽에 대한 어카운팅을 활성화합니다.
aaa accounting command	관리 액세스의 어카운팅을 활성화합니다.
aaa-server host	AAA 서버를 구성합니다.
clear configure aaa	AAA 컨피그레이션을 지웁니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa accounting match

ASA를 통한 TCP 또는 UDP 연결에 대한 어카운팅을 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa accounting match** 명령을 사용합니다. 트래픽에 대한 어카운팅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

구문 설명

acl_name	ACL 이름을 매칭하여 어카운팅해야 하는 트래픽을 지정합니다. ACL의 허용 항목은 어카운팅되지만, 거부 항목은 어카운팅에서 제외됩니다. 이 명령은 TCP 및 UDP 트래픽에 대해서만 지원됩니다. 이 명령을 입력했는데 다른 프로토콜을 허용하는 ACL을 참조할 경우 경고 메시지가 표시됩니다.
interface_name	어떤 인터페이스 이름에서 사용자의 어카운팅이 필요한지 지정합니다.
server_tag	**aaa-server** 명령으로 정의된 AAA 서버 그룹 태그를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서는 ASA를 통과하는 어떤 TCP 또는 UDP 트래픽에 대한 어카운팅 정보도 RADIUS 또는 TACACS+ 서버에 보낼 수 있습니다. 또한 이 트래픽이 인증된 경우 AAA 서버는 사용자 이름을 기준으로 어카운팅 정보를 유지 관리할 수 있습니다. 트래픽이 인증되지 않은 경우 AAA 서버는 IP 주소를 기준으로 어카운팅 정보를 유지 관리할 수 있습니다. 어카운팅 정보에는 세션이 시작하고 중지한 시간, 사용자 이름, 해당 세션에서 ASA를 통과한 바이트 수, 사용된 서비스, 각 세션의 기간이 포함됩니다.

이 명령을 사용하려면 먼저 **aaa-server** 명령으로 AAA 서버를 지정해야 합니다.

aaa-server 프로토콜 컨피그레이션 모드에서 **accounting-mode** 명령을 사용하여 동시 어카운팅을 활성화하지 않는 한 어카운팅 정보는 서버 그룹의 활성 서버에만 보내집니다.

aaa accounting match 명령은 **aaa accounting include** 및 **exclude** 명령과 동일한 컨피그레이션에서 사용할 수 없습니다. **include** 및 **exclude** 명령 대신 **match** 명령을 사용하는 것이 좋습니다. **include** 및 **exclude** 명령은 ASDM에서 지원하지 않습니다.

예

다음 예에서는 acl2라는 ACL과 매칭하는 트래픽에 대한 어카운팅을 활성화합니다.

```
ciscoasa(config)# access-list acl12 extended permit tcp any any
ciscoasa(config)# aaa accounting match acl2 outside radserver1
```

관련 명령

명령	설명
aaa accounting include, exclude	명령에서 직접 IP 주소를 지정하여 어카운팅을 활성화합니다.
access-list extended	ACL을 생성합니다.
clear configure aaa	AAA 컨피그레이션을 제거합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa authentication console

직렬, SSH, HTTPS(ASDM) 또는 텔넷 연결을 통해 ASA CLI에 액세스하는 사용자를 인증하거나 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스하는 사용자를 인증하려면 글로벌 컨피그레이션 모드에서 **aaa authentication console** 명령을 사용합니다. 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

no aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

구문 설명

enable	특별 권한 EXEC 모드에 액세스하는 사용자가 **enable** 명령을 사용할 때 이 사용자를 인증합니다.
HTTP	HTTPS를 통해 ASA에 액세스하는 ASDM 사용자를 인증합니다. RADIUS 또는 TACACS+ 서버를 사용하려는 경우에만 HTTPS 인증을 구성하면 됩니다. 이 명령을 구성하지 않더라도 기본적으로 ASDM에서는 인증에 로컬 데이터베이스를 사용합니다.

LOCAL	인증에 로컬 데이터베이스를 사용합니다. **LOCAL** 키워드는 대/소문자를 구분합니다. 로컬 데이터베이스가 비어 있는 경우 다음 경고 메시지가 나타납니다.
	`Warning:local database is empty! Use 'username' command to define local users.`
	
	LOCAL 키워드가 컨피그레이션에 남아 있는 상태에서 로컬 데이터베이스가 비워질 경우 다음 경고 메시지가 나타납니다.
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	**aaa-server** 명령으로 정의된 AAA 서버 그룹 태그를 지정합니다. HTTPS 관리 인증에서는 AAA 서버 그룹에 대해 SDI 프로토콜을 지원하지 않습니다. **LOCAL** 키워드를 *server-tag* 인수에 추가하여 사용할 경우, AAA 서버가 사용 불가능할 때 대체 방법으로 로컬 데이터베이스를 사용하게끔 ASA를 구성할 수 있습니다. **LOCAL** 키워드는 대/소문자를 구분합니다. 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다.
serial	직렬 콘솔 포트를 사용하여 ASA에 액세스하는 사용자를 인증합니다.
ssh	SSH를 사용하여 ASA에 액세스하는 사용자를 인증합니다.
telnet	텔넷을 사용하여 ASA에 액세스하는 사용자를 인증합니다.

기본값

기본적으로 로컬 데이터베이스를 사용하는 대체 방법은 비활성화되어 있습니다.

aaa authentication telnet console 명령이 정의되지 않은 경우 ASA 로그인 비밀번호(**password** 명령으로 설정)를 사용하여 ASA CLI에 대한 액세스 권한을 얻을 수 있습니다.

aaa authentication http console 명령이 정의되지 않은 경우, 사용자 이름 및 ASA enable 비밀번호(**enable password** 명령으로 설정) 없이 (ASDM을 통해) ASA에 대한 액세스 권한을 얻을 수 있습니다. **aaa** 명령이 정의되었지만 HTTPS 인증에서 시간 초과를 요청할 경우(AAA 서버가 중단되었거나 사용 불가능한 상태일 가능성이 있음), 기본 관리자 사용자 이름과 enable 비밀번호를 사용하여 ASA에 대한 액세스 권한을 얻을 수 있습니다. 기본적으로 enable 비밀번호는 설정되어 있지 않습니다.

aaa authentication ssh console 명령이 정의되지 않은 경우, 사용자 이름 **pix**와 ASA enable 비밀번호(**enable password** 명령으로 설정)를 사용하여 ASA CLI에 대한 액세스 권한을 얻을 수 있습니다. 기본적으로 enable 비밀번호는 비어 있습니다. 이는 AAA가 구성되지 않은 상태에서 ASA에 로그인할 때와 다릅니다. 그 경우에는 로그인 비밀번호(**password** 명령으로 설정)를 사용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서 텔넷 또는 SSH 사용자를 인증하려면 먼저 **telnet** 또는 **ssh** 명령을 사용하여 ASA에 대한 액세스를 구성해야 합니다. 이 명령은 ASA와 통신할 수 있는 IP 주소를 식별합니다.

ASA 로그인

ASA에 연결한 다음 로그인하고 사용자 EXEC 모드에 액세스합니다.

- 텔넷에 대한 어떤 인증도 활성화하지 않을 경우 사용자 이름을 입력하지 않습니다. 로그인 비밀번호(**password** 명령으로 설정)를 입력합니다. SSH의 경우 사용자 이름으로 "pix"를 입력하고 로그인 비밀번호를 입력합니다.
- 이 명령을 사용하여 텔넷 또는 SSH 인증을 활성화할 경우, AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다.

특별 권한 EXEC 모드 액세스

특별 권한 EXEC 모드를 시작하려면 **enable** 명령 또는 **login** 명령(로컬 데이터베이스만 사용 중인 경우)을 입력합니다.

- enable 인증을 구성하지 않을 경우 **enable** 명령을 입력할 때 시스템 enable 비밀번호(**enable password** 명령으로 설정)를 입력합니다. 그러나 enable 인증을 사용하지 않을 경우, **enable** 명령을 입력하면 더 이상 특정 사용자로 로그인한 상태가 아닙니다. 사용자 이름을 유지하려면 enable 인증을 사용합니다.
- enable 인증을 구성할 경우 ASA에서는 사용자 이름과 비밀번호를 묻습니다.

로컬 데이터베이스를 사용하는 인증의 경우 **login** 명령을 사용할 수 있습니다. 이 명령은 사용자 이름을 유지하지만 인증을 실행하는 데 어떤 컨피그레이션도 필요하지 않습니다.

ASDM 액세스

기본적으로 빈 사용자 이름과 **enable password** 명령을 통해 설정된 enable 비밀번호를 사용하여 ASDM에 로그인할 수 있습니다. 그러나 로그인 화면에서 (사용자 이름을 비워 두지 않고) 사용자 이름과 비밀번호를 입력한 경우 ASDM은 로컬 데이터베이스에 일치하는 항목이 있는지 확인합니다.

이 명령을 사용하여 HTTPS 인증을 구성하고 로컬 데이터베이스를 지정할 수 있지만, 기본적으로 이 기능은 항상 활성화되어 있습니다. 인증에 AAA 서버를 사용하려는 경우에만 HTTPS 인증을 구성합니다. HTTPS 관리 인증은 AAA 서버 그룹을 위해 SDI 프로토콜을 지원하지 않습니다. HTTPS 인증을 위해 입력할 수 있는 사용자 이름은 최대 30자입니다. 비밀번호는 최대 16자입니다.

시스템 실행 영역에서 AAA 명령 지원 안 함

다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 어떤 AAA 명령도 구성할 수 없습니다.

허용되는 로그인 시도 횟수

다음 표에서처럼, ASA CLI에 대한 인증된 액세스의 프롬프트 동작은 **aaa authentication console** 명령으로 선택하는 옵션에 따라 달라집니다.

옵션	허용되는 로그인 시도 횟수
enable	3번 시도 후 액세스 거부
serial	성공할 때까지 계속
ssh	3번 시도 후 액세스 거부
telnet	성공할 때까지 계속
HTTP	성공할 때까지 계속

사용자 CLI 및 ASDM 액세스 제한

aaa authorization exec 명령을 사용하여 관리 권한 부여를 구성함으로써 로컬 사용자, RADIUS, TACACS+ 또는 (LDAP 특성을 RADIUS 특성에 매핑한 경우) LDAP 사용자가 CLI, ASDM 또는 **enable** 명령에 액세스하는 것을 제한할 수 있습니다.

참고 직렬 액세스는 관리 권한 부여에 포함되지 않습니다. 따라서 **aaa authentication serial console**을 구성할 경우 인증하는 어떤 사용자도 콘솔 포트에 액세스할 수 있습니다.

관리 권한 부여를 위해 사용자를 구성하려면 각 AAA 서버 유형 또는 로컬 사용자에 대한 다음 요구 사항을 확인하십시오.

- RADIUS 또는 LDAP (매핑된) 사용자—Service-Type 특성을 다음 값 중 하나로 구성합니다. (LDAP 특성의 매핑에 대해서는 **ldap attribute-map** 명령 참조)
  - Service-Type 6 (Administrative)—**aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.
  - Service-Type 7 (NAS prompt)—**aaa authentication {telnet | ssh} console** 명령을 구성할 때 CLI에 대한 액세스를 허용하지만, **aaa authentication http console** 명령을 구성할 경우에는 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **aaa authentication enable console** 명령으로 **enable** 인증을 구성할 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다.
  - Service-Type 5 (Outbound)—관리 액세스를 거부합니다. 사용자는 **aaa authentication console** 명령으로 지정된 어떤 서비스도 사용할 수 없습니다(**serial** 키워드 제외, 직렬 액세스는 허용). 원격 액세스(IPSec 및 SSL) 사용자는 원격 액세스 세션을 계속 인증하고 종료할 수 있습니다.

- TACACS+ 사용자—"service=shell"로 권한 부여가 요청되고 서버는 PASS 또는 FAIL로 응답합니다.
  - PASS, 권한 레벨 1—**aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.
  - PASS, 권한 레벨 2 이상—**aaa authentication {telnet | ssh} console** 명령을 구성할 때 CLI에 대한 액세스를 허용하지만, **aaa authentication http console** 명령을 구성할 경우 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **aaa authentication enable console** 명령으로 enable 인증을 구성할 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다.
  - FAIL—관리 액세스를 거부합니다. 사용자는 **aaa authentication console** 명령으로 지정된 어떤 서비스도 사용할 수 없습니다(**serial** 키워드 제외, 직렬 액세스는 허용).
- 로컬 사용자—**service-type** 명령을 설정합니다. 기본적으로 **service-type**은 **admin**이며, 이는 **aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.

예

다음 예에서는 서버 태그가 "radius"인 RADIUS 서버와의 텔넷 연결을 위해 **aaa authentication console** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# aaa authentication telnet console radius
```

다음 예에서는 enable 인증을 위해 서버 그룹 "AuthIn"을 식별합니다.

```
ciscoasa(config)# aaa authentication enable console AuthIn
```

다음 예에서는 "svrgrp1" 그룹의 모든 서버에서 오류가 발생할 경우 LOCAL 사용자 데이터베이스를 대신 사용하도록 지정하는 데 **aaa authentication console** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs
ciscoasa(config)# aaa authentication ssh console svrgrp1 LOCAL
```

관련 명령

명령	설명
aaa authentication	사용자 인증을 활성화하거나 비활성화합니다.
aaa-server host	사용자 인증에 사용할 AAA 서버를 지정합니다.
clear configure aaa	구성된 AAA 어카운팅 값을 제거하거나 재설정합니다.
ldap map-attributes	LDAP 특성을 ASA에서 이해할 수 있는 RADIUS 특성에 매핑합니다.
service-type	로컬 사용자 CLI 액세스를 제한합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa authentication include, exclude

ASA를 통한 연결에 대한 인증을 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa authentication include** 명령을 사용합니다. 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 인증에서 주소를 제외하려면 **aaa authentication exclude** 명령을 사용합니다. 인증에서 주소를 제외하지 않으려면 이 명령의 **no** 형식을 사용합니다.

aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* **[***outside_ip outside_mask***] {***server_tag* **| LOCAL}**

no aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* **| LOCAL}**

구문 설명

exclude	지정된 서비스 및 주소가 **include** 명령으로 이미 지정된 경우 이를 인증에서 제외합니다.
include	인증이 필요한 서비스 및 IP 주소를 지정합니다. **include** 문에서 지정되지 않은 트래픽은 처리되지 않습니다.
inside_ip	상위 보안 인터페이스의 IP 주소를 지정합니다. 이 주소는 이 명령을 적용하는 인터페이스에 따라 소스 주소 또는 수신 주소일 수 있습니다. 하위 보안 인터페이스에 명령을 적용할 경우 이 주소는 수신 주소입니다. 상위 보안 인터페이스에 명령을 적용할 경우 이 주소는 소스 주소입니다. 모든 호스트를 가리키려면 0을 사용합니다.
inside_mask	내부 IP 주소에 대한 네트워크 마스크를 지정합니다. IP 주소가 0이라면 0을 사용합니다. 호스트에는 255.255.255.255를 사용합니다.
interface_name	어떤 인터페이스 이름에서 사용자 인증이 필요한지 지정합니다.
LOCAL	로컬 사용자 데이터베이스를 지정합니다.
outside_ip	(선택 사항) 하위 보안 인터페이스의 IP 주소를 지정합니다. 이 주소는 이 명령을 적용하는 인터페이스에 따라 소스 주소 또는 수신 주소일 수 있습니다. 하위 보안 인터페이스에 명령을 적용할 경우 이 주소는 소스 주소입니다. 상위 보안 인터페이스에 명령을 적용할 경우 이 주소는 수신 주소입니다. 모든 호스트를 가리키려면 0을 사용합니다.
outside_mask	(선택 사항) 외부 IP 주소에 대한 네트워크 마스크를 지정합니다. IP 주소가 0이라면 0을 사용합니다. 호스트에는 255.255.255.255를 사용합니다.

server_tag	**aaa-server** 명령으로 정의된 AAA 서버 그룹을 지정합니다.
service	인증이 필요한 서비스를 지정합니다. 다음 값 중 하나를 지정할 수 있습니다. • **any** 또는 **tcp/0**(모든 TCP 트래픽 지정) • **ftp** • **HTTP** • **https** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] 임의의 프로토콜 또는 서비스에 대한 네트워크 액세스에 인증을 요구하도록 ASA를 구성할 수 있으나, 사용자는 HTTP, HTTPS, 텔넷 또는 FTP를 통해서만 직접 인증할 수 있습니다. ASA에서 인증을 필요로 하는 다른 트래픽을 허용하기 전에 사용자가 먼저 이 서비스 중 하나로 인증해야 합니다. 자세한 내용은 "사용 지침" 섹션을 참조하십시오.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ACL로 지정된 트래픽에 대한 인증을 활성화하려면 **aaa authentication match** 명령을 사용합니다. **match** 명령은 **include** 및 **exclude** 명령과 동일한 컨피그레이션에서 사용할 수 없습니다. **include** 및 **exclude** 명령 대신 **match** 명령을 사용하는 것이 좋습니다. **include** 및 **exclude** 명령은 ASDM에서 지원하지 않습니다.

동일한 보안 인터페이스 간에 **aaa authentication include** 명령과 **exclude** 명령을 사용할 수 없습니다. 그러한 경우에는 **aaa authentication match** 명령을 사용해야 합니다.

시퀀스 임의 지정을 비활성화하더라도 TCP 세션이 임의의 시퀀스 번호를 가질 수 있습니다. 이는 액세스를 허용하기 전에 사용자를 인증하기 위해 AAA 서버가 TCP 세션을 프록시할 때 일어납니다.

일회성 인증

지정된 IP 주소의 사용자는 인증 세션이 만료될 때까지 모든 규칙 및 유형에 대해 한 번만 인증을 수행하면 됩니다. (시간 초과 값에 대해서는 **timeout uauth** 명령 참조) 예를 들어, ASA에서 텔넷 및 FTP를 인증하도록 구성한 가운데 사용자가 처음으로 텔넷 인증에 성공할 경우, 인증 세션이 지속되는 한 사용자는 FTP로도 인증할 필요 없습니다.

HTTP 또는 HTTPS 인증에서는 일단 인증이 이루어지면 **timeout uauth** 명령이 얼마나 오랫동안 설정되었는지 상관없이 사용자가 재인증할 필요가 없습니다. 해당 사이트와 다시 연결할 때마다 브라우저에서 "Basic=Uuhjksdkfhk==" 문자열을 캐시에 저장하기 때문입니다. 이는 사용자가 웹 브라우저의 *모든* 인스턴스를 종료하고 재시작하는 경우에만 지워집니다. 캐시를 비우는 것은 아무 소용 없습니다.

인증 질문을 받아야 하는 애플리케이션

임의의 프로토콜 또는 서비스에 대한 네트워크 액세스에 인증을 요구하도록 ASA를 구성할 수 있으나, 사용자는 HTTP, HTTPS, 텔넷 또는 FTP를 통해서만 직접 인증할 수 있습니다. ASA에서 인증을 필요로 하는 다른 트래픽을 허용하기 전에 사용자가 먼저 이 서비스 중 하나로 인증해야 합니다.

ASA에서 AAA에 지원하는 인증 포트는 고정되어 있습니다.

- FTP는 포트 21
- 텔넷은 포트 23
- HTTP는 포트 80
- HTTPS는 포트 443

ASA 인증 프롬프트

텔넷과 FTP의 경우 ASA에서 인증 프롬프트를 생성합니다.

HTTP는 ASA에서 기본 HTTP 인증을 기본적으로 사용하며 인증 프롬프트를 제공합니다. 원하는 경우 ASA에서 사용자 이름과 비밀번호(**aaa authentication listener** 명령으로 구성)를 입력하는 내부 웹 페이지로 사용자를 리디렉션하도록 구성할 수 있습니다.

HTTPS의 경우 ASA에서 사용자 지정 로그인 화면을 생성합니다. 원하는 경우 ASA에서 사용자 이름과 비밀번호(**aaa authentication listener** 명령으로 구성)를 입력하는 내부 웹 페이지로 사용자를 리디렉션하도록 구성할 수 있습니다.

리디렉션은 기본 방식보다 우수한 기능입니다. 인증 시 더 나은 사용자 경험을 제공하고 Easy VPN 및 방화벽 모드 모두에서 HTTP와 HTTPS에 동일한 사용자 경험을 선사하기 때문입니다. ASA와의 직접 인증도 지원합니다.

ASA에서 수신 포트를 여는 것을 원치 않을 경우, 라우터에서 NAT를 사용하는데 ASA에서 서비스하는 웹 페이지에 대해 변환 규칙을 생성하지 않으려는 경우, 해당 네트워크에서 기본 HTTP 인증이 더 효과적일 경우에는 기본 HTTP 인증을 계속 사용할 수도 있습니다. 예를 들어, URL이 이메일에 임베드된 경우처럼 브라우저 기반이 아닌 애플리케이션은 기본 인증과의 호환성이 더 우수할 수 있습니다.

올바르게 인증하면 ASA는 원래의 목적지로 리디렉션합니다. 목적지 서버에서도 자체적으로 인증을 수행할 경우 사용자는 또 다른 사용자 이름과 비밀번호를 입력합니다. 기본 HTTP 인증을 사용하는 데 목적지 서버에서 다른 사용자 이름과 비밀번호를 입력해야 할 경우 **virtual http** 명령을 구성해야 합니다.

참고 **aaa authentication secure-http-client** 명령을 사용하지 않고 HTTP 인증을 사용할 경우 사용자 이름과 비밀번호가 일반 텍스트 형식으로 클라이언트에서 ASA에 보내집니다. HTTP 인증을 활성화할 때마다 **aaa authentication secure-http-client** 명령을 사용하는 것이 좋습니다.

FTP의 경우 사용자는 ASA 사용자 이름, @ 기호, FTP 사용자 이름을 차례로 입력할 수 있습니다(예: name1@name2). 비밀번호에는 ASA 비밀번호, @ 기호, FTP 비밀번호를 차례로 입력합니다(예: password1@password2). 이를테면 다음과 같이 입력합니다.

```
name> asa1@partreq
password> letmein@he110
```

이 기능은 다중 로그인이 필요한 방화벽을 중첩한 경우에 유용합니다. 여러 이름과 비밀번호는 @ 기호를 여러 번 사용하여 구분할 수 있습니다.

허용되는 로그인 시도 횟수는 지원되는 프로토콜에 따라 달라집니다.

프로토콜	허용되는 로그인 시도 횟수
FTP	잘못된 비밀번호를 입력하면 즉시 연결이 끊깁니다.
HTTP HTTPS	로그인에 성공할 때까지 계속 프롬프트를 다시 표시합니다.
텔넷	4번 시도한 다음 연결이 끊깁니다.

고정 PAT 와 HTTP

HTTP 인증에서 ASA는 고정 PAT가 구성된 경우 실제 포트를 확인합니다. 실제 포트 80이 목적지인 트래픽을 감지할 경우, 매핑된 포트와 상관없이 ASA는 HTTP 연결을 인터셉트하고 강제적으로 인증을 수행합니다.

예를 들어, 외부 TCP 포트 889가 포트 80(www)으로 변환되었고 모든 관련 ACL에서 트래픽을 허용한다고 가정하면,

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

사용자가 포트 889에서 10.48.66.155에 대한 액세스를 시도하면 ASA는 트래픽을 인터셉트하고 강제적으로 HTTP 인증을 수행합니다. 사용자의 웹 브라우저에 HTTP 인증 페이지가 표시된 후에야 ASA에서 HTTP 연결을 완료할 수 있습니다.

다음 예와 같이 로컬 포트가 포트 80이 아닐 경우

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

사용자에게 인증 페이지가 표시되지 않습니다. 그 대신 ASA에서 웹 브라우저에 오류 메시지를 보내 사용자가 요청한 서비스를 이용하려면 인증받아야 함을 알립니다.

ASA 직접 인증

HTTP, HTTPS, 텔넷 또는 FTP가 ASA를 거치는 것을 원치 않지만 다른 트래픽 유형은 인증하려는 경우, **aaa authentication listener** 명령을 구성하여 HTTP 또는 HTTPS로 ASA와 직접 인증할 수 있습니다.

인터페이스에 대해 AAA를 활성화하면 다음 URL에서 ASA와 직접 인증할 수 있습니다.

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

또는 (**virtual telnet** 명령을 사용하여) 가상 텔넷을 구성할 수 있습니다. 가상 텔넷에서는 사용자가 ASA에 구성된 IP 주소에 텔넷 연결하며 ASA에서 텔넷 프롬프트를 제공합니다.

예

다음 예에서는 외부 인터페이스의 인증 TCP 트래픽을 포함합니다. 내부 IP 주소는 192.168.0.0, 넷마스크는 255.255.0.0이고 모든 호스트의 단일 외부 IP 주소, tacacs+라는 이름의 서버 그룹을 사용합니다. 두 번째 명령행에서는 외부 인터페이스의 텔넷 트래픽을 제외합니다. 내부 주소는 192.168.38.0이고 모든 호스트의 단일 외부 IP 주소를 사용합니다.

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
ciscoasa(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

다음 예는 *interface-name* 매개변수를 사용하는 방법을 보여줍니다. ASA는 내부 네트워크 192.168.1.0, 외부 네트워크 209.165.201.0(서브넷 마스크 255.255.255.224), 경계 네트워크 209.165.202.128(서브넷 마스크 255.255.255.224)이 있습니다.

이 예에서는 소스가 내부 네트워크, 목적지가 외부 네트워크인 연결에 대한 인증을 활성화합니다.

```
ciscoasa(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

이 예에서는 소스가 내부 네트워크, 목적지가 경계 네트워크인 연결에 대한 인증을 활성화합니다.

```
ciscoasa(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

이 예에서는 소스가 외부 네트워크, 목적지가 내부 네트워크인 연결에 대한 인증을 활성화합니다.

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

이 예에서는 소스가 외부 네트워크, 목적지가 경계 네트워크인 연결에 대한 인증을 활성화합니다.

```
ciscoasa(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

이 예에서는 소스가 경계 네트워크, 목적지가 외부 네트워크인 연결에 대한 인증을 활성화합니다.

```
ciscoasa(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

관련 명령

명령	설명
aaa authentication console	관리 액세스를 위한 인증을 활성화합니다.
aaa authentication match	통과 트래픽에 대한 사용자 인증을 활성화합니다.
aaa authentication secure-http-client	HTTP 요청의 ASA 통과를 허용하기 전에 ASA에 대한 사용자 인증을 안전하게 수행할 방법을 제공합니다.
aaa-server	그룹 기반 서버 특성을 구성합니다.
aaa-server host	호스트 관련 특성을 구성합니다.

aaa authentication listener

네트워크 사용자 인증을 위해 HTTP(S) 수신 포트를 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa authentication listener** 명령을 사용합니다. 수신 포트를 활성화할 때 ASA는 직접 연결을 위해 그리고 선택적으로 통과 트래픽을 위해 인증 페이지를 서비스합니다. 리스너를 비활성화하려면 이 명령의 **no** 형태를 사용합니다.

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

구문 설명

http[**s**]	수신할 프로토콜을 HTTP 또는 HTTPS로 지정합니다. 각 프로토콜에 개별적으로 이 명령을 입력합니다.
interface_name	리스너를 활성화하는 인터페이스를 지정합니다.
port *portnum*	ASA에서 직접 트래픽 또는 리디렉션된 트래픽을 위해 수신하는 포트 번호를 지정합니다. 기본값은 80(HTTP), 443(HTTPS)입니다. 임의의 포트 번호를 사용해도 기능은 동일하지만, 직접 인증 사용자가 포트 번호를 알고 있어야 합니다. 리디렉션된 트래픽은 자동으로 정확한 포트 번호에 보내지지만, 직접 인증자는 수동으로 포트 번호를 지정해야 합니다.
redirect	ASA에서 서비스하는 인증 웹 페이지에 통과 트래픽을 리디렉션합니다. 이 키워드가 없으면 ASA 인터페이스에 전송되는 트래픽만 인증 웹 페이지에 액세스할 수 있습니다.

기본값

기본적으로 어떤 리스너 서비스도 활성화되지 않으며 HTTP 연결은 기본 HTTP 인증을 사용합니다. 리스너를 활성화할 경우 기본 포트는 80(HTTP), 443(HTTPS)입니다.

7.2(1)에서 업그레이드하는 경우 포트 1080(HTTP) 및 1443(HTTPS)에서 리스너가 활성화됩니다. **redirect** 옵션도 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(2)	이 명령을 도입했습니다.

사용 지침

aaa authentication listener 명령을 사용하지 않을 경우, **aaa authentication match** 또는 **aaa authentication include** 명령을 구성한 다음 HTTP(S) 사용자가 ASA와 인증해야 할 때 ASA에서는 기본 HTTP 인증을 사용합니다. HTTPS의 경우 ASA에서 사용자 지정 로그인 화면을 생성합니다.

aaa authentication listener 명령을 **redirect** 키워드와 함께 구성할 경우 ASA는 모든 HTTP(S) 인증 요청을 ASA에서 서비스하는 웹 페이지에 리디렉션합니다.

리디렉션은 기본 방식보다 우수한 기능입니다. 인증 시 더 나은 사용자 경험을 제공하고 Easy VPN 및 방화벽 모드 모두에서 HTTP와 HTTPS에 동일한 사용자 경험을 선사하기 때문입니다. ASA와의 직접 인증도 지원합니다.

ASA에서 수신 포트를 여는 것을 원치 않을 경우, 라우터에서 NAT를 사용하는데 ASA에서 서비스하는 웹 페이지에 대해 변환 규칙을 생성하지 않으려는 경우, 해당 네트워크에서 기본 HTTP 인증이 더 효과적일 경우에는 기본 HTTP 인증을 계속 사용할 수도 있습니다. 예를 들어, URL이 이메일에 임베드된 경우처럼 브라우저 기반이 아닌 애플리케이션은 기본 인증과의 호환성이 더 우수할 수 있습니다.

aaa authentication listener 명령을 **redirect** 옵션 *없이* 입력할 경우, ASA와의 직접 인증만 활성화되며 통과 트래픽에서는 기본 HTTP 인증을 사용하게 됩니다. **redirect** 옵션은 직접 인증과 통과 트래픽 인증을 모두 활성화합니다. 직접 인증은 인증 질문을 지원하지 않는 트래픽 유형을 인증해야 할 때 유용합니다. 다른 서비스를 사용하기 전에 각 사용자가 ASA와 직접 인증하게 할 수 있습니다.

참고 **redirect** 옵션을 활성화할 경우 인터페이스 IP 주소를 변환하는 인터페이스 및 리스너에 사용되는 포트에 대해 고정 PAT 도 구성할 수 없습니다 . NAT 는 성공하지만 인증에 실패합니다 . 예를 들어 , 다음 컨피그레이션은 지원되지 않습니다 .

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside redirect
```

다음 컨피그레이션은 지원됩니다. 리스너가 기본 포트인 80 대신 1080을 사용합니다.

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside port 1080 redirect
```

예

다음 예에서는 ASA에서 HTTP 및 HTTPS 연결을 기본 포트에 리디렉션하도록 구성합니다.

```
ciscoasa(config)# aaa authentication http redirect
ciscoasa(config)# aaa authentication https redirect
```

다음 예에서는 인증 요청이 ASA에 직접 전달되는 것을 허용합니다. 통과 트래픽에서는 기본 HTTP 인증을 사용합니다.

```
ciscoasa(config)# aaa authentication http
ciscoasa(config)# aaa authentication https
```

다음 예에서는 ASA에서 HTTP 및 HTTPS 연결을 기본 포트가 아닌 포트에 리디렉션하도록 구성합니다.

```
ciscoasa(config)# aaa authentication http port 1100 redirect
ciscoasa(config)# aaa authentication https port 1400 redirect
```

관련 명령

명령	설명
aaa authentication match	통과 트래픽에 대한 사용자 인증을 구성합니다.
aaa authentication secure-http-client	SSL을 활성화하고 HTTP 클라이언트와 ASA 간의 사용자 이름 및 비밀번호 교환을 보호합니다.
clear configure aaa	구성된 AAA 컨피그레이션을 제거합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.
virtual http	기본 HTTP 인증으로 캐스케이딩 HTTP 인증을 지원합니다.

aaa authentication match

ASA를 통한 연결에 대한 인증을 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa authentication match** 명령을 사용합니다. 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

구문 설명

acl_name	확장된 ACL 이름을 지정합니다.
interface_name	어떤 인터페이스 이름에서 사용자를 인증할지 지정합니다.
LOCAL	로컬 사용자 데이터베이스를 지정합니다.
server_tag	**aaa-server** 명령으로 정의된 AAA 서버 그룹 태그를 지정합니다.
user-identity	ID 방화벽에 매핑되는 사용자 ID를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	**user-identity** 키워드가 추가되었습니다.

사용 지침

aaa authentication match 명령은 **include** 및 **exclude** 명령과 동일한 컨피그레이션에서 사용할 수 없습니다. **include** 및 **exclude** 명령 대신 **match** 명령을 사용하는 것이 좋습니다. **include** 및 **exclude** 명령은 ASDM에서 지원하지 않습니다.

시퀀스 임의 지정을 비활성화하더라도 TCP 세션이 임의의 시퀀스 번호를 가질 수 있습니다. 이는 액세스를 허용하기 전에 사용자를 인증하기 위해 AAA 서버가 TCP 세션을 프록시할 때 일어납니다.

일회성 인증

지정된 IP 주소의 사용자는 인증 세션이 만료될 때까지 모든 규칙 및 유형에 대해 한 번만 인증을 수행하면 됩니다. (시간 초과 값에 대해서는 **timeout uauth** 명령 참조) 예를 들어, ASA에서 텔넷 및 FTP를 인증하도록 구성한 가운데 사용자가 처음으로 텔넷 인증에 성공할 경우, 인증 세션이 지속되는 한 사용자는 FTP로도 인증할 필요 없습니다.

HTTP 또는 HTTPS 인증에서는 일단 인증이 이루어지면 **timeout uauth** 명령이 얼마나 오랫동안 설정되었는지 상관없이 사용자가 재인증할 필요가 없습니다. 해당 사이트와 다시 연결할 때마다 브라우저에서 "Basic=Uuhjksdkfhk==" 문자열을 캐시에 저장하기 때문입니다. 이는 사용자가 웹 브라우저의 *모든* 인스턴스를 종료하고 재시작하는 경우에만 지워집니다. 캐시를 비우는 것은 아무 소용 없습니다.

인증 질문을 받아야 하는 애플리케이션

임의의 프로토콜 또는 서비스에 대한 네트워크 액세스에 인증을 요구하도록 ASA를 구성할 수 있으나, 사용자는 HTTP, HTTPS, 텔넷 또는 FTP를 통해서만 직접 인증할 수 있습니다. ASA에서 인증을 필요로 하는 다른 트래픽을 허용하기 전에 사용자가 먼저 이 서비스 중 하나로 인증해야 합니다.

ASA에서 AAA에 지원하는 인증 포트는 고정되어 있습니다.

- FTP는 포트 21
- 텔넷은 포트 23
- HTTP는 포트 80
- HTTPS는 포트 443(**aaa authentication listener** 명령 필요)

ASA 인증 프롬프트

텔넷과 FTP의 경우 ASA에서 인증 프롬프트를 생성합니다.

HTTP는 ASA에서 기본 HTTP 인증을 기본적으로 사용하며 인증 프롬프트를 제공합니다. 원하는 경우 ASA에서 사용자 이름과 비밀번호(**aaa authentication listener** 명령으로 구성)를 입력하는 내부 웹 페이지로 사용자를 리디렉션하도록 구성할 수 있습니다.

HTTPS의 경우 ASA에서 사용자 지정 로그인 화면을 생성합니다. 원하는 경우 ASA에서 사용자 이름과 비밀번호(**aaa authentication listener** 명령으로 구성)를 입력하는 내부 웹 페이지로 사용자를 리디렉션하도록 구성할 수 있습니다.

리디렉션은 기본 방식보다 우수한 기능입니다. 인증 시 더 나은 사용자 경험을 제공하고 Easy VPN 및 방화벽 모드 모두에서 HTTP와 HTTPS에 동일한 사용자 경험을 선사하기 때문입니다. ASA와의 직접 인증도 지원합니다.

ASA에서 수신 포트를 여는 것을 원치 않을 경우, 라우터에서 NAT를 사용하는데 ASA에서 서비스하는 웹 페이지에 대해 변환 규칙을 생성하지 않으려는 경우, 해당 네트워크에서 기본 HTTP 인증이 더 효과적일 경우에는 기본 HTTP 인증을 계속 사용할 수도 있습니다. 예를 들어, URL이 이메일에 임베드된 경우처럼 브라우저 기반이 아닌 애플리케이션은 기본 인증과의 호환성이 더 우수할 수 있습니다.

올바르게 인증하면 ASA는 원래의 목적지로 리디렉션합니다. 목적지 서버에서도 자체적으로 인증을 수행할 경우 사용자는 또 다른 사용자 이름과 비밀번호를 입력합니다. 기본 HTTP 인증을 사용하는 데 목적지 서버에서 다른 사용자 이름과 비밀번호를 입력해야 할 경우 **virtual http** 명령을 구성해야 합니다.

참고 **aaa authentication secure-http-client** 명령을 사용하지 않고 HTTP 인증을 사용할 경우 사용자 이름과 비밀번호가 일반 텍스트 형식으로 클라이언트에서 ASA에 보내집니다. HTTP 인증을 활성화할 때마다 **aaa authentication secure-http-client** 명령을 사용하는 것이 좋습니다.

FTP의 경우 사용자는 ASA 사용자 이름, @ 기호, FTP 사용자 이름을 차례로 입력할 수 있습니다(예: name1@name2). 비밀번호에는 ASA 비밀번호, @ 기호, FTP 비밀번호를 차례로 입력합니다(예: password1@password2). 이를테면 다음과 같이 입력합니다.

```
name> asa1@partreq
password> letmein@he110
```

이 기능은 다중 로그인이 필요한 방화벽을 중첩한 경우에 유용합니다. 여러 이름과 비밀번호는 @ 기호를 여러 번 사용하여 구분할 수 있습니다.

허용되는 로그인 시도 횟수는 지원되는 프로토콜에 따라 달라집니다.

프로토콜	허용되는 로그인 시도 횟수
FTP	잘못된 비밀번호를 입력하면 즉시 연결이 끊깁니다.
HTTP HTTPS	로그인에 성공할 때까지 계속 프롬프트를 다시 표시합니다.
텔넷	4번 시도한 다음 연결이 끊깁니다.

고정 PAT 와 HTTP

HTTP 인증에서 ASA는 고정 PAT가 구성된 경우 실제 포트를 확인합니다. 실제 포트 80이 목적지인 트래픽을 감지할 경우, 매핑된 포트와 상관없이 ASA는 HTTP 연결을 인터셉트하고 강제적으로 인증을 수행합니다.

예를 들어, 외부 TCP 포트 889가 포트 80(www)으로 변환되었고 모든 관련 ACL에서 트래픽을 허용한다고 가정하면,

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

사용자가 포트 889에서 10.48.66.155에 대한 액세스를 시도하면 ASA는 트래픽을 인터셉트하고 강제적으로 HTTP 인증을 수행합니다. 사용자의 웹 브라우저에 HTTP 인증 페이지가 표시된 후에야 ASA에서 HTTP 연결을 완료할 수 있습니다.

다음 예와 같이 로컬 포트가 포트 80이 아닐 경우

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

사용자에게 인증 페이지가 표시되지 않습니다. 그 대신 ASA에서 웹 브라우저에 오류 메시지를 보내 사용자가 요청한 서비스를 이용하려면 인증받아야 함을 알립니다.

ASA 직접 인증

HTTP, HTTPS, 텔넷 또는 FTP가 ASA를 거치는 것을 원치 않지만 다른 트래픽 유형은 인증하려는 경우, **aaa authentication listener** 명령을 구성하여 HTTP 또는 HTTPS로 ASA와 직접 인증할 수 있습니다.

인터페이스에 대해 AAA를 활성화하면 다음 URL에서 ASA와 직접 인증할 수 있습니다.

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

또는 (**virtual telnet** 명령을 사용하여) 가상 텔넷을 구성할 수 있습니다. 가상 텔넷에서는 사용자가 ASA에 구성된 IP 주소에 텔넷 연결하며 ASA에서 텔넷 프롬프트를 제공합니다.

예

다음 예제 모음에서는 **aaa authentication match** 명령을 사용하는 방법을 보여줍니다.

```
ciscoasa(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)

ciscoasa(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

이 컨텍스트에서는 다음 명령은

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

다음 명령과 동일합니다.

```
ciscoasa(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

aaa 명령문 목록은 **access-list** 명령문의 순서에 따라 달라집니다. 다음 명령을

```
ciscoasa(config)# aaa authentication match mylist outbound TACACS+
```

다음 명령보다 먼저 입력하면

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

ASA는 먼저 **mylist access-list** 명령문 그룹에서 일치하는 항목을 찾아본 다음 **yourlist access-list** 명령문 그룹에서 일치하는 항목을 찾습니다.

ASA를 통한 연결에 대한 인증을 활성화하고 이를 ID 방화벽 기능에 매칭하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# aaa authenticate match access_list_name inside user-identity
```

관련 명령

명령	설명
aaa authorization	사용자 권한 부여 서비스를 활성화합니다.
access-list extended	ACL을 생성합니다.
clear configure aaa	구성된 AAA 컨피그레이션을 제거합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa authentication secure-http-client

SSL을 활성화하고 HTTP 클라이언트와 ASA 간의 사용자 이름 및 비밀번호 교환을 보호하려면 글로벌 컨피그레이션 모드에서 **aaa authentication secure-http-client** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa authentication secure-http-client

no aaa authentication secure-http-client

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

aaa authentication secure-http-client 명령은 사용자 HTTP 기반 웹 요청이 ASA를 통과하는 것을 허용하기 전에 안전하게 ASA와의 사용자 인증을 수행할 수 있는 방법을 제공합니다. 이 명령은 SSL을 통한 HTTP 컷스루 프록시 인증에 사용됩니다.

aaa authentication secure-http-client 명령은 다음과 같은 제한 사항이 있습니다.

- 런타임에서 최대 16개의 HTTPS 인증 프로세스가 허용됩니다. 16개 HTTPS 인증 프로세스가 모두 실행되는 경우, 인증이 필요한 17번째의 신규 HTTPS 연결은 허용되지 않습니다.
- **uauth timeout 0**이 구성된 경우(**uauth timeout**이 0으로 설정됨) HTTPS 인증이 작동하지 않을 수도 있습니다. HTTPS 인증 이후 웹 페이지를 로드하기 위해 브라우저에서 여러 TCP 연결을 시작하는 경우, 첫 번째 연결은 허용되지만 이후의 연결은 인증을 트리거합니다. 따라서 매번 정확한 사용자 이름과 비밀번호를 입력하더라도 사용자에게 계속 인증 페이지가 표시됩니다. 이 문제를 해결하려면 **timeout uauth 0:0:1** 명령을 사용하여 **uauth timeout**을 1로 설정합니다. 그러나 이 방법을 적용하면 동일한 소스 IP 주소에서 온 인증되지 않은 사용자도 방화벽을 통과하는 것이 1초 동안 가능해집니다.

- HTTPS 인증은 SSL 포트 443에서 이루어지므로 사용자가 HTTP 클라이언트에서 HTTP 서버에 보내는 트래픽을 포트 443에서 차단하도록 **access-list** 명령문을 구성해서는 안 됩니다. 또한 고정 PAT가 포트 80에서 웹 트래픽을 위해 구성된 경우 SSL 포트에서도 구성되어야 합니다. 다음 예에서 첫 번째 행은 웹 트래픽을 위한 고정 PAT를 구성하며, 두 번째 행은 HTTPS 인증 컨피그레이션을 지원하기 위해 추가해야 합니다.

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

예

다음 예에서는 HTTP 트래픽이 안전하게 인증될 수 있도록 구성합니다.

```
ciscoasa(config)# aaa authentication secure-http-client
ciscoasa(config)# aaa authentication include http...
```

여기서 "..."은 *authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag*의 값입니다.

다음 명령은 HTTPS 트래픽이 안전하게 인증될 수 있도록 구성합니다.

```
ciscoasa (config)# aaa authentication include https...
```

여기서 "..."은 *authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*의 값입니다.

참고 HTTPS 트래픽에는 **aaa authentication secure-https-client** 명령이 필요하지 않습니다.

관련 명령

명령	설명
aaa authentication	**aaa-server** 명령으로 지정된 서버에서 LOCAL, TACACS+ 또는 RADIUS 사용자 인증을 활성화합니다.
virtual telnet	ASA 가상 서버에 액세스합니다.

aaa authorization command

명령 권한 부여를 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa authorization command** 명령을 사용합니다. 명령 권한 부여를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa authorization command {LOCAL | *tacacs+ server_tag* [LOCAL]}

no aaa authorization command {LOCAL | *tacacs+ server_tag* [LOCAL]}

구문 설명

LOCAL	**privilege** 명령으로 설정된 로컬 명령 권한 레벨을 활성화합니다. 로컬, RADIUS 또는 LDAP(LDAP 특성을 RADIUS 특성에 매핑한 경우) 사용자가 CLI 액세스를 위해 인증할 경우, ASA에서는 로컬 데이터베이스, RADIUS 또는 LDAP 서버에서 정의한 권한 레벨을 사용자에게 부여합니다. 사용자는 사용자 권한 레벨 이하의 명령에 액세스할 수 있습니다. TACACS+ 서버 그룹 태그 다음에 **LOCAL**을 지정할 경우, TACACS+ 서버 그룹을 사용할 수 없을 때만 명령 권한 부여에 로컬 사용자 데이터베이스를 사용합니다.
tacacs+ server_tag	TACACS+ 권한 부여 서버에 대해 미리 정의된 서버 그룹 태그를 지정합니다. **aaa-server** 명령으로 정의된 AAA 서버 그룹 태그입니다.

기본값

권한 부여에 로컬 데이터베이스를 대신 사용하는 것은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	TACACS+ 서버 그룹을 일시적으로 사용할 수 없을 때 LOCAL 권한 부여를 대신 사용하는 것에 대한 지원을 추가했습니다.
8.0(2)	RADIUS 또는 LDAP 서버에 정의된 권한 레벨에 대한 지원을 추가했습니다.

사용 지침

aaa authorization command 명령은 CLI에서의 명령 실행이 권한 부여 대상인지 여부를 지정합니다. 기본적으로 로그인할 때 사용자 EXEC 모드에 액세스할 수 있습니다. 이 모드는 최소 개수의 명령만 제공합니다. **enable** 명령(또는 로컬 데이터베이스를 사용할 때는 **login** 명령)을 입력하면 특별 권한 EXEC 모드와 고급 명령(컨피그레이션 명령 포함)에 액세스할 수 있습니다. 명령에 대한 액세스를 제어하고 싶은 경우 ASA에서 명령 권한 부여를 구성할 수 있습니다. 이는 사용자가 어떤 명령을 사용할 수 있는가를 결정하는 것입니다.

지원되는 명령 권한 부여 방식

다음 2가지 명령 권한 부여 방식 중 하나를 사용할 수 있습니다.

- 로컬 권한 레벨—ASA에서 명령 권한 레벨을 구성합니다. 로컬, RADIUS 또는 LDAP(LDAP 특성을 RADIUS 특성에 매핑한 경우) 사용자가 CLI 액세스를 위해 인증할 경우, ASA에서는 로컬 데이터베이스, RADIUS 또는 LDAP 서버에서 정의한 권한 레벨을 사용자에게 부여합니다. 사용자는 사용자 권한 레벨 이하의 명령에 액세스할 수 있습니다. 모든 사용자가 처음 로그인할 때는 사용자 EXEC 모드에 액세스합니다(레벨 0 또는 1의 명령). 사용자는 **enable** 명령을 사용하여 다시 인증해야 특별 권한 EXEC 모드(레벨 2 이상의 명령)에 액세스할 수 있습니다. 또는 **login** 명령을 사용하여 로그인할 수 있습니다(로컬 데이터베이스만).

참고 로컬 데이터베이스에 어떤 사용자도 없는 상태에서, CLI 또는 enable 인증 없이 로컬 명령 권한 부여를 사용할 수 있습니다. 그 대신 **enable** 명령을 입력할 때는 시스템 enable 비밀번호를 입력합니다. 그러면 ASA에서는 레벨 15를 부여합니다. 그러면 각 레벨의 enable 비밀번호를 만들 수 있습니다. 즉 **enable** *n*(2~15)을 입력하면 ASA에서는 레벨 *n*을 부여합니다. 이 레벨은 로컬 명령 권한 부여를 활성화한 경우에만 사용합니다. (자세한 내용은 **enable** 명령을 참조하십시오).

- TACACS+ 서버 권한 레벨—TACACS+ 서버에서 사용자 또는 그룹이 CLI 액세스를 위한 인증 이후에 사용할 수 있는 명령을 구성합니다. 사용자가 CLI에서 입력하는 모든 명령에 대해 TACACS+ 서버를 사용한 검사가 실시됩니다.

보안 컨텍스트 및 명령 권한 부여

다음은 다중 보안 컨텍스트로 명령 권한 부여를 구현할 때 중요하게 고려할 사항입니다.

- AAA 설정은 컨텍스트끼리 공유하지 않고 컨텍스트마다 다릅니다.

  명령 권한 부여를 구성할 때 각 보안 컨텍스트를 따로 구성해야 합니다. 따라서 여러 보안 컨텍스트에서 각기 다른 명령 권한 부여를 적용하는 것이 가능합니다.

  보안 컨텍스트 간 전환에서 관리자는 로그인 시 지정된 사용자 이름에 대해 허용된 명령이 새 컨텍스트 세션에서는 다를 수 있음을 또는 새 컨텍스트에서는 명령 권한 부여가 아예 구성되지 않았을 수도 있음을 알고 있어야 합니다. 명령 권한 부여가 보안 컨텍스트마다 다를 수 있음을 모르는 관리자는 혼란스러워 할 수도 있습니다. 이는 다음 사항 때문에 더욱 복잡해집니다.

- **changeto** 명령으로 시작한 새 컨텍스트 세션은 항상 기본 "enable_15" 사용자 이름을 관리자 ID로 사용합니다. 이전 컨텍스트 세션에서 어떤 사용자 이름을 사용했는가는 상관없습니다. 따라서 enable_15 사용자에 대해 명령 권한 부여가 구성되지 않은 경우 또는 enable_15 사용자에 대한 권한 부여가 이전 컨텍스트 세션 사용자에 대한 권한 부여와 다를 경우 혼란이 일어날 수 있습니다.

  이러한 동작은 명령 어카운팅에도 영향을 줍니다. 명령 어카운팅은 실행된 각 명령을 특정 관리자와 정확하게 연결할 수 있는 경우에만 유용합니다. **changeto** 명령을 사용할 권한이 있는 모든 관리자는 다른 컨텍스트에서 enable_15 사용자 이름을 사용할 수 있으므로 명령 어카운팅 레코드에서 누가 enable_15 사용자 이름으로 로그인했는지 즉시 식별하기 어렵습니다. 컨텍스트마다 다른 어카운팅 서버를 사용하는 경우, 누가 enable_15 사용자 이름을 사용하고 있었는지 추적하려면 여러 서버의 데이터를 연계하여 파악해야 합니다.

  명령 권한 부여를 구성할 때 다음 사항을 고려하십시오.

  - **changeto** 명령을 사용할 권한이 있는 관리자는 enable_15 사용자에게 허용된 모든 명령을 사실상 다른 모든 컨텍스트에서 사용할 수 있습니다.
  - 명령 권한 부여를 컨텍스트마다 다르게 하려는 경우, 각 컨텍스트에서 enable_15 사용자 이름에 허용되지 않은 명령은 **changeto** 명령 사용 권한을 가진 관리자에게도 거부되어야 합니다.

다른 보안 컨텍스트로 전환할 때 관리자는 특별 권한 EXEC 모드를 종료하고 **enable** 명령을 다시 입력하여 필요한 사용자 이름을 사용할 수 있습니다.

참고 시스템 실행 영역에서는 **aaa** 명령을 지원하지 않습니다. 따라서 시스템 실행 영역에서는 명령 권한 부여를 사용할 수 없습니다.

로컬 명령 권한 부여의 전제 조건

- **aaa authentication enable console** 명령을 사용하여 로컬, RADIUS 또는 LDAP 인증에 대한 enable 인증을 구성합니다.

  enable 인증은 사용자가 **enable** 명령에 액세스한 다음 사용자 이름을 유지하려면 필요합니다.

  또는 컨피그레이션이 필요 없는 **login** 명령을 사용할 수도 있습니다. 이는 인증과 관련해서는 **enable** 명령과 동일한 기능을 합니다. 이 옵션은 enable 인증만큼 안전하지 않으므로 권장하지 않습니다.

  CLI 인증(**aaa authentication** {**ssh** | **telnet** | **serial**} **console**)도 사용할 수도 있지만, 필수는 아닙니다.

- RADIUS가 인증에 사용될 경우 **aaa authorization exec** 명령을 사용하여 RADIUS 관리 사용자 권한 레벨의 지원을 활성화할 수도 있으나, 필수는 아닙니다. 이 명령은 로컬, RADIUS, LDAP(매핑됨), TACACS+ 사용자에 대한 관리 권한 부여도 활성화합니다.
- 사용자 유형별로 다음 전제 조건을 확인하십시오.
  - 로컬 데이터베이스 사용자—**username** 명령을 사용하여 0~15의 권한 레벨로 로컬 데이터베이스의 각 사용자를 구성합니다.
  - RADIUS 사용자—값이 0~15인 Cisco VSA CVPN3000-Privilege-Level로 사용자를 구성합니다.
  - LDAP 사용자—0~15의 권한 레벨로 사용자를 구성한 다음 **ldap map-attributes** 명령을 사용하여 LDAP 특성을 Cisco VAS CVPN3000-Privilege-Level에 매핑합니다.
- 명령 권한 레벨 설정에 대한 자세한 내용은 **privilege** 명령을 참조하십시오.

TACACS+ 명령 권한 부여

TACACS+ 명령 권한 부여를 활성화한 경우 어떤 사용자가 CLI에서 명령을 입력하면 ASA에서는 TACACS+ 서버에 명령과 사용자 이름을 보내 권한 부여된 명령인지 확인합니다.

TACACS+ 서버와의 명령 권한 부여를 구성할 때 컨피그레이션이 원하는 대로 작동한다고 확신하는 경우에만 컨피그레이션을 저장하십시오. 실수로 잠긴 경우 대개는 ASA를 다시 시작하면 액세스를 복구할 수 있습니다.

TACACS+ 시스템이 확실히 안정적이고 신뢰할 수 있는지 확인합니다. 필요한 수준의 신뢰도에 이르기 위해서는 일반적으로 완전 이중 TACACS+ 서버 시스템이 있고 ASA와 완전 이중 방식으로 연결되어야 합니다. 예를 들어, TACACS+ 서버 풀에서 인터페이스 1과 연결된 서버 1대와 인터페이스 2와 연결된 또 다른 서버를 포함합니다. TACACS+ 서버를 사용할 수 없을 경우를 위한 대비책으로 로컬 명령 권한 부여를 구성할 수도 있습니다. 그러한 경우 로컬 사용자와 명령 권한 레벨을 구성해야 합니다.

TACACS+ 서버 컨피그레이션에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

TACACS+ 명령 권한 부여의 전제 조건

- **aaa authentication** {**ssh** | **telnet** | **serial**} **console** 명령을 사용하여 CLI 인증을 구성합니다.
- **aaa authentication enable console** 명령을 사용하여 **enable** 인증을 구성합니다.

예

다음 예에서는 tplus1이라는 TACACS+ 서버 그룹을 사용하여 명령 권한 부여를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa authorization command tplus1
```

다음 예에서는 tplus1 서버 그룹의 모든 서버가 사용 불가능할 경우 로컬 사용자 데이터베이스를 대신 사용할 수 있도록 관리 권한 부여를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa authorization command tplus1 LOCAL
```

관련 명령

명령	설명
aaa authentication console	CLI, ASDM, enable 인증을 활성화합니다.
aaa authorization exec	RADIUS 관리 사용자 권한 레벨의 지원을 활성화합니다.
aaa-server host	호스트 관련 특성을 구성합니다.
aaa-server	그룹 기반 서버 특성을 구성합니다.
enable	특별 권한 EXEC 모드를 시작합니다.
ldap map-attributes	LDAP 특성을 ASA에서 사용할 수 있는 RADIUS 특성에 매핑합니다.
login	인증에 로컬 데이터베이스를 사용하면서 특별 권한 EXEC 모드를 시작합니다.
service-type	로컬 데이터베이스 사용자 CLI, ASDM, enable 액세스를 제한합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa authorization exec

명령 권한 부여를 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa authorization exec** 명령을 사용합니다. 관리 권한 부여를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa authorization exec {authentication-server | LOCAL} [auto-enable]

no aaa authorization exec {authentication-server | LOCAL} [auto-enable]

구문 설명

authentication-server	사용자 인증에 쓰인 서버에서 권한 부여 특성을 검색할 것임을 나타냅니다.
auto-enable	충분한 권한이 있는 관리자가 인증 자격 증명을 한 번 입력하면 특별 권한 EXEC 모드에 들어갈 수 있습니다.
LOCAL	인증 방식과 상관없이 ASA의 로컬 사용자 데이터베이스에서 권한 부여 특성을 검색할 것임을 나타냅니다.

기본값

기본적으로 이 명령은 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
8.2(2)	**LOCAL** 옵션을 추가했습니다.
9.2(1)	**auto-enable** 옵션을 추가했습니다.

사용 지침

aaa authorization exec 명령을 사용할 때 콘솔 액세스를 허용하려면 먼저 사용자의 service-type 자격 증명을 확인합니다.

no aaa authorization exec 명령을 사용하여 관리 권한 부여를 비활성화할 때 다음 사항을 주의하십시오.

- 콘솔 액세스를 허용하기 전에 사용자의 service-type 자격 증명을 확인하지 않습니다.
- 명령 권한 부여가 구성된 경우 권한 레벨 특성이 RADIUS, LDAP, TACACS+ 사용자의 AAA 서버에 있는 한 이 특성이 계속 적용됩니다.

사용자가 CLI, ASDM 또는 **enable** 명령에 액세스할 때 사용자를 인증하도록 **aaa authentication console** 명령을 구성할 경우, **aaa authorization exec** 명령이 사용자 컨피그레이션에 따라 관리 액세스를 제한할 수 있습니다.

참고 직렬 액세스는 관리 권한 부여에 포함되지 않습니다. 따라서 **aaa authentication serial console**을 구성할 경우 인증하는 어떤 사용자도 콘솔 포트에 액세스할 수 있습니다.

관리 권한 부여를 위해 사용자를 구성하려면 각 AAA 서버 유형 또는 로컬 사용자에 대한 다음 요구 사항을 확인하십시오.

- LDAP 매핑된 사용자—LDAP 특성을 매핑하려면 **ldap attribute-map** 명령을 참조하십시오.
- RADIUS 사용자—IETF RADIUS 숫자 **service-type** 특성을 사용합니다. 이는 다음 값 중 하나에 매핑됩니다.
  - Service-Type 5(Outbound)—관리 액세스를 거부합니다. 사용자는 **aaa authentication console** 명령으로 지정된 어떤 서비스도 사용할 수 없습니다(**serial** 키워드 제외, 직렬 액세스는 허용). 원격 액세스(IPSec 및 SSL) 사용자는 원격 액세스 세션을 계속 인증하고 종료할 수 있습니다.
  - Service-Type 6(Administrative)—**aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.
  - Service-Type 7(NAS prompt)—**aaa authentication {telnet | ssh} console** 명령을 구성할 때 CLI에 대한 액세스를 허용하지만, **aaa authentication http console** 명령을 구성할 경우에는 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **aaa authentication enable console** 명령으로 **enable** 인증을 구성할 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다.

참고 service-type은 Login (1), Framed (2), Administrative (6), NAS-Prompt (7)만 인식됩니다. 다른 service-type을 사용하면 액세스가 거부됩니다.

- TACACS+ 사용자—"service=shell" 엔트리로 권한 부여를 요청하며, 서버는 다음과 같이 PASS 또는 FAIL로 응답합니다.
  - PASS, 권한 레벨 1—**aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.
  - PASS, 권한 레벨 2 이상—**aaa authentication {telnet | ssh} console** 명령을 구성할 때 CLI에 대한 액세스를 허용하지만, **aaa authentication http console** 명령을 구성할 경우 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **aaa authentication enable console** 명령으로 enable 인증을 구성할 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다.
  - FAIL이면 관리 액세스를 거부합니다. 사용자는 **aaa authentication console** 명령으로 지정된 어떤 서비스도 사용할 수 없습니다(**serial** 키워드 제외, 직렬 액세스는 허용).
- 로컬 사용자—**service-type** 명령을 설정합니다. 이는 **username** 명령의 사용자 이름 컨피그레이션 모드에 있습니다. 기본적으로 **service-type**은 **admin**이며, 이는 **aaa authentication console** 명령으로 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다.

예 다음 예에서는 로컬 데이터베이스를 사용하는 관리 권한 부여를 활성화합니다.

```
ciscoasa(config)# aaa authorization exec LOCAL
```

관련 명령

명령	설명
aaa authentication console	콘솔 인증을 활성화합니다.
ldap attribute-map	LDAP 특성을 매핑합니다.
service-type	로컬 사용자에 대해 CLI 액세스를 제한합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa authorization include, exclude

ASA를 통한 연결에 대한 권한 부여를 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa authorization include** 명령을 사용합니다. 권한 부여를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 권한 부여에서 주소를 제외하려면 **aaa authorization exclude** 명령을 사용합니다. 권한 부여에서 주소를 제외하지 않으려면 이 명령의 **no** 형식을 사용합니다.

aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* **[***outside_ip outside_mask***]** *server_tag*

no aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

구문 설명

exclude	지정된 서비스 및 주소가 **include** 명령으로 이미 지정된 경우 이를 권한 부여에서 제외합니다.
include	권한 부여가 필요한 서비스 및 IP 주소를 지정합니다. **include** 문에서 지정되지 않은 트래픽은 처리되지 않습니다.
inside_ip	상위 보안 인터페이스의 IP 주소를 지정합니다. 이 주소는 이 명령을 적용하는 인터페이스에 따라 소스 주소 또는 수신 주소일 수 있습니다. 하위 보안 인터페이스에 명령을 적용할 경우 이 주소는 수신 주소입니다. 상위 보안 인터페이스에 명령을 적용할 경우 이 주소는 소스 주소입니다. 모든 호스트를 가리키려면 0을 사용합니다.
inside_mask	내부 IP 주소에 대한 네트워크 마스크를 지정합니다. IP 주소가 0이라면 0을 사용합니다. 호스트에는 255.255.255.255를 사용합니다.
interface_name	어떤 인터페이스 이름에서 사용자 권한 부여가 필요한지 지정합니다.
outside_ip	(선택 사항) 하위 보안 인터페이스의 IP 주소를 지정합니다. 이 주소는 이 명령을 적용하는 인터페이스에 따라 소스 주소 또는 수신 주소일 수 있습니다. 하위 보안 인터페이스에 명령을 적용할 경우 이 주소는 소스 주소입니다. 상위 보안 인터페이스에 명령을 적용할 경우 이 주소는 수신 주소입니다. 모든 호스트를 가리키려면 0을 사용합니다.
outside_mask	(선택 사항) 외부 IP 주소에 대한 네트워크 마스크를 지정합니다. IP 주소가 0이라면 0을 사용합니다. 호스트에는 255.255.255.255를 사용합니다.

server_tag	**aaa-server** 명령으로 정의된 AAA 서버 그룹을 지정합니다.
service	권한 부여가 필요한 서비스를 지정합니다. 다음 값 중 하나를 지정할 수 있습니다. • **any** 또는 **tcp/0**(모든 TCP 트래픽 지정) • **ftp** • **HTTP** • **https** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] **참고** 포트 범위를 지정하면 권한 부여 서버에서 예기치 않은 결과가 나올 수 있습니다. ASA는 서버에 포트 범위를 문자열로 보내는데, 서버에서 이를 특정 포트로 구문 분석할 것으로 예상합니다. 일부 서버는 그렇게 하지 않습니다. 게다가 특정 서비스에 대해 사용자의 권한 부여가 필요할 수 있는데, 범위가 승인되면 이러한 권한 부여가 이루어지지 않습니다.

기본값

IP 주소가 **0**이면 "모든 호스트"를 의미합니다. 로컬 IP 주소를 **0**으로 설정하면 권한 부여 서버에서 권한 부여할 호스트를 결정할 수 있습니다.

권한 부여에 로컬 데이터베이스를 대신 사용하는 것은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	사용자는 **exclude** 매개변수를 사용하여 특정 호스트에 대해 제외할 포트를 지정할 수 있습니다.

사용 지침

ACL에 의해 지정된 트래픽에 대한 권한 부여를 활성화하려면 **aaa authorization match** 명령을 사용합니다. **match** 명령은 **include** 및 **exclude** 명령과 동일한 컨피그레이션에서 사용할 수 없습니다. **include** 및 **exclude** 명령 대신 **match** 명령을 사용하는 것이 좋습니다. **include** 및 **exclude** 명령은 ASDM에서 지원하지 않습니다.

동일한 보안 인터페이스 간에 **aaa authorization include** 명령과 **exclude** 명령을 사용할 수 없습니다. 그러한 경우에는 **aaa authorization match** 명령을 사용해야 합니다.

ASA에서 TACACS+와의 네트워크 액세스 권한 부여를 수행하도록 구성할 수 있습니다. 인증문과 권한 부여문은 상호 독립적입니다. 그러나 권한 부여문과 매칭하지만 인증되지 않은 트래픽은 거부됩니다. 권한 부여가 성공하려면 사용자가 먼저 ASA와 인증해야 합니다. 특정 IP 주소의 사용자가 모든 규칙 및 유형에 대해 한 번만 인증하면 되므로, 인증 세션이 만료되지 않은 경우 트래픽이 인증문과 매칭하더라도 권한 부여가 이루어질 수 있습니다.

사용자가 인증하면 ASA는 권한 부여 규칙을 검사하여 트래픽이 매칭하는지 확인합니다. 트래픽이 권한 부여문과 매칭하면 ASA는 TACACS+ 서버에 사용자 이름을 보냅니다. TACACS+ 서버는 사용자 프로필에 따라 해당 트래픽을 허용하거나 거부하는 응답을 ASA에 보냅니다. ASA는 그에 대한 응답으로 권한 부여 규칙을 적용합니다.

사용자에 대해 네트워크 액세스 권한 부여를 구성하는 것에 대한 자세한 내용은 TACACS+ 서버의 설명서를 참조하십시오.

각 IP 주소에 대해 하나의 **aaa authorization include** 명령이 허용됩니다.

첫 번째 권한 부여 시도가 실패하고 두 번째 시도에서 시간 초과된 경우, **service resetinbound** 명령을 사용하여 권한 부여에 실패한 클라이언트를 재설정하여 어떤 연결도 재전송하지 않게 합니다. 다음은 텔넷의 권한 부여 시간 초과 메시지의 예입니다.

```
Unable to connect to remote host: Connection timed out
```

참고 포트 범위를 지정하면 권한 부여 서버에서 예기치 않은 결과가 나올 수 있습니다. ASA는 서버에 포트 범위를 문자열로 보내는데, 서버에서 이를 특정 포트로 구문 분석할 것으로 예상합니다. 일부 서버는 그렇게 하지 않습니다. 게다가 특정 서비스에 대해 사용자의 권한 부여가 필요할 수 있는데, 범위가 승인되면 이러한 권한 부여가 이루어지지 않습니다.

예

다음 예에서는 TACACS+ 프로토콜을 사용합니다.

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authorization include any inside 0 0 0 0
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authentication ssh console tplus1
```

이 예에서 첫 번째 명령문은 tplus1이라는 서버 그룹을 만들고 이 그룹에서 사용할 TACACS+ 프로토콜을 지정합니다. 두 번째 명령은 IP 주소가 10.1.1.10인 인증 서버가 내부 인터페이스에 상주하고 tplus1 서버 그룹에 속하도록 지정합니다. 다음 3개의 명령문은 외부 인터페이스를 통해 임의의 외부 호스트와의 연결을 시작하는 모든 사용자가 tplus1 서버 그룹을 사용하여 인증되고, 성공적으로 인증된 사용자는 모든 서비스를 사용할 권한이 부여되며, 모든 아웃바운드 연결 정보가 어카운팅 데이터베이스에 기록되도록 지정합니다. 마지막 명령문은 ASA 콘솔에 대한 SSH 액세스에 tplus1 서버 그룹의 인증이 필요함을 지정합니다.

다음 예에서는 외부 인터페이스로부터의 DNS 조회에 대한 권한 부여를 활성화합니다.

```
ciscoasa(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

다음 예에서는 내부 호스트에서 내부 인터페이스에 도달하는 ICMP echo-reply 패킷에 대한 권한 부여를 활성화합니다.

```
ciscoasa(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

이는 텔넷, HTTP 또는 FTP를 사용하여 인증되지 않은 사용자는 외부 호스트를 Ping할 수 없음을 의미합니다.

다음 예에서는 내부 호스트에서 내부 인터페이스에 도달하는 ICMP 에코(ping)에 대해서만 권한 부여를 활성화합니다.

```
ciscoasa(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

관련 명령

명령	설명
aaa authorization command	명령 실행이 권한 부여 대상인지 여부를 지정합니다. 또는 지정된 서버 그룹의 모든 서버가 비활성 상태일 경우 로컬 사용자 데이터베이스를 대신 사용하도록 관리 권한 부여를 구성합니다.
aaa authorization match	특정 access-list 명령 이름에 대해 LOCAL 또는 TACACS+ 사용자 권한 부여 서비스를 활성화하거나 비활성화합니다.
clear configure aaa	구성된 AAA 어카운팅 값을 제거하거나 재설정합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa authorization match

ASA를 통한 연결에 대한 권한 부여를 활성화하려면 글로벌 컨피그레이션 모드에서 **aaa authorization match** 명령을 사용합니다. 권한 부여를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

구문 설명

acl_name	확장된 ACL 이름을 지정합니다. **access-list extended** 명령을 참조하십시오. **permit** ACE는 매칭하는 트래픽을 권한 부여 대상으로 표시하지만, **deny** 엔트리는 매칭하는 트래픽을 권한 부여에서 제외합니다.
interface_name	어떤 인터페이스 이름에서 사용자 인증이 필요한지 지정합니다.
server_tag	**aaa-server** 명령으로 정의된 대로 AAA 서버 그룹 태그를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

aaa authorization match 명령은 **include** 및 **exclude** 명령과 동일한 컨피그레이션에서 사용할 수 없습니다. **include** 및 **exclude** 명령 대신 **match** 명령을 사용하는 것이 좋습니다. **include** 및 **exclude** 명령은 ASDM에서 지원하지 않습니다.

ASA에서 TACACS+와의 네트워크 액세스 권한 부여를 수행하도록 구성할 수 있습니다. **aaa authorization match** 명령을 사용한 RADIUS 권한 부여는 ASA와의 VPN 관리 연결에 대해서만 권한 부여를 지원합니다.

인증문과 권한 부여문은 상호 독립적입니다. 그러나 권한 부여문과 매칭하지만 인증되지 않은 트래픽은 거부됩니다. 권한 부여가 성공하려면 사용자가 먼저 ASA와 인증해야 합니다. 특정 IP 주소의 사용자가 모든 규칙 및 유형에 대해 한 번만 인증하면 되므로, 인증 세션이 만료되지 않은 경우 트래픽이 인증문과 매칭하더라도 권한 부여가 이루어질 수 있습니다.

사용자가 인증하면 ASA는 권한 부여 규칙을 검사하여 트래픽이 매칭하는지 확인합니다. 트래픽이 권한 부여문과 매칭하면 ASA는 TACACS+ 서버에 사용자 이름을 보냅니다. TACACS+ 서버는 사용자 프로필에 따라 해당 트래픽을 허용하거나 거부하는 응답을 ASA에 보냅니다. ASA는 그에 대한 응답으로 권한 부여 규칙을 적용합니다.

사용자에 대해 네트워크 액세스 권한 부여를 구성하는 것에 대한 자세한 내용은 TACACS+ 서버의 설명서를 참조하십시오.

첫 번째 권한 부여 시도가 실패하고 두 번째 시도에서 시간 초과된 경우, **service resetinbound** 명령을 사용하여 권한 부여에 실패한 클라이언트를 재설정하여 어떤 연결도 재전송하지 않게 합니다. 다음은 텔넷의 권한 부여 시간 초과 메시지의 예입니다.

```
Unable to connect to remote host: Connection timed out
```

참고 포트 범위를 지정하면 권한 부여 서버에서 예기치 않은 결과가 나올 수 있습니다. ASA는 서버에 포트 범위를 문자열로 보내는데, 서버에서 이를 특정 포트로 구문 분석할 것으로 예상합니다. 일부 서버는 그렇게 하지 않습니다. 게다가 특정 서비스에 대해 사용자의 권한 부여가 필요할 수 있는데, 범위가 승인되면 이러한 권한 부여가 이루어지지 않습니다.

예

다음 예에서는 **aaa** 명령과 함께 tplus1 서버 그룹을 사용합니다.

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authorization match myacl inside tplus1
```

이 예에서 첫 번째 명령문은 tplus1 서버 그룹을 TACACS+ 그룹으로 정의합니다. 두 번째 명령은 IP 주소가 10.1.1.10인 인증 서버가 내부 인터페이스에 상주하고 tplus1 서버 그룹에 속하도록 지정합니다. 다음 두 명령문은 내부 인터페이스를 거치는 임의의 외부 호스트와의 연결이 모두 tplus1 서버 그룹을 사용하여 인증되고 이 모든 연결이 어카운팅 데이터베이스에 로깅되게 합니다. 마지막 명령문은 myacl의 ACE와 매칭하는 모든 연결에 대해 tplus1 서버 그룹의 AAA 서버를 통해 권한 부여하도록 지정합니다.

관련 명령

명령	설명
aaa authorization	사용자 권한 부여를 활성화하거나 비활성화합니다.
clear configure aaa	모든 aaa 컨피그레이션 매개변수를 기본값으로 재설정합니다.
clear uauth	어떤 사용자 또는 모든 사용자에 대해 AAA 권한 부여 및 인증 캐시를 삭제합니다. 그러면 사용자가 다음에 연결을 생성할 때 반드시 재인증해야 합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.
show uauth	인증 및 권한 부여를 위해 권한 부여 서버에 제공된 사용자 이름, 사용자 이름이 바인딩된 IP 주소, 사용자 인증만 이루어지는지 아니면 캐시에 저장되는 서비스가 있는지 여부를 표시합니다.

aaa local authentication attempts max-fail

ASA에서 특정 사용자 계정(이 기능이 적용되지 않는 권한 레벨 15 사용자는 제외)에 허용하는 로컬 로그인의 연속 시도 실패 횟수를 제한하려면 글로벌 컨피그레이션 모드에서 **aaa local authentication attempts max-fail** 명령을 사용합니다. 이 기능을 비활성화하고 실패 횟수의 제한 없이 로컬 로그인의 연속 시도를 허용하려면 이 명령의 **no** 형식을 사용합니다.

aaa local authentication attempts max-fail *number*

구문 설명

number	사용자가 잠기기 전까지 허용되는 비밀번호 입력 오류의 최대 횟수. 1~16 범위의 숫자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 로컬 사용자 데이터베이스를 사용한 인증에만 적용됩니다. 이 명령을 생략할 경우 사용자의 비밀번호 입력 오류 횟수가 제한되지 않습니다.

구성된 횟수만큼 사용자의 비밀번호 입력 오류가 발생하면 사용자는 잠기며 관리자가 그 사용자 이름의 잠금을 해제할 때까지는 로그인할 수 없습니다. 사용자 이름을 잠그거나 잠금 해제하면 syslog 메시지가 생성됩니다.

권한 레벨이 15인 사용자는 이 명령이 적용되지 않습니다. 이 사용자는 잠글 수 없습니다.

사용자가 성공적으로 인증하거나 ASA가 재부팅되면 실패 횟수가 0으로, 잠금 상태가 No로 재설정됩니다.

예

다음 예에서는 **aaa local authentication attempts max-limits** 명령을 사용하여 허용되는 최대 실패 횟수를 2로 설정하는 것을 보여줍니다.

```
ciscoasa(config)# aaa local authentication attempts max-limits 2
```

관련 명령

명령	설명
clear aaa local user lockout	지정된 사용자의 잠금 상태를 지우고 그 failed-attempts 카운터를 0으로 설정합니다.
clear aaa local user fail-attempts	사용자 잠금 상태를 수정하지 않고 사용자 인증 시도의 실패 횟수를 0으로 재설정합니다.
show aaa local user	현재 잠겨 있는 사용자 이름의 목록을 표시합니다.

aaa mac-exempt

인증 및 권한 부여에서 제외하는 데 미리 정의된 MAC 주소의 목록을 사용하도록 지정하려면 글로벌 컨피그레이션 모드에서 **aaa mac-exempt** 명령을 사용합니다. MAC 주소 목록의 사용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

구문 설명

id	**mac-list** 명령으로 구성된 MAC 목록 번호를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

aaa mac-exempt 명령은 하나만 추가할 수 있습니다. **aaa mac-exempt** 명령을 사용하기 전에 **mac-list** 명령을 사용하여 MAC 목록 번호를 구성합니다. MAC 목록의 permit 엔트리는 해당 MAC 주소를 인증 및 권한 부여에서 제외하지만, deny 엔트리는 활성화된 경우 MAC 주소에 대한 인증 및 권한 부여가 이루어져야 합니다. **aaa mac-exempt** 명령의 인스턴스를 하나만 추가할 수 있으므로 제외할 모든 MAC 주소를 MAC 목록에 포함해야 합니다.

예

다음 예에서는 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 Phone에서 인증을 우회합니다.

```
ciscoasa(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
ciscoasa(config)# aaa mac-exempt match acd
```

다음 예에서는 00a0.c95d.02b2를 제외하고 어떤 MAC 주소 그룹에 대해 인증을 우회합니다.

```
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 권한 부여 서비스를 활성화합니다.
aaa mac-exempt	MAC 주소의 목록을 인증 및 권한 부여에서 제외합니다.
show running-config mac-list	**mac-list** 명령에서 이미 지정된 MAC 주소의 목록을 표시합니다.
mac-list	MAC 주소를 인증 및/또는 권한 부여에서 제외하는 데 사용할 MAC 주소의 목록을 지정합니다.

aaa proxy-limit

특정 IP 주소에 대해 동시에 이루어지는 인증 시도의 횟수를 제한하려면 글로벌 컨피그레이션 모드에서 **aaa proxy-limit** 명령을 사용합니다. proxy-limit 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

구문 설명

disable	허용되는 프록시가 없도록 지정합니다.
proxy_limit	사용자당 허용되는 동시 프록시 연결 수를 1~128 범위에서 지정합니다.

기본값

proxy-limit 기본값은 16입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

소스 주소가 프록시 서버일 경우 이 IP 주소를 인증에서 제외하거나 허용되는 미처리 AAA 요청 수를 늘려 보십시오.

예를 들어, 두 사용자가 동일한 IP 주소에 있고(아마도 터미널 서버에 연결되어 있음) 둘 다 브라우저를 열거나 연결을 시작하고 정확히 동시에 인증을 시도하는 경우 그중 하나만 허용되며 다른 하나는 차단됩니다.

이 IP 주소의 첫 번째 세션은 프록시되고 인증 요청이 전송되지만, 다른 세션은 시간 초과됩니다. 이는 어떤 단일 사용자 이름의 연결 수와는 상관없습니다.

예

다음 예에서는 특정 IP 주소에 대해 미처리 인증 (동시) 시도의 최대 횟수를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa proxy-limit 6
```

관련 명령

명령	설명
aaa authentication	**aaa-server** 명령으로 또는 ASDM 사용자 인증에 의해 지정된 서버에서 LOCAL, TACACS+ 또는 RADIUS 사용자 인증을 활성화, 비활성화하거나 표시합니다.
aaa authorization	LOCAL 또는 TACACS+ 사용자 권한 부여 서비스를 활성화하거나 비활성화합니다.
aaa-server host	AAA 서버를 지정합니다.
clear configure aaa	구성된 AAA 어카운팅 값을 제거하거나 재설정합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

aaa-server

AAA 서버 그룹을 만들고 모든 그룹 호스트에 공통적으로 적용되는, 그룹에 특화된 AAA 서버 매개변수를 구성하려면 글로벌 컨피그레이션 모드에서 **aaa-server** 명령을 사용합니다. 지정된 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

구문 설명

protocol *server-protocol*	그룹의 서버가 지원하는 AAA 프로토콜을 지정합니다. • **http-form** • **kerberos** • **ldap** • **nt**(이 옵션은 9.3(1) 릴리스부터 더 이상 사용할 수 없음) • **radius** • **sdi** • **tacacs+**
server-tag	**aaa-server host** 명령에서 지정된 이름과 매칭하는 서버 그룹 이름을 지정합니다. 다른 AAA 명령은 AAA 서버 그룹 이름을 참조합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	**http-form** 프로토콜을 추가했습니다.
8.2(2)	단일 모드의 AAA 서버 그룹 최대 개수를 15개에서 100개로 늘렸습니다.
8.4(2)	aaa-server group 컨피그레이션 모드의 **ad-agent-mode** 옵션을 추가했습니다.
9.3(1)	**nt** 옵션은 더 이상 사용할 수 없습니다. Windows NT 도메인 인증이 더 이상 지원되지 않습니다.

사용 지침

단일 모드로 최대 100개의 서버 그룹 또는 다중 모드로 컨텍스트당 4개의 서버 그룹을 포함할 수 있습니다. 각 그룹은 단일 모드에서 최대 15개의 서버 또는 다중 모드에서 4대의 서버를 포함할 수 있습니다. 사용자가 로그인하면, 컨피그레이션에서 지정한 첫 번째 서버부터 시작하여 서버가 응답할 때까지 한 번에 하나씩 서버에 액세스합니다.

aaa-server 명령으로 AAA 서버 그룹 프로토콜을 정의하여 AAA 서버 컨피그레이션을 제어한 다음 **aaa-server host** 명령을 사용하여 그룹에 서버를 추가합니다. **aaa-server protocol** 명령을 입력하면 aaa-server 서버 컨피그레이션 모드가 됩니다.

aaa-server group 컨피그레이션 모드에서 RADIUS 프로토콜을 사용하는 경우 다음 사항을 주의하십시오.

- 클라이언트리스 SSL 및 AnyConnect 세션에 대해 다중 세션 어카운팅을 활성화하려면 **interim-accounting-update** 옵션을 입력합니다. 이 옵션을 선택할 경우 시작 및 중단 레코드 외에 임시 어카운팅 레코드도 RADIUS 서버에 보내집니다.
- ASA와 AD 에이전트 간의 공유 암호를 지정하고 RADIUS 서버 그룹이 모든 기능을 갖춘 RADIUS 서버가 아닌 AD 에이전트를 포함하도록 지정하려면 **ad-agent-mode** 옵션을 입력합니다. 이 옵션을 사용하여 구성된 RADIUS 서버 그룹만 사용자 ID에 연결할 수 있습니다. 따라서 **ad-agent-mode** 옵션으로 구성되지 않은 RADIUS 서버 그룹이 지정되면 **test aaa-server** {**authentication** | **authorization**} *aaa-server-group* 명령을 사용할 수 없습니다.

참고 ASA는 **aaa-server protocol nt** 명령을 입력하거나 시작 중에 컨피그레이션에서 읽을 때마다 콘솔에 메시지를 표시합니다. 이 메시지는 ASA의 다음 주 릴리스에서 이 인증 방법이 제거될 것임을 알립니다.

예

다음 예에서는 TACACS+ 서버 그룹 컨피그레이션의 세부사항을 수정하는 데 **aaa-server** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# reactivation mode timed
ciscoasa(config-aaa-server-group)# max-failed attempts 2
```

관련 명령

명령	설명
accounting-mode	어카운팅 메시지가 단일 서버에 보내지는지(단일 모드) 또는 그룹의 모든 서버에 보내지는지(동시 모드) 나타냅니다.
reactivation-mode	오류가 발생한 서버가 재활성화되는 방법을 지정합니다.
max-failed-attempts	서버 그룹의 어떤 서버가 비활성화되기 전에 허용되는 오류 횟수를 지정합니다.
clear configure aaa-server	모든 AAA 서버 컨피그레이션을 제거합니다.
show running-config aaa-server	특정 서버 그룹, 특정 그룹에 속한 특정 서버 또는 특정 프로토콜에 대해 모든 AAA 서버의 AAA 서버 통계를 표시합니다.

aaa-server active, fail

오류가 발생한 것으로 표시된 AAA 서버를 재활성화하려면 특별 권한 EXEC 모드에서 **aaa-server active** 명령을 사용합니다. 활성 서버를 오류 상태로 만들려면 특별 권한 EXEC 모드에서 **aaa-server fail** 명령을 사용합니다.

aaa-server *server_tag* **[active | fail] host {***server_ip* **|** *name***}**

구문 설명

active	서버를 활성 상태로 설정합니다.
fail	서버를 오류가 발생한 상태로 설정합니다.
host	호스트 IP 주소 이름 또는 IP 주소를 지정합니다.
name	**name** 명령을 통해 로컬에서 지정된 이름 또는 DNS 이름을 사용하여 서버의 이름을 지정합니다. DNS 이름은 최대 128자, **name** 명령으로 지정되는 이름은 63자입니다.
server_ip	AAA 서버의 IP 주소를 지정합니다.
server_tag	**aaa-server** 명령으로 지정된 이름과 매칭하는 서버 그룹의 심볼 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

이 명령을 사용하지 않으면, 어떤 그룹에서 오류가 발생한 서버는 해당 그룹의 모든 서버에서 오류가 발생할 때까지 오류 상태로 있다가 모두 재활성화됩니다.

예

다음 예에서는 서버 192.168.125.60의 상태를 표시하고 이를 수동으로 재활성화합니다.

```
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
```

```
ciscoasa# aaa-server active host 192.168.125.60
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

관련 명령

명령	설명
aaa-server	AAA 서버 그룹을 만들고 수정합니다.
clear configure aaa-server	모든 AAA 서버 컨피그레이션을 제거합니다.
show running-config aaa-server	특정 서버 그룹, 특정 그룹에 속한 특정 서버 또는 특정 프로토콜에 대해 모든 AAA 서버의 AAA 서버 통계를 표시합니다.

aaa-server host

어떤 AAA 서버를 AAA 서버 그룹의 일원으로 구성하고 호스트에 특화된 AAA 서버 매개변수를 구성하려면 글로벌 컨피그레이션 모드에서 **aaa-server host** 명령을 사용합니다. 호스트 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

aaa-server *server-tag* **[**(*interface-name*)**] host {***server-ip* **|** *name***}** [*key*] **[timeout** *seconds*]

no aaa-server *server-tag* **[**(*interface-name*)**] host {***server-ip* **|** *name***}** [*key*] **[timeout** *seconds*]

구문 설명

(*interface-name*)	(선택 사항) 인증 서버가 상주하는 네트워크 인터페이스를 지정합니다. 이 매개변수에서는 괄호가 필요합니다. 인터페이스를 지정하지 않을 경우 기본값인 **inside**가 사용 가능하면 적용됩니다.
key	(선택 사항) 대/소문자를 구분하는 최대 127자의 영숫자 키워드로 RADIUS 또는 TACACS+ 서버의 키와 같은 값을 지정합니다. 127자를 초과하여 입력되는 문자는 무시됩니다. 이 키는 ASA와 서버 간의 데이터 암호화에 사용됩니다. 이 키가 ASA와 서버 시스템 모두에서 동일해야 합니다. 키에서 공백은 허용되지 않지만, 다른 특수 문자는 사용 가능합니다. 호스트 모드에서 **key** 명령을 사용하여 키를 추가하거나 수정할 수 있습니다.
name	**name** 명령을 통해 로컬에서 지정된 이름 또는 DNS 이름을 사용하여 서버의 이름을 지정합니다. DNS 이름은 최대 128자, **name** 명령으로 지정되는 이름은 63자입니다.
server-ip	AAA 서버의 IP 주소를 지정합니다.
server-tag	**aaa-server** 명령으로 지정된 이름과 매칭하는 서버 그룹의 심볼 이름을 지정합니다.
timeout *seconds*	(선택 사항) 요청의 시간 초과 간격입니다. 이 시간이 경과하면 ASA는 기본 AAA 서버에 대한 요청을 포기합니다. 대기 AAA 서버가 있을 경우 ASA는 그 백업 서버에 요청을 보냅니다. 호스트 컨피그레이션 모드에서 **timeout** 명령을 사용하여 시간 초과 간격을 수정할 수 있습니다.

기본값

시간 초과의 기본값은 10초입니다.

기본 인터페이스는 inside입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	DNS 이름 지원을 추가했습니다.
9.0(1)	사용자 ID 지원을 추가했습니다.

사용 지침

aaa-server 명령으로 AAA 서버 그룹을 정의하여 AAA 서버 컨피그레이션을 제어한 다음 **aaa-server host** 명령을 사용하여 그룹에 서버를 추가합니다. **aaa-server host** 명령을 사용하여 aaa-server 호스트 컨피그레이션 모드를 시작합니다. 여기서 호스트별 AAA 서버 연결 데이터를 지정하고 관리할 수 있습니다.

단일 모드로 최대 15개의 서버 그룹 또는 다중 모드로 컨텍스트당 4개의 서버 그룹을 포함할 수 있습니다. 각 그룹은 단일 모드에서 최대 16개의 서버 또는 다중 모드에서 4대의 서버를 포함할 수 있습니다. 사용자가 로그인하면, 컨피그레이션에서 지정한 첫 번째 서버부터 시작하여 서버가 응답할 때까지 한 번에 하나씩 서버에 액세스합니다.

예

다음 예에서는 "watchdogs"라는 Kerberos AAA 서버 그룹을 구성하고 이 그룹에 AAA 서버를 추가하며 서버를 위한 Kerberos 영역을 정의합니다.

참고 Kerberos 영역 이름에는 숫자와 대문자만 사용합니다. ASA에서는 영역 이름으로 소문자를 허용하지만 소문자를 대문자로 변환하지는 않습니다. 반드시 대문자만 사용하십시오.

```
ciscoasa(config)# aaa-server watchdogs protocol kerberos
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

다음 예에서는 "svrgrp1"이라는 SDI AAA 서버 그룹을 구성한 다음 이 그룹에 AAA 서버를 추가하고 시간 초과 간격을 6초로, 재시도 간격을 7초로 설정하고 SDI 버전을 버전 5로 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol sdi
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 6
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# sdi-version sdi-5
```

다음 예에서는 LDAP 검색을 위해 **aaa-server** *aaa_server_group_tag* 명령을 사용할 때 검색 경로를 대상 그룹으로 좁히는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server CISCO_AD_SERVER protocol ldap
ciscoasa(config)# aaa-server CISCO_AD_SERVER host 10.1.1.1
ciscoasa(config-aaa-server-host)# server-port 636
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Cisco Groups,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password *
ciscoasa(config-aaa-server-host)# ldap-login-dn CISCO\username1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
```

참고 **ldap-group-base-dn** 명령이 지정되면 모든 그룹이 LDAP 디렉토리 계층 구조에서 그 아래에 있어야 하며 어떤 그룹도 이 경로를 벗어난 곳에 상주할 수 없습니다.

ldap-group-base-dn 명령은 활성화된 사용자 ID 기반 정책이 하나 이상 있을 때만 적용됩니다.

기본 설정이 아닌 **server-type microsoft** 명령을 구성해야 합니다.

첫 번째 **aaa-server** *aaa_server_group_tag* **host** 명령은 LDAP 작업에 사용됩니다.

관련 명령

명령	설명
aaa-server	AAA 서버 그룹을 만들고 수정합니다.
clear configure aaa-server	모든 AAA 서버 컨피그레이션을 제거합니다.
show running-config aaa-server	특정 서버 그룹, 특정 그룹에 속한 특정 서버 또는 특정 프로토콜에 대해 모든 AAA 서버의 AAA 서버 통계를 표시합니다.

absolute

시간 범위가 유효한 절대 시간을 정의하려면 시간 범위 컨피그레이션 모드에서 **absolute** 명령을 사용합니다. 어떤 시간 범위에 대해 시간을 지정하지 않으려면 이 명령의 **no** 형식을 사용합니다.

absolute [**end** *time date*] [**start** *time date*]

no absolute

구문 설명

date	(선택 사항) 일 월 연도의 형식으로 날짜를 지정합니다(예: 1 January 2006). 연도는 1993~2035 범위에서 선택합니다.
end	(선택 사항) 시간 범위의 끝을 지정합니다.
start	(선택 사항) 시간 범위의 시작을 지정합니다.
time	(선택 사항) HH:MM 형식으로 시간을 지정합니다. 예를 들어, 8:00은 오전 8:00입니다. 그리고 20:00은 오후 8:00입니다.

기본값

시작 시간 및 날짜가 지정되지 않으면 허용 또는 거부 구문이 즉시 그리고 계속 효력을 갖습니다. 종료 시간의 최대값은 23:59 31 December 2035입니다. 종료 시간 및 날짜가 지정되지 않으면 해당 허용 또는 거부 구문이 즉시 무한정 적용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
시간 범위 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

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.

예

다음 예에서는 2006년 1월 1일 오전 8시에 ACL을 활성화합니다.

```
ciscoasa(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

관련 명령

명령	설명
access-list extended	ASA를 지나는 IP 트래픽을 허용하거나 거부하는 정책을 구성합니다.
default	**time-range** 명령 **absolute** 및 **periodic** 키워드의 기본 설정을 복원합니다.
periodic	시간 범위 기능을 지원하는 기능에 대한 반복적 (주간) 시간 범위를 지정합니다.
time-range	시간을 기준으로 한 ASA에 대한 액세스 제어를 정의합니다.

accept-subordinates

디바이스에 하위 CA 인증서가 설치되지 않은 상태에서 1단계 IKE 교환 중에 제공된 하위 CA 인증서를 승인하도록 ASA를 구성하려면 crypto ca trustpoint 컨피그레이션 모드에서 **accept-subordinates** 명령을 사용합니다. 기본 설정으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

accept-subordinates

no accept-subordinates

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 설정은 on입니다(하위 인증서 승인됨).

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

1단계 처리에서 IKE 피어가 하위 인증서와 ID 인증서를 모두 통과할 수도 있습니다. 하위 인증서가 ASA에 설치되지 않을 수도 있습니다. 관리자는 설정된 모든 신뢰 지점의 모든 하위 CA 인증서가 적합해야 한다는 요구 사항 없이 이 명령을 사용하여 디바이스에 신뢰 지점으로 구성되지 않은 하위 CA 인증서를 지원할 수 있습니다. 즉 이 명령은 디바이스에서 로컬에 전체 인증서 체인을 설치하지 않고도 어떤 인증서 체인을 인증할 수 있게 합니다.

예

다음 예에서는 trustpoint central에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작하고 ASA에서 trustpoint central에 대한 하위 인증서를 승인할 수 있게 합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# accept-subordinates
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.
default enrollment	등록 매개변수를 기본값으로 되돌립니다.

access-group

확장 ACL을 단일 인터페이스에 바인딩하려면 글로벌 컨피그레이션 모드에서 **access-group** 명령을 사용합니다. 인터페이스에서 ACL의 바인딩을 해제하려면 이 명령의 **no** 형식을 사용합니다.

access-group *access_list* **{in | out} interface** *interface_name* **[per-user-override | control-plane]**

no access-group *access_list* **{in | out} interface** *interface_name*

단일 명령으로 모든 인터페이스에 단일 전역 규칙 집합을 적용하려면 글로벌 컨피그레이션 모드에서 **access-group global** 명령을 사용합니다. 구성된 모든 인터페이스에서 전역 규칙을 제거하려면 이 명령의 **no** 형식을 사용합니다.

access-group *access_list* **[global]**

no access-group *access_list* **[global]**

구문 설명

access_list	확장 ACL *id*
control-plane	(선택 사항) ACL을 to-the-box 트래픽에 사용할 수 있는지 여부를 지정합니다. 예를 들어, ISAKMP를 차단하여 특정 원격 IP 주소에서 ASA와의 VPN 세션을 시작할 수 없게 하는 데 이 옵션을 사용할 수 있습니다. to-the-box 관리 트래픽에 대한 액세스 규칙(**http**, **ssh**, **telnet**과 같은 명령으로 정의됨)은 **control-plane** 옵션으로 적용되는 ACL보다 우선순위가 높습니다. 따라서 이렇게 허용된 관리 트래픽은 to-the-box ACL에서 명시적으로 거부하더라도 통과가 허용됩니다. 이 옵션은 **in** 방향에서만 사용 가능합니다.
global	모든 인터페이스의 모든 트래픽에 ACL을 적용합니다.
in	지정된 인터페이스의 인바운드 패킷을 필터링합니다.
interface *interface_name*	네트워크 인터페이스의 이름입니다.
out	지정된 인터페이스의 아웃바운드 패킷을 필터링합니다.
per-user-override	(선택 사항) 다운로드 가능한 사용자 ACL이 인터페이스에 적용된 ACL을 재정의할 수 있게 합니다. 이 옵션은 **in** 방향에서만 사용 가능합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.3(1)	전역 정책을 지원하도록 이 명령을 수정했습니다.

사용 지침

인터페이스별 액세스 그룹 규칙이 전역 규칙보다 우선순위가 높습니다. 따라서 패킷 분류 시 인터페이스별 규칙이 전역 규칙보다 먼저 처리됩니다.

인터페이스별 규칙의 사용 지침

access-group 명령은 확장 ACL을 인터페이스에 바인딩합니다. 먼저 **access-list extended** 명령을 사용하여 ACL을 만들어야 합니다.

인터페이스의 인바운드 트래픽 또는 아웃바운드 트래픽에 ACL을 적용할 수 있습니다. **access-list** 명령문에서 **permit** 옵션을 입력할 경우 ASA에서는 계속 패킷을 처리합니다. **access-list** 명령문에서 **deny** 옵션을 입력할 경우 ASA에서는 패킷을 폐기하고 syslog 메시지 106023(기본 설정이 아닌 로깅을 사용하는 ACE는 106100)을 생성합니다.

인바운드 ACL의 경우 **per-user-override** 옵션은 다운로드 가능한 ACL이 인터페이스에 적용된 ACL을 재정의할 수 있게 합니다. **per-user-override** 옵션이 없을 경우 ASA는 기존 필터링 동작을 유지합니다. **per-user-override**가 있으면 ASA는 어떤 사용자와 연결된 사용자별 액세스 목록(다운로드된 경우)의 **permit** 또는 **deny** 상태가 **access-group** 명령과 연결된 ACL의 permit 또는 deny 상태를 재정의할 수 있게 합니다. 또한 다음 규칙이 적용됩니다.

- 패킷이 도달했을 때, 그 패킷과 연결된 사용자별 ACL이 없을 경우 인터페이스 ACL이 적용됩니다.
- 사용자별 ACL은 **timeout** 명령의 **uauth** 옵션으로 지정되는 시간 초과 값이 적용됩니다. 그러나 AAA 사용자별 세션 시간 초과 값으로 재정의될 수 있습니다.
- 기존 ACL 로그 동작은 동일합니다. 예를 들어, 사용자 트래픽이 사용자별 ACL 때문에 거부될 경우 syslog 메시지 109025가 로깅됩니다. 사용자 트래픽이 허용될 경우 syslog 메시지가 생성되지 않습니다. 사용자별 액세스 목록의 로그 옵션은 적용되지 않습니다.

기본적으로 VPN 원격 액세스 트래픽은 인터페이스 ACL을 기준으로 확인되지 않습니다. 그러나 **no sysopt connection permit-vpn** 명령을 사용하여 이러한 우회를 해제하면, 그룹 정책에 적용된 **vpn-filter**가 있는지 여부 및 **per-user-override** 옵션이 설정되었는지 여부에 따라 동작이 달라집니다.

- No **per-user-override**, no **vpn-filter** - 인터페이스 ACL을 기준으로 트래픽을 확인합니다.
- No **per-user-override**, **vpn-filter** - 처음에는 인터페이스 ACL을 기준으로 트래픽을 확인한 후 VPN 필터를 기준으로 확인합니다.
- **per-user-override**, **vpn-filter** - VPN 필터만을 기준으로 트래픽을 확인합니다.

참고 하나 이상의 **access-group** 명령에서 참조하는 ACL의 모든 기능 엔트리(허용 및 거부 구문)가 제거될 경우 **access-group** 명령은 자동으로 컨피그레이션에서 제거됩니다. **access-group** 명령은 빈 ACL 또는 설명만 있는 ACL을 참조할 수 없습니다.

전역 규칙의 사용 지침

access-group global 명령은 트래픽이 어떤 인터페이스에서 ASA에 도달하는가와 상관없이 모든 트래픽에 하나의 전역 규칙 집합을 적용합니다.

모든 전역 규칙은 인그레스(인바운드) 방향의 트래픽에만 적용됩니다. 전역 규칙은 이그레스(아웃바운드) 트래픽을 지원하지 않습니다. 전역 규칙이 인바운드 인터페이스 액세스 규칙과 함께 구성된 경우, 특화된 인터페이스 액세스 규칙이 일반적인 전역 액세스 규칙보다 먼저 처리됩니다.

예

다음 예에서는 **access-group global** 명령을 사용하여 구성된 모든 인터페이스에 ACL을 적용하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list acl-1 extended permit ip host 10.1.2.2 host 10.2.2.2
ciscoasa(config)# access-list acl-2 extended deny ip any any

ciscoasa(config)# access-group acl-2
ciscoasa(config)# access-group acl-1 in interface outside

ciscoasa(config)# show run access-group acl-2
ciscoasa(config)# access-group acl-1 in interface outside

ciscoasa(config)# access-group acl-2 global
```

앞의 액세스 규칙 컨피그레이션은 분류 테이블(**show asp table classify** 명령의 출력)에 다음 규칙을 추가합니다.

```
in  id=0xb1f90068, priority=13, domain=permit, deny=false
        hits=0, user_data=0xaece1ac0, cs_id=0x0, flags=0x0, protocol=0
        src ip=10.1.2.2, mask=255.255.255.255, port=0
        dst ip=10.2.2.2, mask=255.255.255.255, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a250, priority=12, domain=permit, deny=true
        hits=0, user_data=0xaece1b40, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
in  id=0xb1f90100, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a3f8, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
```

앞의 규칙은 출력 인터페이스에서 10.1.2.2의 트래픽을 10.2.2.2로 전달하고, 전역 거부 규칙 때문에 출력 인터페이스에서 10.1.1.10에서 10.2.2.20으로 보내는 트래픽을 폐기합니다.

다음 예에서는 임의 위치의 DMZ에서 HTTP 서버(IP 주소는 10.2.2.2)에 대한 전역 액세스를 허용합니다.

```
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

앞의 규칙은 외부 호스트 10.1.2.2에서 호스트 10.2.2.2로의 HTTP 연결을 허용하고 내부 호스트 192.168.0.0에서 호스트 10.2.2.2로의 HTTP 연결을 허용합니다.

다음 예에서는 전역 규칙과 인터페이스 규칙을 어떻게 함께 사용할 수 있는지 보여줍니다. 이 예에서는 임의의 내부 호스트에서 서버(IP 주소는 10.2.2.2)에 액세스하는 것을 허용하되 다른 호스트에서 서버에 액세스하는 것은 거부합니다. 인터페이스 정책이 우선적으로 적용됩니다.

```
ciscoasa(config)# access-list inside_acl permit tcp any host 10.2.2.2 eq 23
ciscoasa(config)# access-list global_acl deny ip any host 10.2.2.2
ciscoasa(config)# access-group inside_acl in interface inside
ciscoasa(config)# access-group global_acl global
```

앞의 규칙은 외부 호스트 10.1.2.2에서 호스트 10.2.2.2로의 SSH 연결을 거부하고 내부 호스트 192.168.0.0에서 호스트 10.2.2.2로의 SSH 연결을 허용합니다.

다음 예에서는 NAT와 전역 액세스 제어 정책이 어떻게 연동하는지 보여줍니다. 이 예에서는 외부 호스트 10.1.2.2에서 호스트 10.2.2.2로의 HTTP 연결 하나를 허용하고 내부 호스트 192.168.0.0에서 호스트 10.2.2.2로의 다른 HTTP 연결을 허용하되 (묵시적 규칙을 통해) 외부 호스트 10.255.255.255에서 호스트 172.31.255.255로의 HTTP 연결은 거부합니다.

```
ciscoasa(config)# object network dmz-server host 10.1.1.2
ciscoasa(config)# nat (any, any) static 10.2.2.2
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

다음 예에서는 NAT와 전역 액세스 제어 정책이 어떻게 연동하는지 보여줍니다. 이 예에서는 호스트 10.1.1.1에서 호스트 192.168.0.0으로의 HTTP 연결 하나를 허용하고 호스트 209.165.200.225에서 호스트 172.16.0.0으로의 또다른 HTTP 연결을 허용하되 호스트 10.1.1.1에서 호스트 172.16.0.0으로의 HTTP 연결은 거부합니다.

```
ciscoasa(config)# object network 10.1.1.1 host 10.1.1.1
ciscoasa(config)# object network 172.16.0.0 host 172.16.0.0
ciscoasa(config)# object network 192.168.0.0 host 192.168.0.0
ciscoasa(config)# nat (inside, any) source static 10.1.1.1 10.1.1.1 destination static
                  192.168.0.0 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip object 10.1.1.1 object 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip host 209.165.200.225 object 172.16.0.0
ciscoasa(config)# access-list global_acl deny ip any 172.16.0.0
ciscoasa(config)# access-group global_acl global
```

관련 명령

명령	설명
access-list extended	확장 ACL을 만듭니다.
clear configure access-group	모든 인터페이스에서 액세스 그룹을 제거합니다.
show running-config access-group	인터페이스에 바인딩된 현재 ACL을 표시합니다.

access-list alert-interval

거부 흐름 최대 메시지의 시간 간격을 지정하려면 글로벌 컨피그레이션 모드에서 **access-list alert-interval** 명령을 사용합니다. 기본 설정으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

access-list alert-interval *secs*

no access-list alert-interval

구문 설명

secs	거부 흐름 최대 메시지를 생성하는 시간 간격입니다. 1초~3600초의 범위에서 선택합니다. 기본값은 300초입니다.

기본값

기본값은 300초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ACL 거부 구문에서 **log** 옵션을 구성할 경우 트래픽 흐름이 ACL 구문과 매칭하면 어플라이언스는 그 흐름 정보를 캐시에 저장합니다. 캐시 과부하를 방지하기 위해 캐시에 저장되는 거부 흐름의 최대 개수가 설정되며, 이 정보는 syslog 메시지 106100에 표시되는 통계를 위해 보존됩니다. 106100이 실행되기 전에 최대 개수에 도달하여 캐시가 재설정되면 syslog 메시지 106101이 실행되어 거부 흐름 최대값을 초과했음을 알립니다.

access-list alert-interval 명령은 syslog 메시지 106101을 생성하기 위한 시간 간격을 설정합니다. 거부 흐름 최대값에 도달하면 또 다른 syslog 메시지 106101이 생성됩니다. 단, 마지막 syslog 메시지 106101이 생성된 후 *secs*초 이상 경과했어야 합니다.

거부 흐름 최대값 메시지 생성에 대한 자세한 내용은 **access-list deny-flow-max** 명령을 참조하십시오.

예

다음 예에서는 거부 흐름 최대값 메시지의 시간 간격을 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list alert-interval 30
```

관련 명령

명령	설명
access-list deny-flow-max	생성 가능한 동시 거부 흐름의 최대 개수를 지정합니다.
access-list extended	컨피그레이션에 ACL을 추가하며, ASA를 지나는 IP 트래픽에 대한 정책을 구성하는 데 쓰입니다.
clear access-group	ACL 카운터를 지웁니다.
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACL 엔트리를 숫자로 표시합니다.

access-list deny-flow-max

메시지 106100을 위한 통계치를 계산하기 위해 캐시에 저장할 수 있는 동시 거부 흐름의 최대 개수를 지정하려면 글로벌 컨피그레이션 모드에서 **access-list deny-flow-max** 명령을 사용합니다. 기본 설정으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

access-list deny-flow-max *number*

no access-list deny-flow-max *number*

구문 설명

number	메시지 106100을 위한 통계치를 계산하기 위해 캐시에 저장할 거부 흐름의 최대 개수이며, 범위는 1~4096입니다. 기본값은 4096입니다.

기본값

기본값은 4096입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서 캐시에 저장된 거부 흐름의 최대 개수에 도달하면 syslog 메시지 106101이 생성됩니다.

예

다음 예에서는 캐시에 저장할 수 있는 동시 거부 흐름의 최대 개수를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list deny-flow-max 256
```

관련 명령

명령	설명
access-list alert-interval	메시지 106101의 실행 간격을 설정합니다.
access-list extended	컨피그레이션에 ACL을 추가하며, ASA를 지나는 IP 트래픽에 대한 정책을 구성하는 데 쓰입니다.
clear access-group	ACL 카운터를 지웁니다.
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACL 엔트리를 숫자로 표시합니다.
show running-config access-list	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

access-list ethertype

이더 타입에 따라 트래픽을 제어하는 ACL을 구성하려면 글로벌 컨피그레이션 모드에서 **access-list ethertype** 명령을 사용합니다. ACL을 제거하려면 이 명령의 **no** 형식을 사용합니다.

access-list *id* **ethertype {deny | permit} {ipx | isis | bpdu | mpls-unicast | mpls-multicast | any | *hex_number*}**

no access-list *id* **ethertype {deny | permit} {ipx | isis | bpdu | mpls-unicast | mpls-multicast | any | *hex_number*}**

구문 설명

any	모든 트래픽을 허용하거나 거부합니다.
bpdu	브리지 프로토콜 데이터 유닛을 허용하거나 거부합니다.
deny	트래픽을 거부합니다.
hex_number	특정 이더 타입의 트래픽을 허용하거나 거부합니다. 이 이더 타입은 0x600 이상의 16비트 16진수로 지정됩니다.
id	ACL의 이름 또는 번호를 지정합니다.
ipx	IPX를 허용하거나 거부합니다.
isis	IS-IS(Intermediate System to Intermediate System)를 허용하거나 거부합니다.
mpls-multicast	MPLS 멀티캐스트를 허용하거나 거부합니다.
mpls-unicast	MPLS 유니캐스트를 허용하거나 거부합니다.
permit	트래픽을 허용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.4(5), 9.1(2)	**isis** 키워드를 추가했습니다.

사용 지침

이더 타입 ACL은 이더 타입을 지정하는 하나 이상의 ACE(액세스 제어 항목)로 구성됩니다. 이더 타입 규칙은 16비트 16진수로 식별되는 임의의 이더 타입 및 선택된 트래픽 유형을 제어합니다.

참고 이더 타입 ACL의 경우 ACL 끝의 암시적 거부는 IP 또는 ARP에 영향을 미치지 않습니다. 예를 들어 이더 타입 8037을 허용하는 경우 ACL 끝의 암시적 거부는 전에 확장 ACL로 허용한(또는 높은 보안 인터페이스에서 낮은 보안 인터페이스로 암시적으로 허용한) IP 트래픽을 차단하지 않습니다. 그러나 어떤 이더 타입 ACE로 모든 트래픽을 명시적으로 거부할 경우, IP 및 ARP 트래픽이 거부됩니다. 자동 협상과 같은 물리적 프로토콜 트래픽만 계속 허용됩니다.

지원되는 이더 타입 및 기타 트래픽

이더 타입 규칙은 다음을 제어합니다.

- 공통 유형 IPX 및 MPLS 유니캐스트 또는 멀티캐스트를 포함하여 16비트 16진수로 식별되는 이더 타입.
- 이더넷 V2 프레임.
- 기본적으로 허용되는 BPDU. BPDU는 SNAP 캡슐화되며, ASA는 BPDU를 처리하도록 설계되었습니다.
- 트렁크 포트(Cisco 독점) BPDU. 트렁크 BPDU는 페이로드 내에 VLAN 정보가 있습니다. 따라서 BPDU를 허용하면 ASA는 발신 VLAN으로 페이로드를 수정합니다.
- IS-IS(Intermediate System to Intermediate System).

다음의 트래픽 유형은 지원되지 않습니다.

- 802.3 형식의 프레임 - 이러한 프레임은 유형 필드와 반대되는 길이 필드를 사용하므로 규칙에 의해 처리되지 않습니다.

반환 트래픽의 액세스 규칙

이더 타입은 연결이 없으므로, 트래픽이 양방향을 통과하도록 하려면 두 인터페이스에 규칙을 적용해야 합니다.

MPLS 허용

MPLS를 허용할 경우 LDP(Label Distribution Protocol) 및 TDP(Tag Distribution Protocol) TCP 연결이 ASA를 통해 설정되게 해야 합니다. 이를 위해 ASA에 연결된 MPLS 라우터가 ASA 인터페이스의 IP 주소를 LDP 또는 TDP 세션의 라우터 ID로 사용하도록 구성합니다 (LDP 및 TDP에서는 MPLS 라우터가 패킷 전달에 사용되는 레이블(주소)을 협상할 수 있습니다.).

Cisco IOS 라우터에서 프로토콜 LDP 또는 TDP에 맞는 적절한 명령을 입력하십시오. 이 인터페이스는 ASA에 연결된 인터페이스입니다.

```
ciscoasa(config)# mpls ldp router-id interface force
```

또는

```
ciscoasa(config)# tag-switching tdp router-id interface force
```

예

다음 예에서는 이더 타입 ACL을 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

관련 명령

명령	설명
access-group	ACL을 인터페이스에 바인딩합니다.
clear access-group	ACL 카운터를 지웁니다.
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACL 엔트리를 숫자로 표시합니다.
show running-config access-list	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

access-list extended

확장 ACL에 ACE를 추가하려면 글로벌 컨피그레이션 모드에서 **access-list extended** 명령을 사용합니다. ACE를 제거하려면 이 명령의 **no** 형식을 사용합니다.

임의의 트래픽 유형 , 포트 없음 :

access-list *access_list_name* [**line** *line_number*] **extended {deny | permit}** *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended {deny | permit}** *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

TCP 또는 UDP 트래픽 , 포트 있음 :

access-list *access_list_name* [**line** *line_number*] **extended {deny | permit} {tcp | udp}** [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended {deny | permit} {tcp | udp}** [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

ICMP 트래픽 , ICMP 유형 :

access-list *access_list_name* [**line** *line_number*] **extended {deny | permit}** **{icmp | icmp6}**[*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended {deny | permit} {icmp | icmp6}** [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

구문 설명

access_list_name	ACL ID를 최대 241자의 문자열 또는 정수로 지정합니다. ID는 대/소문자를 구분합니다. 팁 컨피그레이션에서 ACL ID 를 쉽게 알아볼 수 있도록 모두 대문자를 사용합니다 .
deny	조건에 매칭할 경우 패킷을 거부합니다. 네트워크 액세스의 경우(**access-group** 명령) 이 키워드는 패킷이 ASA를 통과하지 못하게 합니다. 클래스 맵에 애플리케이션 검사를 적용하는 경우(**class-map** 및 **inspect** 명령) 이 키워드는 트래픽을 검사에서 제외합니다. 일부 기능에서는 거부 ACE를 사용할 수 없습니다. 자세한 내용은 ACL을 사용하는 각 기능에 대한 명령 설명서를 참조하십시오.
dest_address_argument	패킷 목적지의 IP 주소 또는 FQDN을 지정합니다. 이용 가능한 인수는 다음과 같습니다. • **host** *ip_address*—IPv4 호스트 주소를 지정합니다. • *ip_address mask* - IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다. 네트워크 마스크를 지정할 때의 방식은 Cisco IOS 소프트웨어 **access-list** 명령과 다릅니다. ASA에서는 네트워크 마스크(예: 클래스 C 마스크는 255.255.255.0)를 사용합니다. Cisco IOS 마스크는 와일드카드 비트(예: 0.0.0.255)를 사용합니다. • *ipv6-address/prefix-length* - IPv6 호스트 또는 네트워크 주소 및 접두사를 지정합니다. • **any**, **any4**, **any6**—**any**는 IPv4 트래픽과 IPv6 트래픽을 모두 지정합니다. **any4**는 IPv4 트래픽만, **any6**는 IPv6 트래픽만 지정합니다. • **interface** *interface_name*—ASA 인터페이스의 이름을 지정합니다. 어떤 인터페이스가 트래픽의 소스 또는 목적지인가에 따라 트래픽에 매칭하도록 IP 주소보다 인터페이스 이름을 사용합니다. 트래픽 소스가 디바이스 인터페이스일 경우 ACL에서 실제 IP 주소 대신 인터페이스 키워드를 지정해야 합니다. 예를 들어, ISAKMP를 차단하여 특정 원격 IP 주소에서 ASA와의 VPN 세션을 시작할 수 없게 하는 데 이 옵션을 사용할 수 있습니다. 소스 또는 목적지가 ASA 자체인 임의의 트래픽에 대해서는 **access-group** 명령을 **control-plane** 키워드와 함께 사용해야 합니다. • **object** *nw_obj_id*—**object network** 명령으로 생성된 네트워크 객체를 지정합니다. • **object-group** *nw_grp_id*—**object-group network** 명령으로 생성된 네트워크 객체 그룹을 지정합니다.
icmp_argument	(선택 사항) ICMP 유형 및 코드를 지정합니다. • *icmp_type* [*icmp_code*]—ICMP 유형을 이름 또는 번호로 지정하며, 선택 사항으로 그 유형에 대한 ICMP 코드를 지정합니다. 코드를 지정하지 않을 경우 모든 코드가 사용됩니다. • **object-group** *icmp_grp_id*—**object-group service** 또는 (더 이상 사용되지 않지만) **object-group icmp** 명령으로 생성된 ICMP/ICMP6용 객체 그룹을 지정합니다.
inactive	(선택 사항) ACE를 비활성화합니다. 다시 활성화하려면 **inactive** 키워드 없이 전체 ACE를 입력합니다. 이 기능으로 컨피그레이션에 비활성 ACE의 레코드를 유지하여 더 손쉽게 다시 활성화할 수 있습니다.

line *line-num*	(선택 사항) ACE를 삽입할 지점의 라인 번호를 지정합니다. 라인 번호를 지정하지 않을 경우 ACE는 ACL의 끝에 추가됩니다. 라인 번호는 컨피그레이션에 저장되지 않으며 ACE를 삽입할 위치만 지정합니다.
log [[*level*] [**interval** *secs*] | **disable** | **default**]	(선택 사항) ACE가 네트워크 액세스를 위해 패킷에 매칭할 때의 로깅 옵션을 설정합니다(**access-group** 명령으로 적용되는 ACL). 인수 없이 **log** 키워드를 입력할 경우 시스템 로그 메시지 106100을 기본 레벨(6)과 기본 간격(300초)으로 활성화합니다. **log** 키워드를 입력하지 않으면, 거부된 패킷에 대해 기본 시스템 로그 메시지 106023이 생성됩니다. 로그 옵션은 다음과 같습니다. • *level*—0부터 7까지의 심각도. 기본값은 6(참조용)입니다. 활성 ACE에 대해 이 레벨을 변경할 경우 새로운 레벨은 신규 연결에 적용됩니다. 기존 연결은 계속 예전의 레벨에서 로깅됩니다. • **interval** *secs*—syslog 메시지의 시간 간격(초)이며 1부터 600까지입니다. 기본값은 300입니다. 이 값은 폐기 통계 수집에 쓰이는 캐시에서 비활성 흐름을 삭제하기 위한 시간 초과 값으로도 사용됩니다. • **disable**—모든 ACE 로깅을 비활성화합니다. • **default**—메시지 106023 로깅을 활성화합니다. 이 설정은 **log** 옵션을 포함하지 않는 것과 같습니다.
permit	조건에 매칭할 경우 패킷을 허용합니다. 네트워크 액세스의 경우(**access-group** 명령) 이 키워드는 패킷이 ASA를 통과하게 합니다. 클래스 맵에 애플리케이션 검사를 적용하는 경우(**class-map** 및 **inspect** 명령) 이 키워드는 패킷에 검사를 적용합니다.
port_argument	(선택 사항) 프로토콜을 TCP 또는 UDP로 설정할 경우 소스 또는 목적지 포트를 지정합니다. 포트를 지정하지 않을 경우 모든 포트가 매칭됩니다. 이용 가능한 인수는 다음과 같습니다. • *operator port*—*operator*는 다음 중 하나일 수 있습니다. – **lt**—보다 작음 – **gt**—보다 큼 – **eq**—같음 – **neq**—같지 않음 – **range**—경계를 포함하는 값 범위. 이 연산자를 사용할 때는 예를 들면 다음과 같이 두 개의 포트 번호를 지정합니다. `range 100 200` *port*는 TCP 또는 UDP 포트의 번호(정수)이거나 이름일 수 있습니다. DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, Talk 각각에서 TCP를 위한 정의와 UDP를 위한 정의가 하나씩 필요합니다. TACACS+는 TCP의 포트 49에서 하나의 정의가 필요합니다. • **object** *service_obj_id*—**object service** 명령으로 생성된 서비스 객체를 지정합니다. • **object-group** *service_grp_id*—**object-group service** 명령으로 생성된 서비스 객체 그룹을 지정합니다.

protocol_argument	IP 프로토콜을 지정합니다. 이용 가능한 인수는 다음과 같습니다. • *name* 또는 *number*—프로토콜 이름 또는 번호를 지정합니다. 즉 UDP는 17, TCP는 6, EGP는 47입니다. 모든 프로토콜에 적용하려면 **ip**라고 지정합니다. 이용 가능한 옵션에 대해서는 CLI 도움말을 참조하십시오. • **object-group** *protocol_grp_id*—**object-group protocol** 명령으로 생성된 프로토콜 객체 그룹을 지정합니다. • **object** *service_obj_id*—**object service** 명령으로 생성된 서비스 객체를 지정합니다. TCP, UDP 또는 ICMP 서비스 객체는 프로토콜, 소스 및/또는 목적지 포트 또는 ICMP 유형과 코드를 포함할 수 있습니다. 이는 ACE에 트래픽을 매칭할 때 사용됩니다. ACE에서 포트/유형을 각각 구성할 필요는 없습니다. • **object-group** *service_grp_id*—**object-group service** 명령으로 생성된 서비스 객체 그룹을 지정합니다.
security_group_argument	TrustSec 기능과 함께 사용할 경우 소스 또는 수신 주소 외에 트래픽을 매칭할 보안 그룹을 지정합니다. 이용 가능한 인수는 다음과 같습니다. • **object-group-security** *security_obj_grp_id*—**object-group security** 명령으로 생성되는 보안 객체 그룹을 지정합니다. • **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*}—보안 그룹 이름 또는 태그를 지정합니다.
source_address_argument	패킷 소스의 IP 주소 또는 FQDN을 지정합니다. 이용 가능한 인수는 *dest_address_argument*와 동일합니다.
tcp	프로토콜을 TCP로 설정합니다.
time-range *time_range_name*	(선택 사항) 시간 범위 객체를 지정합니다. 이는 하루 중 언제, 무슨 요일에 ACE가 활성 상태인지 결정합니다. 시간 범위를 지정하지 않을 경우 ACE는 항상 활성 상태입니다. 시간 범위 정의에 대한 자세한 내용은 **time-range** 명령을 참조하십시오.
udp	프로토콜을 UDP로 설정합니다.
user_argument	ID 방화벽 기능과 함께 사용할 경우 소스 주소 외에 트래픽을 매칭할 사용자 또는 그룹을 지정합니다. 이용 가능한 인수는 다음과 같습니다. • **object-group-user** *user_obj_grp_id*—**object-group user** 명령으로 생성된 사용자 객체 그룹을 지정합니다. • **user** {[*domain_nickname*\\]*name* | **any** | **none**}—사용자 이름을 지정합니다. 사용자 자격 증명이 있는 모든 사용자에 매칭하려면 **any**를, 사용자 이름에 매핑되지 않은 주소에 매칭하려면 **none**을 지정합니다. 이 옵션은 **access-group** 정책과 **aaa authentication match** 정책을 연계할 때 특히 유용합니다. • **user-group** [*domain_nickname*\\\\]*user_group_name*—사용자 그룹 이름을 지정합니다. 이중 \\는 도메인과 그룹 이름을 구분합니다.

기본값

- 거부 ACE에 대한 기본 로깅에서는 거부된 패킷에 대해서만 시스템 로그 메시지 106023을 생성합니다.
- **log** 키워드가 지정될 경우 시스템 로그 메시지 106100의 기본 레벨이 6(참조용), 기본 간격은 300초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.3(1)	NAT 또는 PAT를 사용할 경우, 일부 기능의 ACL에서 매핑된 주소 및 포트가 더 이상 필요하지 않습니다. 이러한 기능에는 변환되지 않은 실제 주소와 포트를 사용해야 합니다. 실제 주소와 포트를 사용할 경우 NAT 컨피그레이션이 바뀌더라도 ACL을 변경할 필요 없습니다. 자세한 내용은 "실제 IP 주소를 사용하는 기능" 페이지의 섹션 1-72를 참조하십시오.
8.4(2)	소스 및 목적지에 소스 또는 목적지 IP 주소 외에 ID 방화벽 사용자와 그룹도 사용할 수 있습니다. 소스 및 목적지에 **user**, **user-group**, **object-group-user**를 추가로 지원합니다.
9.0(1)	소스 및 목적지에 소스 또는 목적지 IP 주소 외에 TrustSec 보안 그룹도 사용할 수 있습니다. 소스 또는 목적지에 **security-group** 및 **object-group-security**를 추가로 지원합니다.
9.0(1)	IPv6 지원을 추가했습니다. **any** 키워드가 IPv4 및 IPv6 트래픽을 나타내도록 변경되었습니다. IPv4 전용 및 IPv6 전용 트래픽을 나타내도록 **any4** 및 **any6** 키워드가 추가되었습니다. 소스 및 목적지에 IPv4 주소와 IPv6 주소를 혼합하여 지정할 수 있습니다. NAT를 사용하여 IPv4와 IPv6를 변환할 경우, 실제 패킷은 IPv4 주소와 IPv6 주소의 혼합을 포함하지 않습니다. 그러나 상당수의 기능에서 ACL은 실제 IP 주소만 사용하며 NAT 매핑 주소를 고려하지 않습니다. IPv6 전용 ACL은 사용되지 않습니다. 기존의 IPv6 ACL은 확장 ACL로 마이그레이션됩니다. 마이그레이션에 대한 자세한 내용은 릴리스 정보를 참조하십시오. ACL 마이그레이션에 대한 자세한 내용은 9.0 릴리스 정보를 참조하십시오.
9.0(1)	ICMP 코드 지원을 추가했습니다. **icmp**를 프로토콜로 지정하면 *icmp_type* [*icmp_code*]를 입력합니다.

사용 지침

ACL은 동일한 ACL ID를 갖는 하나 이상의 ACE로 구성됩니다. 네트워크 액세스를 제어하거나 여러 기능이 실행될 트래픽을 지정하는 데 ACL을 사용합니다. 어떤 ACL 이름에 대해 입력하는 각 ACE는 ACE에 라인 번호가 지정되지 않는 한 ACL의 끝에 추가됩니다. 전체 ACL을 제거하려면 **clear configure access-list** 명령을 사용합니다.

ACE 의 순서

ACE의 순서는 중요합니다. ASA에서 패킷을 전달할지 아니면 폐기할지 결정할 때 ASA는 각 ACE에 대해, 각 항목이 나열된 순서에 따라 패킷을 테스트합니다. 일치가 발견되면 ACE가 더 이상 점검되지 않습니다. 예를 들어, ACL의 시작 부분에 모든 트래픽을 명시적으로 허용하는 ACE를 만들면 다른 내용은 점검되지 않습니다.

실제 IP 주소를 사용하는 기능

다음 명령과 기능에서는 ACL에 실제 IP 주소를 사용합니다.

- **access-group** 명령
- Modular Policy Framework **match access-list** 명령
- Botnet Traffic Filter **dynamic-filter enable classify-list** 명령
- AAA **aaa ... match** 명령
- WCCP **wccp redirect-list group-list** 명령

매핑된 IP 주소를 사용하는 기능

다음 기능에서 ACL을 사용하는데, 이 ACL에서는 인터페이스에 나타나는 매핑된 값을 사용합니다.

- IPsec ACL
- **capture** 명령 ACL
- 사용자별 ACL
- 라우팅 프로토콜 ACL
- 다른 모든 기능의 ACL

ID 방화벽 , FQDN, TrustSec ACL 을 지원하지 않는 기능

다음 기능에서는 ACL을 사용하지만 ID 방화벽(사용자 또는 그룹 이름 지정), FQDN(정규화된 도메인 이름) 또는 TrustSec 값을 갖는 ACL을 허용할 수 없습니다.

- **route-map** 명령
- VPN **crypto map** 명령
- VPN **group-policy** 명령(**vpn-filter** 제외)
- WCCP
- DAP

예

다음 ACL은 (ACL을 적용하는 인터페이스의) 모든 호스트가 ASA를 지나는 것을 허용합니다.

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

다음 예의 ACL은 192.168.1.0/24의 호스트가 209.165.201.0/27 네트워크에 액세스할 수 없게 합니다. 다른 모든 주소는 허용됩니다.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

일부 호스트만 액세스할 수 있도록 제한하려면 제한 **허용 ACE**를 입력합니다. 기본적으로 다른 모든 트래픽은 명시적으로 허용되지 않는 한 거부됩니다.

```
ciscoasa(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

다음 ACL은 (ACL을 적용하는 인터페이스의) 모든 호스트가 주소 209.165.201.29의 웹 사이트에 액세스할 수 없게 합니다. 다른 모든 트래픽은 허용됩니다.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

객체 그룹을 사용하는 다음 ACL은 내부 네트워크의 일부 호스트가 일부 웹 서버에 액세스할 수 없게 합니다. 다른 모든 트래픽은 허용됩니다.

```
ciscoasa(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

한 네트워크 객체 그룹(A)에서 다른 네트워크 객체 그룹(B)으로 가는 트래픽을 허용하는 ACL을 일시적으로 비활성화하려면

```
ciscoasa(config)# access-list 104 permit ip host object-group A object-group B inactive
```

시간 기준 ACL를 구현하려면 **time-range** 명령을 사용하여 구체적인 요일과 시간대를 정의합니다. 그런 다음 **access-list extended** 명령을 사용하여 시간 범위를 ACL에 바인딩합니다. 다음 예에서는 "Sales"라는 ACL을 "New_York_Minute"라는 시간 범위에 바인딩합니다.

```
ciscoasa(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

시간 범위를 정의하는 방법에 대한 자세한 내용은 **time-range** 명령을 참조하십시오.

다음 ACL은 임의의 ICMP 트래픽을 허용합니다.

```
ciscoasa(config)# access-list abc extended permit icmp any any
```

다음 ACL은 객체 그룹 "obj_icmp_1"에 대해 임의의 ICMP 트래픽을 허용합니다.

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

다음 ACL은 소스 호스트 10.0.0.0에서 목적지 호스트 10.1.1.1로 보내는 ICMP 유형 3 및 ICMP 코드 4인 ICMP 트래픽을 허용합니다. 다른 모든 ICMP 트래픽 유형은 허용되지 않습니다.

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3 4
```

다음 ACL은 소스 호스트 10.0.0.0에서 목적지 호스트 10.1.1.1로 보내는 ICMP 유형 3 및 임의의 ICMP 코드를 갖는 ICMP 트래픽을 허용합니다. 다른 모든 ICMP 트래픽 유형은 허용되지 않습니다.

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3
```

관련 명령

명령	설명
access-group	ACL을 인터페이스에 바인딩합니다.
clear access-group	ACL 카운터를 지웁니다.
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACE를 숫자로 표시합니다.
show running-config access-list	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

access-list remark

확장 이더 타입 또는 표준 ACE의 앞이나 뒤에 추가할 설명의 텍스트를 지정하려면 글로벌 컨피그레이션 모드에서 **access-list remark** 명령을 사용합니다. 설명을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

access-list *id* **[line** *line-num***] remark** *text*

no access-list *id* **[line** *line-num***] remark** *text*

구문 설명

id	ACL의 이름입니다.
line *line-num*	(선택 사항) 설명을 삽입할 지점의 라인 번호입니다.
remark text	설명의 텍스트입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

설명 텍스트는 공백이 아닌 문자를 하나 이상 포함해야 합니다. 빈 설명은 허용되지 않습니다. 설명 텍스트는 공백과 구두점을 포함하여 최대 100자입니다.

설명만 있는 ACL에 대해 **access-group** 명령을 사용할 수 없습니다.

예

다음 예에서는 ACL의 끝에 설명 텍스트를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list MY_ACL remark checklist
```

관련 명령

명령	설명
access-list extended	컨피그레이션에 ACL을 추가하며, ASA를 지나는 IP 트래픽에 대한 정책을 구성하는 데 쓰입니다.
clear access-group	ACL 카운터를 지웁니다.
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACL 엔트리를 숫자로 표시합니다.
show running-config access-list	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

access-list rename

ACL의 이름을 변경하려면 글로벌 컨피그레이션 모드에서 **access-list rename** 명령을 사용합니다.

access-list *id* **rename** *new_acl_id*

구문 설명

id	기존 ACL의 이름입니다.
rename *new_acl_id*	새 ACL ID를 최대 241자의 문자열 또는 정수로 지정합니다. ID는 대/소문자를 구분합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ACL이 동일한 이름으로 변경되면 ASA는 자동으로 명령을 무시합니다.

예

다음 예에서는 ACL의 이름을 TEST에서 OUTSIDE로 변경하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list TEST rename OUTSIDE
```

관련 명령

명령	설명
access-list extended	컨피그레이션에 ACL을 추가하며, ASA를 지나는 IP 트래픽에 대한 정책을 구성하는 데 쓰입니다.
clear access-group	ACL 카운터를 지웁니다.
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACL 엔트리를 숫자로 표시합니다.
show running-config access-list	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

access-list standard

표준 ACL에 ACE를 추가하려면 글로벌 컨피그레이션 모드에서 **access-list standard** 명령을 사용합니다. ACE를 제거하려면 이 명령의 **no** 형식을 사용합니다.

access-list *id* **standard {deny | permit} {any4 | host** *ip_address* **|** *ip_address subnet_mask***}**

no access-list *id* **standard {deny | permit} {any4 | host** *ip_address* **|** *ip_address subnet_mask***}**

구문 설명

any4	임의의 IPv4 주소와 매칭합니다.
deny	조건에 매칭할 경우 패킷을 거부하거나 제외합니다.
host *ip_address*	IPv4 호스트 주소(즉 서브넷 마스크는 255.255.255.255)를 지정합니다.
id	ACL의 이름 또는 번호입니다.
ip_address subnet_mask	IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다.
permit	조건에 매칭할 경우 패킷을 허용하거나 포함합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

표준 ACL은 동일한 ACL ID 또는 이름을 갖는 모든 ACE로 구성됩니다. 표준 ACL은 경로 맵, VPN 필터 등 몇몇 기능에 사용됩니다. 표준 ACL에서는 IPv4 주소만 사용하며, 수신 주소만 정의합니다.

예

다음 예에서는 표준 ACL에 규칙을 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

관련 명령

명령	설명
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACL 엔트리를 숫자로 표시합니다.
show running-config access-list	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

access-list webtype

클라이언트리스 SSL VPN 연결을 필터링하는 웹 타입 ACL에 ACE를 추가하려면 글로벌 컨피그레이션 모드에서 **access-list webtype** 명령을 사용합니다. ACE을 제거하려면 이 명령의 **no** 형식을 사용합니다.

access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} **[log [[***level***] [interval** *secs***] | disable | default]] [time_range** *name***] [inactive]**

no access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} **[log [[***level***] [interval** *secs***] | disable | default]] [time_range** *name***] [inactive]**

access-list *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* **[***operator port***] [log [[***level***] [interval** *secs***] | disable | default]] [time_range** *name***] [inactive]**

no access-list *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* **[***operator port***] [log [[***level***] [interval** *secs***] | disable | default]] [time_range** *name***] [inactive]**

구문 설명

deny	조건에 매칭하면 액세스를 거부합니다.
dest_address_argument	패킷 목적지의 IP 주소를 지정합니다. 수신 주소 옵션은 다음과 같습니다. • **host** *ip_address*—IPv4 호스트 주소를 지정합니다. • *dest_ip_address mask*—IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다(예: 10.100.10.0 255.255.255.0). • *ipv6-address/prefix-length* - IPv6 호스트 또는 네트워크 주소 및 접두사를 지정합니다. • **any**, **any4**, **any6**—**any**는 IPv4 트래픽과 IPv6 트래픽을 모두 지정합니다. **any4**는 IPv4 트래픽만, **any6**는 IPv6 트래픽만 지정합니다.
id	ACL의 이름 또는 번호를 지정합니다.
inactive	(선택 사항) ACE를 비활성화합니다. 다시 활성화하려면 **inactive** 키워드 없이 전체 ACE를 입력합니다. 이 기능으로 컨피그레이션에 비활성 ACE의 레코드를 유지하여 더 손쉽게 다시 활성화할 수 있습니다.
log [[*level*] [**interval** *secs*] | **disable** | **default**]	(선택 사항) ACE가 패킷과 매칭할 때의 로깅 옵션을 설정합니다. 인수 없이 **log** 키워드를 입력할 경우 VPN 필터 시스템 로그 메시지 106102를 기본 레벨(6)과 기본 간격(300초)으로 활성화합니다. **log** 키워드를 입력하지 않으면, 기본 VPN 필터 시스템 로그 메시지 106103이 생성됩니다. 로그 옵션은 다음과 같습니다. • *level*—0부터 7까지의 심각도. 기본값은 6(참조용)입니다. • **interval** *secs*—syslog 메시지의 시간 간격(초)이며 1부터 600까지입니다. 기본값은 300입니다. 이 값은 폐기 통계 수집에 쓰이는 캐시에서 비활성 흐름을 삭제하기 위한 시간 초과 값으로도 사용됩니다. • **disable**—모든 ACE 로깅을 비활성화합니다. • **default**—메시지 106103 로깅을 활성화합니다. 이 설정은 **log** 옵션을 포함하지 않는 것과 같습니다.

operator port	(선택 사항) **tcp**를 지정하면 목적지 포트입니다. 포트를 지정하지 않을 경우 모든 포트가 매칭됩니다. *operator*는 다음 중 하나일 수 있습니다. • **lt**—보다 작음 • **gt**—보다 큼 • **eq**—같음 • **neq**—같지 않음 • **range**—경계를 포함하는 값 범위. 이 연산자를 사용할 때는 예를 들면 다음과 같이 두 개의 포트 번호를 지정합니다. `range 100 200` *port*는 TCP 포트의 번호(정수)이거나 이름일 수 있습니다.
permit	조건에 매칭하면 액세스를 허용합니다.
time_range *name*	(선택 사항) 시간 범위 객체를 지정합니다. 이는 하루 중 언제, 무슨 요일에 ACE가 활성 상태인지 결정합니다. 시간 범위를 지정하지 않을 경우 ACE는 항상 활성 상태입니다. 시간 범위 정의에 대한 자세한 내용은 **time-range** 명령을 참조하십시오.
url {*url_string* | **any**}	매칭할 URL을 지정합니다. 모든 URL 기준 트래픽에 매칭하려면 **url any**를 사용합니다. 그러지 않으면 URL 문자열을 입력하며, 와일드카드를 넣을 수 있습니다. URL 문자열에 대한 팁은 사용 지침을 참조하십시오.

기본값

기본 설정은 다음과 같습니다.

- ACL 로깅에서는 거부된 패킷에 대해 syslog 메시지 106103을 생성합니다.
- 선택적 **log** 키워드를 지정할 경우 syslog 메시지 106102의 기본 레벨은 6(참조용)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

access-list webtype 명령은 클라이언트리스 SSL VPN 필터링을 구성하는 데 사용합니다.

다음은 URL 지정에 관한 팁과 제한 사항입니다.

모든 URL에 매칭하려면 **any**를 선택합니다.

- 'Permit url any'은 protocol://server-ip/path 형식의 모든 URL을 허용하며, port-forwarding과 같이 이 패턴과 일치하지 않은 트래픽은 차단합니다. 암시적 거부가 일어나지 않도록 필요한 포트(Citrix의 경우 포트 1494)와의 연결을 허용하는 ACE가 있어야 합니다.
- 스마트 터널과 ica plug-in인 'permit url any' ACL의 영향을 받지 않습니다. mart-tunnel:// and ica:// 유형에만 매칭하기 때문입니다.
- cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel://, and smtp:// 프로토콜을 사용할 수 있습니다. 또한 프로토콜에 와일드카드를 사용할 수 있습니다. 예를 들어, htt*는 http 및 https에, 별표 *는 모든 프로토콜에 매칭됩니다. 예를 들어, *://*.example.com은 example.com 네트워크로 가는 모든 유형의 URL 기준 트래픽에 매칭합니다.
- smart-tunnel:// URL을 지정할 경우 서버 이름만 포함할 수 있습니다. URL은 경로를 포함할 수 없습니다. 예를 들어, smart-tunnel://www.example.com은 허용되지만, smart-tunnel://www.example.com/index.html은 허용되지 않습니다.
- 별표 *는 무엇과도 매칭하지 않거나 임의의 문자 수에 매칭합니다. 모든 http URL에 매칭하려면 http://*/*를 입력합니다.
- 물음표 ?는 임의의 한 문자에만 매칭합니다.
- 대괄호 []는 범위 연산자로서 해당 범위에 속한 모든 문자에 매칭합니다. 예를 들어, http://www.cisco.com:80/와 http://www.cisco.com:81/ 모두에 매칭하려면 **http://www.cisco.com:8[01]/**를 입력합니다.

예

다음 예는 특정 회사 URL에 대한 액세스를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

다음 예는 특정 웹 페이지에 대한 액세스를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

다음 예는 포트 8080을 지나는, 특정 서버에 있는 임의의 URL에 대한 HTTP 액세스를 거부하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

관련 명령

명령	설명
clear configure access-list	실행 중인 컨피그레이션에서 ACL을 지웁니다.
show access-list	ACL 엔트리를 숫자로 표시합니다.
show running-config access-list	ASA에서 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

accounting-mode

어카운팅 메시지가 단일 서버에 보내지는지(단일 모드) 또는 그룹의 모든 서버에 보내지는지(동시 모드) 지정하려면 aaa-server 컨피그레이션 모드에서 **accounting-mode** 명령을 사용합니다. 어카운팅 모드 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

accounting-mode {simultaneous | single}

구문 설명

simultaneous	그룹의 모든 서버에 어카운팅 메시지를 전송합니다.
single	단일 서버에 어카운팅 메시지를 전송합니다.

기본값

기본값은 single mode입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

단일 서버에 어카운팅 메시지를 보내려면 **single** 키워드를 사용합니다. 서버 그룹의 모든 서버에 어카운팅 메시지를 보내려면 **simultaneous** 키워드를 사용합니다.

이 명령은 서버 그룹이 어카운팅에 사용되는 경우(RADIUS 또는 TACACS+)에만 의미가 있습니다.

예

다음 예에서는 그룹의 모든 서버에 어카운팅 메시지를 보내는 데 **accounting-mode** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
aaa accounting	어카운팅 서비스를 활성화하거나 비활성화합니다.
aaa-server protocol	AAA 서버 그룹 컨피그레이션 모드를 시작합니다. 그러면 그룹의 모든 호스트에 공통적으로 적용되는, 그룹에 특화된 AAA 서버 매개변수를 구성할 수 있습니다.
clear configure aaa-server	모든 AAA 서버 컨피그레이션을 제거합니다.
show running-config aaa-server	특정 서버 그룹, 특정 그룹에 속한 특정 서버 또는 특정 프로토콜에 대해 모든 AAA 서버의 AAA 서버 통계를 표시합니다.

accounting-port

이 호스트의 RADIUS 어카운팅에 사용할 포트 번호를 지정하려면 aaa-server 호스트 컨피그레이션 모드에서 **accounting-port** 명령을 사용합니다. 인증 포트 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

accounting-port *port*

no accounting-port

구문 설명

port	RADIUS 어카운팅을 위한 포트 번호이며, 범위는 1~65535입니다.

기본값

기본적으로 디바이스는 어카운팅을 위해 포트 1646에서 RADIUS를 수신합니다(RFC 2058 규격). 포트가 지정되지 않으면 RADIUS 어카운팅의 기본 포트 번호(1646)가 사용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 어카운팅 레코드를 보낼 원격 RADIUS 서버 호스트의 목적지 TCP/UDP 포트 번호를 지정합니다. RADIUS 어카운팅 서버에서 1646이 아닌 포트를 사용할 경우, RADIUS 서비스를 시작하기에 앞서 **aaa-server** 명령을 사용하여 ASA에서 알맞은 포트를 구성합니다.

이 명령은 RADIUS를 위해 구성된 서버 그룹에서만 유효합니다.

예

다음 예에서는 호스트 "1.2.3.4"에서 "srvgrp1"이라는 RADIUS AAA 서버를 구성하고 시간 초과를 9초로, 재시도 간격을 7초로 설정하고 어카운팅 포트 2222를 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-interval 7
ciscoasa(config-aaa-server-host)# accountinq-port 2222
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
aaa accounting	사용자가 어떤 네트워크 서비스에 액세스했는가에 대한 기록을 유지합니다.
aaa-server host	AAA 서버 호스트 컨피그레이션 모드를 시작합니다. 그러면 호스트에 특화된 AAA 서버 매개변수를 구성할 수 있습니다.
clear configure aaa-server	모든 AAA 명령문을 컨피그레이션에서 제거합니다.
show running-config aaa-server	특정 서버 그룹, 특정 그룹에 속한 특정 서버 또는 특정 프로토콜에 대해 모든 AAA 서버의 AAA 서버 통계를 표시합니다.

accounting-server-group

어카운팅 레코드를 보내기 위해 AAA 서버 그룹을 지정하려면 여러 모드에서 **accounting-server-group** 명령을 사용합니다. 어카운팅 서버를 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

accounting-server-group *group_tag*

no accounting-server-group [*group_tag*]

구문 설명

group_tag	이미 구성된 어카운팅 서버 또는 서버 그룹을 식별합니다. 어카운팅 서버를 구성하려면 **aaa-server** 명령을 사용합니다.

기본값

기본적으로 어떤 어카운팅 서버도 구성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Imap4s 컨피그레이션	• 예	—	• 예	—	—
Pop3s 컨피그레이션	• 예	—	• 예	—	—
Smtps 컨피그레이션	• 예	—	• 예	—	—
Tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—
config-mdm-proxy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	이 명령은 webvpn 컨피그레이션 모드가 아닌 tunnel-group general-attributes 컨피그레이션 모드에서만 사용 가능합니다.
9.3(1)	이 명령은 config-mdm-proxy 모드에서만 사용 가능합니다.

사용 지침

ASA에서는 사용자가 액세스하는 네트워크 리소스를 추적하기 위해 어카운팅을 사용합니다. webvpn 컨피그레이션 모드에서 이 명령을 입력하면 tunnel-group general-attributes 컨피그레이션 모드의 동일한 명령으로 변환됩니다.

예

tunnel-group-general attributes 컨피그레이션 모드에서 입력된 다음 예에서는 IPSec LAN-to-LAN 터널 그룹 "xyz"를 위해 "aaa-server123"이라는 어카운팅 서버 그룹을 구성합니다.

```
ciscoasa(config)# tunnel-group xyz type IPSec_L2L
ciscoasa(config)# tunnel-group xyz general-attributes
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)#
```

다음 예에서는 POP3SSVRS라는 어카운팅 서버 집합을 사용하기 위해 POP3S 이메일 프록시를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# accounting-server-group POP3SSVRS
```

다음 예에서는 MDM Proxy 어카운팅 서버 그룹을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# accounting-server-group MDMSVRGRP
```

관련 명령

명령	설명
aaa-server	인증, 권한 부여, 어카운팅 서버를 구성합니다.

2 장

acl-netmask-convert ~ application-access hide-details 명령

acl-netmask-convert

ASA에서 **aaa-server host** 명령을 통해 액세스하는 RADIUS 서버로부터 받은 다운로드 가능 ACL의 넷마스크를 처리하는 방법을 지정하려면 aa-server 호스트 컨피그레이션 모드에서 **acl-netmask-convert** 명령을 사용합니다. ASA에 대해 지정된 동작을 제거하려면 이 명령의 **no** 형식을 사용합니다.

acl-netmask-convert {auto-detect | standard | wildcard}

no acl-netmask-convert

구문 설명

auto-detect	ASA에서 사용된 넷마스크 표현의 유형을 확인하도록 지정합니다. ASA에서 와일드카드 넷마스크 표현을 발견하면 이를 표준 넷마스크 표현으로 변환합니다. 이 키워드에 대한 자세한 내용은 "사용 지침"을 참조하십시오.
standard	ASA에서 RADIUS 서버로부터 받은 다운로드 가능 ACL이 표준 넷마스크 표현만 포함하는 것으로 가정하도록 지정합니다. 와일드카드 넷마스크 표현에 대한 변환이 이루어지지 않습니다.
wildcard	ASA에서 RADIUS 서버로부터 받은 다운로드 가능 ACL이 와일드카드 넷마스크 표현만 포함한다고 가정하고 ACL를 다운로드할 때 모두 표준 넷마스크 표현으로 변환하도록 지정합니다.

기본값

기본적으로 와일드카드 넷마스크 표현으로부터의 변환이 일어나지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(4)	이 명령을 도입했습니다.

사용 지침

RADIUS 서버가 와일드카드 형식의 넷마스크를 포함한 다운로드 가능 ACL을 제공할 때 wildcard 또는 auto-detect 키워드와 함께 **acl-netmask-convert** 명령을 사용합니다. ASA는 다운로드 가능 ACL이 표준 넷마스크 표현을 포함할 것으로 예상하지만, Cisco VPN 3000 시리즈의 집선 장치는 다운로드 가능 ACL이 표준 넷마스크 표현의 정반대인 와일드카드 넷마스크 표현을 포함할 것으로 예상합니다. 와일드카드 넷마스크는 무시할 비트 위치에 1이, 매칭할 비트 위치에 0이 있습니다. **acl-netmask-convert** 명령을 사용하면 이와 같이 RADIUS 서버에서 다운로드 가능 ACL을 구성하는 방법의 차이에 따른 효과를 최소화할 수 있습니다.

auto-detect 키워드는 RADIUS 서버가 어떻게 구성되었는지 잘 모를 때 유용합니다. 그러나 "홀(hole)"이 있는 와일드카드 넷마스크 표현은 명확하게 감지하여 변환할 수 없습니다. 예를 들어, 와일드카드 넷마스크 0.0.255.0은 3번째 옥텟에서 어떤 것도 허용하며 Cisco VPN 3000 시리즈 집선 장치에서 유효하게 사용될 수 있으나, ASA는 이 표현을 와일드카드 넷마스크로 감지하지 않을 수 있습니다.

예

다음 예에서는 호스트 "192.168.3.4"에 "srvgrp1"이라는 RADIUS AAA 서버를 구성하고 다운로드 가능 ACL 넷마스크의 변환을 활성화하며 시간 초과를 9초로, 재시도 간격을 7초로 설정하고 인증 포트 1650을 구성합니다.

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
aaa authentication	**aaa-server** 명령에 의해 또는 ASDM 사용자 인증에 의해 지정된 서버에서 LOCAL, TACACS+ 또는 RADIUS 사용자 인증을 활성화하거나 비활성화합니다.
aaa-server host	AAA 서버 호스트 컨피그레이션 모드를 시작합니다. 그러면 호스트에 특화된 AAA 서버 매개변수를 구성할 수 있습니다.
clear configure aaa-server	모든 AAA 명령문을 컨피그레이션에서 제거합니다.
show running-config aaa-server	특정 서버 그룹, 특정 그룹에 속한 특정 서버 또는 특정 프로토콜에 대해 모든 AAA 서버의 AAA 서버 통계를 표시합니다.

action

세션에 액세스 정책을 적용하거나 세션을 종료하려면 dynamic-access-policy-record 컨피그레이션 모드에서 **action** 명령을 사용합니다. 세션에 액세스 정책을 적용하기 위해 세션을 재설정하려면 이 명령의 **no** 형식을 사용합니다.

action {continue | terminate}

no action {continue | terminate}

구문 설명

continue	세션에 액세스 정책을 적용합니다.
terminate	연결을 종료합니다.

기본값

기본값은 continue입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Dynamic-access-policy-record 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

선택된 모든 DAP 레코드에서 세션에 액세스 정책을 적용하려면 **continue** 키워드를 사용합니다. 선택된 임의의 DAP 레코드에서 연결을 종료하려면 **terminate** 키워드를 사용합니다.

예

다음 예에서는 DAP 정책인 Finance에 대해 세션을 종료하는 방법을 보여줍니다.

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# action terminate
ciscoasa(config-dynamic-access-policy-record)#
```

관련 명령

명령	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
show running-config dynamic-access-policy-record [*name*]	모든 DAP 레코드 또는 명명된 DAP 레코드에 대해 실행 중인 컨피그레이션을 표시합니다.

action cli command

이벤트 관리자 애플릿에 대한 작업을 구성하려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **action cli command** 명령을 사용합니다. 구성된 작업을 제거하려면 **no action** *n* 명령을 입력합니다.

action *n* **cli command** "*command*"

no action *n*

구문 설명

"*command*"	명령의 이름을 지정합니다. *command* 옵션의 값은 따옴표로 감싸야 합니다. 이렇게 하지 않으면 명령이 여러 개의 단어로 이루어진 경우 오류가 발생합니다. 명령은 글로벌 컨피그레이션 모드에서 권한 수준이 15(가장 높음)인 사용자 권한으로 실행됩니다. 명령은 비활성화되어 있으므로 입력을 승인하지 않습니다. 명령에 사용 가능한 **noconfirm** 옵션이 있는 경우 이 옵션을 사용합니다.
n	작업 ID를 지정합니다. 유효한 ID 범위는 0~42947295입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

이벤트 관리자 애플릿에 대한 작업을 구성할 때 이 명령을 사용합니다.

예

다음 예에서는 이벤트 관리자 애플릿에 대한 작업을 구성하는 방법을 보여줍니다.

```
hostname (config-applet)# action 1 cli command "show version"
```

관련 명령

명령	설명
description	애플릿에 대해 설명합니다.
event manager run	이벤트 관리자 애플릿을 실행합니다.
show event manager	구성된 각 이벤트 관리자 애플릿에 대한 통계 정보를 표시합니다.
debug event manager	이벤트 관리자를 위한 디버깅 추적을 관리합니다.

action-uri

SSO(single sign-on) 인증을 위한 사용자 이름과 비밀번호를 받기 위해 웹 서버 URI를 지정하려면 aaa-server-host 컨피그레이션 모드에서 **action-uri** 명령을 사용합니다. URI 매개변수 값을 재설정하려면 이 명령의 **no** 형식을 사용합니다.

action-uri *string*

no action-uri

참고 HTTP 프로토콜을 사용하여 SSO를 올바르게 구성하려면 인증 및 HTTP 프로토콜 교환에 대해 잘 알고 있어야 합니다.

구문 설명

string	인증 프로그램의 URI. 여러 행으로 입력할 수 있습니다. 각 행의 최대 길이는 255자입니다. 전체 URI의 최대 길이는 2048자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

이는 HTTP Forms 명령을 사용하는 SSO입니다. URI(Uniform Resource Identifier)는 인터넷에서 어떤 콘텐츠 지점을 식별하는 짧은 문자열로서 이는 텍스트 페이지, 비디오 또는 사운드 클립, 정지 영상 또는 동영상, 소프트웨어 프로그램일 수 있습니다. 가장 일반적인 URI 형식은 웹 페이지 주소로서 이는 특정 형식이거나 URL이라고 부르는 URI의 하위 집합입니다.

ASA의 WebVPN 서버는 인증 웹 서버에 SSO 인증 요청을 보내는 데 POST 요청을 사용할 수 있습니다. 그러기 위해서는 ASA에서 HTTP POST 요청을 통해 인증 웹 서버의 작업 URI에 사용자 이름과 비밀번호를 전달하도록 구성합니다. **action-uri** 명령은 ASA에서 POST 요청을 보내는 웹 서버에 있는 인증 프로그램의 위치와 이름을 지정합니다.

브라우저에서 곧바로 웹 서버 로그인 페이지에 연결하여 인증 웹 서버의 작업 URI를 찾을 수 있습니다. 브라우저에 표시되는 로그인 웹 페이지의 URL은 인증 웹 서버의 작업 URI입니다.

입력의 편의성을 위해 연속적인 여러 행에 URI를 입력할 수 있습니다. 그러면 ASA는 그 행을 연결하여 사용자가 입력한 URI로 만듭니다. action-uri 행별 최대 길이는 255자이지만 각 행에서 더 짧게 입력할 수 있습니다.

참고 문자열에 물음표가 있으면 그 앞에 Ctrl+v 이스케이프 시퀀스가 와야 합니다.

예

다음 예에서는 www.example.com의 URI를 지정합니다.

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
ciscoasa(config)# aaa-server testgrp1 host www.example.com
ciscoasa(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
ciscoasa(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
ciscoasa(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
ciscoasa(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
ciscoasa(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
ciscoasa(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
ciscoasa(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
ciscoasa(config-aaa-server-host)# action-uri %2Fauth.example.com
ciscoasa(config-aaa-server-host)#
```

참고 작업 URI에 호스트 이름과 프로토콜을 포함해야 합니다. 앞의 예에서는 URI 시작 부분에서 http://www.example.com에 포함되어 있습니다.

관련 명령

명령	설명
auth-cookie-name	인증 쿠키의 이름을 지정합니다.
hidden-parameter	SSO 서버와의 교환을 위해 숨겨진 매개변수를 만듭니다.
password-parameter	SSO 인증을 위해 사용자 비밀번호를 전송해야 하는 HTTP POST 요청 매개변수의 이름을 지정합니다.
start-url	로그인 전 쿠키를 검색할 URL을 지정합니다.
user-parameter	SSO 인증을 위해 사용자 이름을 전송해야 하는 HTTP POST 요청 매개변수의 이름을 지정합니다.

activation-key

ASA에 라이센스 활성화 키를 입력하려면 특별 권한 EXEC 모드에서 **activation-key** 명령을 사용합니다.

activation-key [noconfirm] *activation_key* **[activate | deactivate]**

구문 설명

activate	기간별 활성화 키를 활성화합니다. **activate**가 기본값입니다. 지정된 기능에 활성화한 최종 기간별 키가 활성화 상태의 키입니다.
activation_key	ASA에 활성화 키를 적용합니다. *activation_key* 키는 5개 요소로 된 16진수 문자열이며 각 요소 사이에 하나의 공백이 있습니다. 맨 앞의 0x 지정자는 선택 사항이며, 모든 값은 16진수로 가정합니다. 하나의 영구 키를 설치하고, 여러 개의 기간별 키를 설치할 수 있습니다. 새 영구 키를 입력하면 이전에 설치한 키를 덮어씁니다.
deactivate	기간별 활성화 키를 비활성화합니다. 활성화 키를 비활성화하면 이 키는 ASA에 계속 설치되어 있으며, 나중에 **activate** 키워드를 사용하여 활성화할 수 있습니다. 키를 처음 입력하고 **deactivate**를 지정하면 ASA에 설치된 키가 비활성 상태가 됩니다.
noconfirm	(선택 사항) 확인 프롬프트 없이 활성화 키를 입력합니다.

기본값

기본적으로 ASA에는 라이센스가 이미 설치된 상태로 배송됩니다. 이러한 라이센스는 원하는 라이센스를 더 추가할 수 있는 Base 라이센스일 수 있습니다. 또는 주문 내역 및 공급업체에서 설치한 내역에 따라 모든 라이센스가 이미 설치되어 있을 수 있습니다. 어떤 라이센스가 설치되었는지 확인하려면 **show activation-key** 명령을 참조하십시오.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(5)	다음 한도를 높였습니다. • ASA5510 Base 라이센스 연결이 32000에서 5000으로 증가하고, VLAN이 0에서 10으로 증가 • ASA5510 Security Plus 라이센스 연결이 64000에서 130000으로 증가하고, VLAN이 10에서 25으로 증가 • ASA5520 연결이 130000에서 280000으로 증가하고, VLAN이 25에서 100으로 증가 • ASA5540 연결이 280000에서 400000으로 증가하고, VLAN이 100에서 200으로 증가
7.1(1)	SSL VPN 라이센스가 도입되었습니다.
7.2(1)	ASA 5550 이상 버전에 5000-사용자 SSL VPN 라이센스가 도입되었습니다.
7.2(2)	• ASA 5505 ASA Security Plus 라이센스의 VLAN 최대 개수를 5개(3개는 전 기능, 1개는 장애 조치, 1개는 백업 인터페이스에 한정)에서 20개 전 기능 인터페이스로 늘렸습니다. 또한 트렁크 포트 수도 1개에서 8개로 늘렸습니다. • ASA 5510의 VLAN 한도도 늘어났습니다. Base 라이센스는 10개에서 50개로, Security Plus 라이센스는 25개에서 100개로 늘어났습니다. ASA 5520은 100개에서 150개로, ASA 5550은 200개에서 250개로 늘어났습니다.
7.2(3)	ASA 5510 Security Plus License는 포트 0과 포트 1에서 GE(기가비트 이더넷)를 지원합니다. Base License를 Security Plus License로 업그레이드할 경우 외부 Ethernet0/0 및 Ethernet0/1 포트의 용량이 원래의 FE(패스트 이더넷)(100Mbps)에서 GE(1000Mbps)로 증가합니다. 인터페이스 이름은 그대로 Ethernet 0/0 및 Ethernet 0/1입니다. **speed** 명령을 사용하여 인터페이스의 속도를 변경하고, **show interface** 명령을 사용하여 각 인터페이스에 현재 구성된 속도를 확인합니다.
8.0(2)	• Advanced Endpoint Assessment 라이센스가 도입되었습니다. • ASA 5510 Security Plus에서 VPN 로드 밸런싱이 지원됩니다.
8.0(3)	AnyConnect for Mobile 라이센스가 도입되었습니다.
8.0(4)/8.1(2)	기간별 라이센스에 대한 지원이 도입되었습니다.
8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
8.0(4)	The UC Proxy Sessions 라이센스가 도입되었습니다.
8.2(1)	• Botnet Traffic Filter 라이센스가 도입되었습니다. • AnyConnect Essentials 라이센스가 도입되었습니다. 기본적으로 ASA에서는 AnyConnect Essentials 라이센스를 사용하지만, **no anyconnect-essentials** 명령을 사용하여 이를 비활성화하고 다른 라이센스를 사용할 수도 있습니다. • SSL VPN용 공유 라이센스가 도입되었습니다.
8.2(2)	Mobility Proxy에 UC Proxy 라이센스가 더 이상 필요하지 않습니다.

릴리스	수정 사항
8.3(1)	• 각 유닛의 장애 조치 라이센스가 더 이상 동일하지 않아도 됩니다. 두 유닛에 사용되는 라이센스는 기본 및 보조 유닛에서 통합된 라이센스입니다. • 기간별 라이센스는 스태킹이 가능합니다. • IME 라이센스가 도입되었습니다. • 여러 기간별 라이센스를 설치할 수 있으며, 기능당 라이센스는 한 번에 하나만 활성화할 수 있습니다. • **activate** 또는 **deactivate** 키워드를 사용하여 기간별 라이센스를 활성화하거나 비활성화할 수 있습니다.
8.4(1)	• SSP-10이 포함된 ASA 5550 및 ASA 5585-X의 경우, 컨텍스트 최대 개수가 50개에서 100개로 늘어났습니다. SSP-20 이상이 포함된 ASA 5580 및 5585-X의 경우 최대 개수가 50개에서 250개으로 늘어났습니다. • ASA 5580 및 5585-X의 VLAN 최대 개수가 250개에서 1024개로 늘어났습니다. • 다음과 같이 방화벽 연결 한도를 증가하였습니다. – ASA 5580-20—1,000K에서 2,000K로 – ASA 5580-40—2,000K에서 4,000K로 – ASA 5585-X(SSP-10 포함): 750K에서 1,000K로 – ASA 5585-X(SSP-20포함): 1,000K에서 2,000K로 – ASA 5585-X(SSP-40포함): 2,000K에서 4,000K로 – ASA 5585-X(SSP-60포함): 2,000K에서 10,000K로 • ASA 5580에서 AnyConnect VPN 세션 한도가 5,000에서 10,000으로 늘어났습니다. • ASA 5580에서 그밖의 VPN 세션 한도가 5,000에서 10,000으로 늘어났습니다. • IKEv2를 사용하는 IPsec 원격 액세스 VPN이 AnyConnect Essentials 및 AnyConnect Premium 라이센스에 추가되었습니다. • 사이트 대 사이트 세션이 다른 VPN 라이센스에 추가되었습니다(이전의 IPsec VPN). • No Payload Encryption이 제공되는 모델(예: ASA 5585-X)의 경우, ASA를 특정 국가에 수출하기 위해 ASA 소프트웨어에서는 Unified Communications 및 VPN 기능을 비활성화합니다.

사용 지침

활성화 키 얻기

활성화 키를 얻으려면 Cisco 어카운트 담당자를 통해 구매할 수 있는 제품 승인 키가 필요합니다. 각 기능 라이센스에 별도의 제품 활성화 키를 구매해야 합니다. 예를 들어, Base 라이센스를 보유한 경우 Advanced Endpoint Assessment 및 추가 SSL VPN 세션에 대한 별도의 키를 구매할 수 있습니다.

제품 승인 키를 받고 다음 URL 중 하나를 통해 Cisco.com에 등록합니다.

- Cisco.com에 등록된 사용자라면 다음 웹 사이트를 방문합니다.
  http://www.cisco.com/go/license
- Cisco.com에 등록된 사용자가 아니라면 다음 웹 사이트를 방문합니다.
  http://www.cisco.com/go/license/public

컨텍스트 모드 지침

- 다중 컨텍스트 모드의 경우 시스템 실행 영역에서 활성화 키를 적용합니다.
- 공유 라이센스는 다중 컨텍스트 모드에서 지원되지 않습니다.

장애 조치 지침

- 공유 라이센스는 액티브/액티브 모드에서 지원되지 않습니다.
- 장애 조치 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다.

  이전 버전의 ASA 소프트웨어에는 각 유닛과 일치하는 라이센스가 필요했습니다. 버전 8.3(1)부터는 더 이상 동일한 라이센스를 설치하지 않아도 됩니다. 일반적으로 기본 유닛에만 라이센스를 구매하며, 액티브/스탠바이 장애 조치가 이루어질 경우 보조 유닛이 액티브 유닛이 되면 보조 유닛에서 기본 라이센스를 상속합니다. 두 유닛에 모두 라이센스가 있는 경우, 해당 라이센스는 실행 중인 단일 장애 조치 클러스터 라이센스로 통합됩니다.
- ASA 5505 및 5510은 둘 다 Security Plus 라이센스가 필요합니다. Base 라이센스는 장애 조치를 지원하지 않으므로 Base 라이센스만 있는 스탠바이 유닛에서는 장애 조치를 활성화할 수 없습니다.

업그레이드 및 다운그레이드 지침

임의의 이전 버전에서 최신 버전으로 업그레이드할 경우 활성화 키는 계속 호환 가능합니다. 그러나 다운그레이드 기능을 유지하려는 경우 문제가 생길 수 있습니다.

- 버전 8.1 이하로 다운그레이드 — 업그레이드 후 *8.2 이전에* 도입된 추가 기능 라이센스를 활성화할 경우, 다운그레이드를 수행하면 활성화 키가 이전 버전과 계속 호환됩니다. 그러나 *8.2 이상* 버전에 도입된 기능 라이센스를 활성화할 경우에는 활성화 키가 이전 버전과 호환되지 않습니다. 호환되지 않는 라이센스 키가 있을 경우 다음 지침을 참조하십시오.
  - 기존에 이전 버전에서 활성화 키를 입력한 경우 ASA에서 해당 키를 사용합니다(버전 8.2 이상에서 활성화된 새 라이센스 없음).
  - 새 시스템이 있으나 이전 활성화 키가 없는 경우, 이전 버전과 호환되는 새 활성화 키를 요청해야 합니다.
- 버전 8.2 이하로 다운그레이드 — 버전 8.3에는 더욱 강력한 기간별 키 용도 및 장애 조치 라이센스 변경 사항이 도입되었습니다.
  - 둘 이상의 시간 기준 활성화 키가 활성 상태일 경우, 다운그레이드하면 가장 최근에 활성화된 시간 기준 키만 활성 상태가 됩니다. 그 밖의 모든 키는 비활성 상태가 됩니다.
  - 장애 조치 쌍에 일치하지 않는 라이센스가 있을 경우 다운그레이드를 수행하면 장애 조치가 비활성화됩니다. 키가 일치하더라도 사용된 라이센스는 더 이상 통합 라이센스가 아닙니다.

추가 지침 및 제한

- 활성화 키는 컨피그레이션 파일에 저장되지 않으며, 플래시 메모리에 숨겨진 파일로 저장됩니다.
- 활성화 키는 디바이스의 일련 번호와 연결되어 있습니다. 기능 라이센스는 디바이스 간에 이동할 수 없습니다(하드웨어 오류가 발생한 경우는 예외). 하드웨어 오류로 인해 디바이스를 교체해야 하는 경우, Cisco Licensing Team에 문의하여 기존 라이센스를 새 일련 번호에 보낼 수 있습니다. Cisco Licensing Team에서는 제품 승인 키 참조 번호와 기존 일련 번호를 요청합니다.
- 구매한 후에는 환불 또는 라이센스 업그레이드를 위해 라이센스를 반환할 수 없습니다.
- 모든 라이센스 유형을 활성화할 수 있으나 일부 기능, 이를테면 다중 컨텍스트 모드와 VPN은 상호 호환되지 않습니다. AnyConnect Essentials 라이센스의 경우 전체 SSL VPN 라이센스, 공유 SSL VPN 라이센스, Advanced Endpoint Assessment 라이센스와 호환되지 않습니다. 기본적으로 AnyConnect Essentials 라이센스가 위 라이센스 대신 사용되지만, **no anyconnect-essentials** 명령을 사용하여 컨피그레이션에서 AnyConnect Essentials 라이센스를 비활성화한 다음 다른 라이센스의 사용을 복원할 수 있습니다.
- 일부 영구 라이센스의 경우 활성화 후 ASA를 다시 로드해야 합니다. 표 2-1에는 다시 로드해야 하는 라이센스가 나열되어 있습니다.

표 2-1 영구 라이센스 다시 로드 요구 사항

모델	다시 로드해야 하는 라이센스 작업
ASA 5505, ASA 5510	Base 라이센스와 Security Plus 라이센스 간 교체
모든 모델	Encryption 라이센스 교체
모든 모델	영구 라이센스 다운그레이드(예: 컨텍스트 10개에서 컨텍스트 2개로)

예

다음 예에서는 ASA에서 활성화 키를 변경하는 방법을 보여줍니다.

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

다음은 **activation-key** 명령의 샘플 출력으로서 새 활성화 키가 기존 활성화 키와 다를 경우 일어나는 장애 조치의 출력을 보여줍니다.

```
ciscoasa# activation-key 0xyadayada 0xyadayada 0xyadayada 0xyadayada 0xyadayada

Validating activation key. This may take a few minutes...
The following features available in the running permanent activation key are NOT available
in the new activation key:
Failover is different.
   running permanent activation key: Restricted (R)
   new activation key: Unrestricted (UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with updating flash activation key? [y]
Flash permanent activation key was updated with the requested key.
```

다음은 라이센스 파일의 샘플 출력입니다.

```
Serial Number Entered: 123456789ja
Number of Virtual Firewalls Selected: 10
Formula One device: ASA 5520

Failover                       : Enabled
VPN-DES                        : Enabled
VPN-3DES-AES                   : Enabled
Security Contexts              : 10
```

```
GTP/GPRS                        : Disabled
SSL VPN Peers                   : Default
Total VPN Peers                 : 750
Advanced Endpoint Assessment    : Disabled
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Disabled
Shared License                  : Disabled
UC Phone Proxy Sessions         : Default
Total UC Proxy Sessions         : Default
AnyConnect Essentials           : Disabled
Botnet Traffic Filter           : Disabled
Intercompany Media Engine       : Enabled

----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ASA SOFTWARE RELEASE 8.2+ ONLY.

Platform = asa

123456789JA:yadayda1 yadayda1 yadayda1 yadayda1 yadayda1
----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ALL ASA SOFTWARE RELEASES, BUT EXCLUDES ANY
8.2+ FEATURES FOR BACKWARDS COMPATIBILITY.

Platform = asa

123456789JA:yadayda2 yadayda2 yadayda2 yadayda2 yadayda2
```

관련 명령

명령	설명
anyconnect-essentials	Anyconnect Essentials 라이센스를 활성화하거나 비활성화합니다.
show activation-key	활성화 키를 표시합니다.
show version	소프트웨어 버전 및 활성화 키를 표시합니다.

activex-relay

클라이언트리스 포털에서 ActiveX를 필요로 하는 애플리케이션을 통합하려면 group-policy webvpn 컨피그레이션 모드 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **activex-relay** 명령을 사용합니다. 기본 그룹 정책에서 **activex-relay** 명령을 상속하려면 이 명령의 **no** 형식을 사용합니다.

activex-relay {enable | disable}

no activex-relay

구문 설명

enable	WebVPN 세션에서 ActiveX를 활성화합니다.
disable	WebVPN 세션에서 ActiveX를 비활성화합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Group-policy webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

사용자가 객체 태그가 있는 HTML 콘텐츠(예: 이미지, 오디오, 비디오, JAVA 애플릿, ActiveX, PDF, 플래시)를 위해 WebVPN 브라우저에서 ActiveX를 실행할 수 있게 하려면 **activex-relay enable** 명령을 사용합니다. 이러한 애플리케이션에서는 WebVPN 세션을 사용하여 ActiveX 컨트롤을 다운로드하고 업로드합니다. ActiveX 릴레이는 WebVPN 세션이 종료할 때까지 계속 작동합니다. Microsoft OWA 2007과 같은 제품을 사용하려면 ActiveX를 비활성화해야 합니다.

참고 서로 동일한 기능을 제공하므로 **activex-relay enable** 명령은 스마트 터널이 비활성화되더라도 스마트 터널 로그를 생성합니다.

다음 예에서는 어떤 그룹 정책과 연결된 WebVPN 세션에서 ActiveX 컨트롤을 활성화합니다.

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# activex-relay enable
```

다음 예에서는 어떤 사용자 이름과 연결된 WebVPN 세션에서 ActiveX 컨트롤을 비활성화합니다.

```
ciscoasa(config-username-policy)# webvpn
ciscoasa(config-username-webvpn)# activex-relay disable
```

ad-agent-mode

Cisco Identify Firewall 인스턴스에 대해 AD 에이전트(Active Directory 에이전트)를 구성할 수 있도록 AD 에이전트 모드를 활성화하려면 글로벌 컨피그레이션 모드에서 **ad-agent-mode** 명령을 사용합니다.

ad-agent-mode

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

ID 방화벽을 위한 AD 에이전트를 구성하려면 **ad-agent-mode** 명령을 입력해야 합니다. 이는 **aaa-server** 명령의 하위 모드입니다. **ad-agent-mode** 명령을 입력하면 aaa 서버 그룹 컨피그레이션 모드가 시작합니다.

AD 에이전트는 정기적으로 또는 온디맨드로 WMI를 통해 Active Directory 서버 보안 이벤트 로그 파일을 모니터링하면서 사용자 로그인 및 로그오프 이벤트를 확인합니다. AD 에이전트는 사용자 ID 및 IP 주소 매핑의 캐시를 유지합니다. 그리고 ASA에 변경 사항을 알립니다.

AD 에이전트 서버 그룹을 위해 기본 및 보조 AD 에이전트를 구성합니다. ASA에서 기본 AD 에이전트가 응답하지 않음을 탐지한 경우, 보조 에이전트가 지정되어 있다면 ASA는 보조 AD 에이전트로 전환합니다. AD 에이전트의 AD 서버는 RADIUS를 통신 프로토콜로 사용합니다. 따라서 ASA와 AD 에이전트의 공유 암호에 대한 키 특성을 지정해야 합니다.

예

다음 예에서는 ID 방화벽을 위해 AD 에이전트를 구성하면서 **ad-agent-mode**를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server adagent protocol radius
ciscoasa(config)# ad-agent-mode
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
ciscoasa(config-aaa-server-host)# key mysecret
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

관련 명령

명령	설명
aaa-server	AAA 서버 그룹을 만들고 그룹 특정 및 모든 그룹 호스트 공통 AAA 서버 매개변수를 구성합니다.
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

address(dynamic-filter 블랙리스트 또는 화이트리스트)

봇넷 트래픽 필터 블랙리스트 또는 화이트리스트에 IP 주소를 추가하려면 dynamic-filter 블랙리스트 또는 화이트리스트 컨피그레이션 모드에서 **address** 명령을 사용합니다. 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

address *ip_address mask*

no address *ip_address mask*

구문 설명

ip_address	블랙리스트에 IP 주소를 추가합니다.
mask	IP 주소에 대한 서브넷 마스크를 정의합니다. *mask*는 단일 호스트 또는 서브넷의 마스크가 될 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
dynamic-filter 블랙리스트 또는 화이트리스트컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

고정 데이터베이스를 사용하면 화이트리스트 또는 블랙리스트에 넣을 도메인 이름 또는 IP 주소를 동적 데이터베이스에 보충할 수 있습니다. dynamic-filter 화이트리스트 또는 블랙리스트 컨피그레이션 모드를 시작한 다음 **address** 및 **name** 명령을 사용하여 화이트리스트에 정상으로 표시하거나 블랙리스트에 악성으로 표시할 도메인 이름 또는 IP 주소(호스트 또는 서브넷)를 직접 입력할 수 있습니다.

여러 엔트리를 위해 이 명령을 여러 번 입력할 수 있습니다. 최대 1,000개의 블랙리스트 및 1,000개의 화이트리스트 엔트리를 추가할 수 있습니다.

예

다음 예에서는 블랙리스트 및 화이트리스트의 엔트리를 생성합니다.

```
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
clear configure dynamic-filter	실행 중인 봇넷 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇넷 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇넷 트래픽 필터 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter blacklist	봇넷 트래픽 필터 블랙리스트를 수정합니다.
dynamic-filter database fetch	봇넷 트래픽 필터 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇넷 트래픽 필터 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter enable	어떤 트래픽 클래스에 대해 또는 액세스 목록을 지정하지 않았다면 모든 트래픽에 대해 봇넷 트래픽 필터를 활성화합니다.
dynamic-filter updater-client enable	동적 데이터베이스의 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스의 사용을 활성화합니다.
dynamic-filter whitelist	봇넷 트래픽 필터 화이트리스트를 수정합니다.
inspect dns dynamic-filter-snoop	봇넷 트래픽 필터 스누핑과 함께 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇넷 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇넷 트래픽 필터로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매칭하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	봇넷 트래픽 필터의 실행 중인 컨피그레이션을 표시합니다.

address(media-termination)

전화 프록시 기능과의 미디어 연결에 사용할 미디어 종료 인스턴스의 주소를 지정하려면 미디어 종료 컨피그레이션 모드에서 **address** 명령을 사용합니다. 미디어 종료 컨피그레이션에서 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

address *ip_address* [**interface** *intf_name*]

no address *ip_address* [**interface** *intf_name*]

구문 설명

interface *intf_name*	미디어 종료 주소가 사용되는 인터페이스의 이름을 지정합니다. 인스턴스당 하나의 미디어 종료 주소만 구성할 수 있습니다.
ip_address	미디어 종료 인스턴스에 사용할 IP 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
미디어 종료 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

ASA는 다음 기준에 부합하는 미디어 종료용 IP 주소가 있어야 합니다.

- 미디어 종료 인스턴스를 위해 모든 인터페이스에 대한 전역 미디어 종료 주소를 구성하거나 서로 다른 인터페이스의 미디어 종료 주소를 구성할 수 있습니다. 그러나 전역 미디어 종료 주소와 각 인터페이스에 대해 구성된 미디어 종료 주소를 동시에 사용할 수는 없습니다.
- 여러 인터페이스에 대해 하나의 미디어 종료 주소를 구성할 경우 각 인터페이스에서 ASA가 IP 전화기와 통신할 때 사용할 주소를 구성해야 합니다.
- 이 IP 주소는 공개적으로 라우팅 가능한 주소로서 해당 인터페이스의 주소 범위에 속하는 미사용 IP 주소입니다.

미디어 종료 인스턴스를 만들고 미디어 종료 주소를 구성할 때 따라야 할 전제 조건의 전체 목록은 CLI 컨피그레이션 가이드를 참조하십시오.

예

다음 예에서는 미디어 연결에 사용할 IP 주소를 지정하기 위해 미디어 종료 주소 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# media-termination mediaterm1
ciscoasa(config-media-termination)# address 192.0.2.25 interface inside
ciscoasa(config-media-termination)# address 10.10.0.25 interface outside
```

관련 명령

명령	설명
phone-proxy	전화 프록시 인스턴스를 구성합니다.
media-termination	전화 프록시 인스턴스에 적용할 미디어 종료 인스턴스를 구성합니다.

address-family ipv4

표준 IPv4(IP Version 4) 주소 접두사를 사용하는 라우팅 세션을 구성하기 위해 주소군을 입력하려면 라우터 컨피그레이션 모드에서 **address-family ipv4** 명령을 사용합니다. 주소군 컨피그레이션 모드를 종료하고 실행 중인 컨피그레이션에서 IPv4 주소군 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

address-family ipv4

no address-family ipv4

기본값

IPv4 주소 접두사는 활성화되어 있지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

address-family ipv4 명령은 컨텍스트 라우터를 주소군 컨피그레이션 모드에 놓습니다. 여기서 표준 IPv4 주소 접두사를 사용하는 라우팅 세션을 구성할 수 있습니다. 주소군 컨피그레이션 모드를 종료하고 라우터 컨피그레이션 모드로 돌아가려면 **exit**를 입력합니다.

참고 기본적으로 **neighbor remote-as** 명령으로 구성된 각 BGP 라우팅 세션에는 주소군 IPv4에 대한 라우팅 정보가 광고됩니다. 단 **neighbor remote-as** 명령을 구성하기 전에 **no bgp default ipv4-unicast** 명령을 입력한 경우는 제외합니다.

예

다음 예에서는 라우터를 IPv4 주소군을 위한 주소군 컨피그레이션 모드에 놓습니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)#
```

관련 명령

명령	설명
bgp default ipv4-unicast	IPv4 유니캐스트 주소군을 BGP 피어링 세션의 기본값으로 설정합니다.
neighbor remote-as	BGP 또는 다중 프로토콜 BGP 네이버 테이블에 엔트리를 추가합니다.

address-pool(tunnel-group general attributes mode)

원격 클라이언트에 주소를 할당하기 위해 주소 풀의 목록을 지정하려면 tunnel-group general-attributes 컨피그레이션 모드에서 **address-pool** 명령을 사용합니다. 주소 풀을 제거하려면 이 명령의 **no** 형식을 사용합니다.

address-pool [(*interface name*)**]** *address_pool1* **[...***address_pool6***]**

no address-pool [(*interface name*)**]** *address_pool1* **[...***address_pool6***]**

구문 설명

address_pool	**ip local pool** 명령으로 구성된 주소 풀의 이름을 지정합니다. 최대 6개의 로컬 주소 풀을 지정할 수 있습니다.
interface name	(선택 사항) 주소 풀에 사용할 인터페이스를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령 각각을 인터페이스마다 하나씩 여러 번 입력할 수 있습니다. 인터페이스가 지정되지 않을 경우 이 명령은 명시적으로 참조되지 않은 모든 인터페이스를 위한 기본값을 지정합니다.

group-policy **address-pools** 명령의 주소 풀 설정은 tunnel group **address-pool** 명령의 로컬 풀 설정을 재정의합니다.

풀을 지정하는 순서가 중요합니다. ASA에서는 이 명령에 풀이 표시되는 순서대로 이 풀에서 주소를 할당합니다.

예

config-tunnel-general 컨피그레이션 모드에서 입력된 다음 예에서는 IPsec 원격 액세스 터널 그룹 테스트를 위해 원격 클라이언트에 주소를 할당하고자 주소 풀의 목록을 지정합니다.

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)#
```

관련 명령

명령	설명
ip 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 그룹의 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group-map default-group	**crypto ca certificate map** 명령으로 생성된 인증서 맵 엔트리를 터널 그룹과 연결합니다.

address-pools(group-policy attributes configuration mode)

원격 클라이언트에 주소를 할당하기 위해 주소 풀의 목록을 지정하려면 group-policy 특성 컨피그레이션 모드에서 **address-pools** 명령을 사용합니다. 그룹 정책에서 특성을 제거하고 다른 그룹 정책 소스에서 상속할 수 있게 하려면 이 명령의 **no** 형식을 사용합니다.

address-pools value *address_pool1* **[...***address_pool6***]**

no address-pools value *address_pool1* **[...***address_pool6***]**

address-pools none

no address-pools none

구문 설명

address_pool	**ip local pool** 명령으로 구성된 주소 풀의 이름을 지정합니다. 최대 6개의 로컬 주소 풀을 지정할 수 있습니다.
none	어떤 주소 풀도 구성되지 않도록 지정하며 다른 그룹 정책 소스로부터의 상속을 비활성화합니다.
value	주소 할당을 위해 최대 6개의 주소 풀 목록을 지정합니다.

기본값

기본적으로 주소 풀 특성은 상속을 허용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Group-policy 특성 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령의 주소 풀 설정이 그룹의 로컬 풀 설정을 재정의합니다. 로컬 주소 할당에 사용하기 위해 최대 6개의 로컬 주소 풀로 된 목록을 지정할 수 있습니다.

풀을 지정하는 순서가 중요합니다. ASA에서는 이 명령에 풀이 표시되는 순서대로 이 풀에서 주소를 할당합니다.

address-pools none 명령은 DefaultGrpPolicy와 같은 다른 정책 출처에서 이 특성을 상속받을 수 없게 합니다. **no address pools none** 명령은 컨피그레이션에서 **address-pools none** 명령을 제거하여 상속을 허용하는 기본값을 복원합니다.

예

config-general 컨피그레이션 모드에서 입력된 다음 예에서는 GroupPolicy1의 원격 클라이언트에 주소를 할당하는 데 사용할 주소 풀의 목록으로 pool_1과 pool_20을 구성합니다.

```
ciscoasa(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
ciscoasa(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# address-pools value pool_1 pool_20
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
ip local pool	VPN 그룹 정책에 사용할 IP 주소 풀을 구성합니다.
clear configure group-policy	구성된 모든 그룹 정책을 지웁니다.
show running-config group-policy	모든 그룹 정책의 또는 특정 그룹 정책의 컨피그레이션을 표시합니다.

admin-context

시스템 컨피그레이션을 위한 관리 컨텍스트를 설정하려면 글로벌 컨피그레이션 모드에서 **admin-context** 명령을 사용합니다.

admin-context *name*

구문 설명

name	최대 32자의 문자열로 이름을 설정합니다. 아직 어떤 컨텍스트도 정의하지 않은 경우 먼저 이 명령으로 관리 컨텍스트 이름을 지정합니다. 그런 다음 **context** 명령으로 추가하는 첫 번째 컨텍스트가 지정된 관리 컨텍스트 이름이 되어야 합니다. 이 이름은 대/소문자를 구분합니다. 즉 "customerA"와 "CustomerA"는 2개의 컨텍스트입니다. 문자, 숫자 또는 하이픈을 사용할 수 있으나 하이픈으로 이름을 시작하거나 끝내서는 안 됩니다. "System"과 "Null"(대문자 및 소문자 모두 해당)은 예약된 이름이므로 사용할 수 없습니다.

기본값

다중 컨텍스트 모드의 새 ASA에서는 관리 컨텍스트를 "admin"이라고 부릅니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

어떤 컨텍스트도 관리 컨텍스트로 설정할 수 있습니다. 단, 컨텍스트 컨피그레이션이 내부 플래시 메모리에 상주해야 합니다.

현재 관리 컨텍스트를 삭제할 수 없습니다. **clear configure context** 명령을 사용하여 모든 컨텍스트를 삭제하는 것만 가능합니다.

시스템 컨피그레이션은 어떤 네트워크 인터페이스 또는 네트워크 설정 자체도 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 대한 액세스가 필요할 때(예: ASA 소프트웨어를 다운로드하거나 관리자를 위해 원격 관리를 허용할 때) 관리 컨텍스트로 지정된 컨텍스트 중 하나를 사용합니다.

예

다음 예에서는 관리 컨텍스트를 "administrator"가 되도록 설정합니다.

```
ciscoasa(config)# admin-context administrator
```

관련 명령

명령	설명
clear configure context	시스템 컨피그레이션에서 모든 컨텍스트를 제거합니다.
context	시스템 컨피그레이션에서 컨텍스트를 구성하고 컨텍스트 컨피그레이션 모드를 시작합니다.
show admin-context	현재 관리 컨텍스트 이름을 표시합니다.

aggregate-address

BGP(Border Gateway Protocol) 데이터베이스에서 종합 엔트리를 생성하려면 주소군 컨피그레이션 모드에서 **aggregate-address** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

aggregate-address *address mask* [**as-set**] [**summary-only] [suppress-map** *map-name*]**[advertise-map** *map-name*] [**attribute-map** *map-name*]

no aggregate-address *address mask* [**as-set**] [**summary-only] [suppress-map** *map-name*]**[advertise-map** *map-name*] [**attribute-map** *map-name*]

구문 설명

address	종합 주소.
mask	종합 마스크.
as-set	(선택 사항) 자율 시스템 설정 경로 정보를 생성합니다.
summary-only	(선택 사항) 더 구체적인 경로를 모두 업데이트에서 필터링합니다.
suppress-map *map-name*	(선택 사항) 억제할 경로를 선택하는 데 사용되는 경로 맵의 이름을 지정합니다.
advertise-map *map-name*	(선택 사항) AS_SET 오리진 커뮤니티를 생성하기 위해 경로를 선택하는 데 사용되는 경로 맵의 이름을 지정합니다.
attribute-map *map-name*	(선택 사항) 종합 경로의 특성을 설정하는 데 사용되는 경로 맵의 이름을 지정합니다.

기본값

이 미세 종합 특성은 **as-set** 키워드를 지정하지 않고 이 명령으로 종합 경로를 생성할 때 자동으로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
컨텍스트 컨피그레이션,	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

BGP 및 mBGP(Multiprotocol BGP)에 종합 라우팅을 구현할 수 있습니다. BGP 또는 mBGP에 종합 경로를 재배포하거나 조건부 종합 라우팅 기능을 사용합니다.

키워드 없이 **aggregate-address** 명령을 사용할 경우, 지정된 범위에 속하는 더 구체적인 BGP 또는 mBGP 경로가 있다면 BGP 또는 mBGP 라우팅 테이블에 종합 엔트리가 생성됩니다. 종합 엔트리와 매칭하는 더 긴 접두사가 RIB(Routing Information Base)에 있어야 합니다. 이 종합 경로는 자율 시스템에서 나온 것으로 광고되며, 정보가 누락되었을 가능성을 나타내기 위해 미세 종합 특성이 설정됩니다. 이 미세 종합 특성은 **as-set** 키워드를 지정하지 않는 한 기본적으로 설정됩니다.

as-set 키워드를 사용하면 이 키워드가 없을 때 명령에서 따르는 것과 동일한 규칙으로 종합 엔트리를 만듭니다. 그러나 이 경로에 대해 광고되는 경로는 요약되는 모든 경로의 모든 요소로 구성된 AS_SET가 됩니다. 여러 경로를 종합할 때는 **aggregate-address** 명령 형식을 사용하지 마십시오. 이 경로는 요약된 경로에 대한 자율 시스템 경로 도달 정보가 변경될 때마다 계속해서 취소 및 업데이트되어야 하기 때문입니다**.**

summary-only 키워드를 사용하면 종합 경로(예: 192.*.*.*)가 생성될 뿐 아니라 모든 네이버에 대한 더 구체적인 경로의 광고가 억제됩니다. 특정 네이버에 대한 광고만 억제하려는 경우 **neighbor distribute-list** 명령을 주의하여 사용할 수 있습니다. 더 구체적인 경로가 제공될 경우 모든 BGP 또는 mBGP 라우터는 (longest-match 라우팅으로) 생성하는 덜 구체적인 종합 경로 대신 그 경로를 선호합니다.

suppress-map 키워드를 사용하면 종합 경로가 생성될 뿐 아니라 지정된 경로의 광고가 억제됩니다. 경로 맵의 **match** clause를 사용하여 종합 경로의 더 구체적인 경로를 선별적으로 억제하고 나머지는 억제하지 않을 수 있습니다. IP 액세스 목록 및 자율 시스템 경로 액세스 목록의 match clause가 지원됩니다.

advertise-map 키워드를 사용하여 AS_SET 또는 커뮤니티와 같이 종합 경로를 구성하는 각기 다른 요소를 이룰 구체적인 경로를 선택합니다. 이 **aggregate-address** 명령 형식은 종합 경로의 구성 요소가 각기 다른 자율 시스템에 있는 상태에서 AS_SET로 종합 경로를 만들고 이를 동일한 자율 시스템에 속한 일부 요소에 다시 광고하려는 경우에 유용합니다. 종합 경로가 수신 라우터에서 BGP 루프 탐지 메커니즘에 의해 삭제되지 않도록 AS_SET에서 특정 자율 시스템 번호를 생략해야 합니다. IP 액세스 목록 및 자율 시스템 경로 액세스 목록의 **match** clause가 지원됩니다.

attribute-map 키워드를 사용하면 종합 경로의 특성을 변경할 수 있습니다. 이 **aggregate-address** 명령 형식은 AS_SET를 구성하는 경로 중 하나에서 커뮤니티 no-export 특성과 같이 종합 경로의 내보내기를 막는 특성이 구성된 경우에 유용합니다. 종합 경로 특성을 변경하기 위해 특성 맵 경로 맵을 만들 수 있습니다.

예

다음 예에서는 종합 경로를 만들고 모든 네이버에 대한 더 구체적인 경로의 광고를 억제합니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

관련 명령

명령	설명
address-family ipv4	표준 IPv4를 사용하는 라우팅 세션을 구성하기 위해 주소군 컨피그레이션 모드를 시작합니다.

allocate-interface

보안 컨텍스트에 인터페이스를 할당하려면 컨텍스트 컨피그레이션 모드에서 **allocate-interface** 명령을 사용합니다. 컨텍스트에서 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

allocate-interface *physical_interface* [*map_name*] **[visible | invisible]**

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] **[visible | invisible]**

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

구문 설명

invisible	(기본값) 컨텍스트 사용자가 **show interface** 명령으로 매핑된 이름(구성된 경우)만 볼 수 있게 합니다.
map_name	(선택 사항) 매핑된 이름을 설정합니다. *map_name*은 컨텍스트 내에서 인터페이스 ID 대신 사용할 수 있는 인터페이스의 영숫자 별칭입니다. 매핑된 이름을 지정하지 않으면 인터페이스 ID가 컨텍스트 내에서 사용됩니다. 보안상의 이유로, 컨텍스트에서 어떤 인터페이스를 사용하고 있는지 컨텍스트 관리자에게 알리고 싶지 않을 때가 있습니다. 매핑된 이름은 문자로 시작하고 문자 또는 숫자로 끝나며, 나머지 자리에는 문자, 숫자, 밑줄만 사용할 수 있습니다. 예를 들어, 다음 이름을 사용할 수 있습니다. **int0** **inta** **int_0** 하위 인터페이스에서는 매핑된 이름의 범위를 지정할 수 있습니다. 범위에 대한 자세한 내용은 "사용 지침" 섹션을 참조하십시오.
physical_interface	**gigabitethernet0/1**과 같이 인터페이스 ID를 설정합니다. 허용되는 값에 대해서는 **interface** 명령을 참조하십시오. 인터페이스 유형과 포트 번호 사이에 공백을 넣지 마십시오.
subinterface	하위 인터페이스 번호를 설정합니다. 하위 인터페이스의 범위를 지정할 수 있습니다.
visible	(선택 사항) 매핑된 이름을 설정했더라도 컨텍스트 사용자가 **show interface** 명령에서 물리적 인터페이스 속성을 볼 수 있게 합니다.

기본값

매핑된 이름을 설정하면 기본적으로 인터페이스 ID는 **show interface** 명령 출력에 표시되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령을 여러 번 입력하여 각기 다른 범위를 지정할 수 있습니다. 매핑된 이름 또는 표시 여부 설정을 변경하려면 해당 인터페이스 ID에 대해 명령을 다시 입력하고 새 값을 설정합니다. **no allocate-interface** 명령을 입력하고 다시 시작할 필요 없습니다. **allocate-interface** 명령을 제거할 경우 ASA는 컨텍스트에서 모든 인터페이스 관련 컨피그레이션을 제거합니다.

투명 방화벽 모드에서는 오로지 2개의 인터페이스만 트래픽을 전달할 수 있습니다. 그러나 ASA에서는 전용 관리 인터페이스인 Management 0/0(물리적 인터페이스 또는 하위 인터페이스)을 3번째 트래픽 관리 인터페이스로 사용할 수 있습니다.

참고 투명 모드를 위한 관리 인터페이스는 MAC 주소에 없는 패킷을 인터페이스 바깥으로 플러딩하지 않습니다.

라우티드 모드에서는 원한다면 여러 컨텍스트에 동일한 인터페이스를 지정할 수 있습니다. 투명 모드에서는 공유 인터페이스를 허용하지 않습니다.

하위 인터페이스의 이름을 지정할 경우 매핑된 이름의 매칭 범위를 지정할 수 있습니다. 범위에 대한 다음 지침을 따르십시오.

- 매핑된 이름은 영문자 다음에 숫자가 와야 합니다. 매핑된 이름에서 영문자 부분은 범위의 양쪽 경계에 매칭해야 합니다. 예를 들어, 다음과 같이 범위를 입력합니다.

  ```
  int0-int10
  ```

  만약 **gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5**라고 입력하면 명령은 실패합니다.

- 매핑된 이름의 숫자 부분은 하위 인터페이스 범위와 동일한 개수의 숫자를 포함해야 합니다. 예를 들어, 두 범위 모두 100개 인터페이스를 포함합니다.

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  만약 **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15**라고 입력하면 명령은 실패합니다.

예

다음 예에서는 gigabitethernet0/1.100, gigabitethernet0/1.200, gigabitethernet0/2.300~gigabitethernet0/1.305가 컨텍스트에 지정되는 것을 보여줍니다. 매핑된 이름은 int1~int8입니다.

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

관련 명령

명령	설명
context	시스템 컨피그레이션에서 보안 컨텍스트를 만들고 컨텍스트 컨피그레이션 모드를 시작합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show context	컨텍스트의 목록(시스템 실행 영역) 또는 현재 컨텍스트에 대한 정보를 표시합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
vlan	하위 인터페이스에 VLAN ID를 지정합니다.

allocate-ips

AIP SSM를 설치한 경우 보안 컨텍스트에 IPS 가상 센서를 할당하려면 컨텍스트 컨피그레이션 모드에서 **allocate-ips** 명령을 사용합니다. 컨텍스트에서 가상 센서를 제거하려면 이 명령의 **no** 형식을 사용합니다.

allocate-ips *sensor_name* [*mapped_name*] **[default]**

no allocate-ips *sensor_name* [*mapped_name*] **[default]**

구문 설명

default	(선택 사항) 컨텍스트당 하나의 센서를 기본 센서로 설정합니다. 컨텍스트 컨피그레이션에서 센서 이름을 지정하지 않을 경우 컨텍스트는 이 기본 센서를 사용합니다. 컨텍스트당 기본 센서를 하나만 구성할 수 있습니다. 기본 센서를 변경하려면 **no allocate-ips** 명령을 입력하여 현재 기본 센서를 제거한 후 새 기본 센서를 할당할 수 있습니다. 기본 센서를 지정하지 않은 상태에서 컨텍스트 컨피그레이션에 센서 이름이 포함되어 있지 않으면 AIP SSM의 기본 센서가 트래픽에 사용됩니다.
mapped_name	(선택 사항) 매핑된 이름을 컨텍스트 내에서 실제 센서 이름 대신 사용 가능한 센서 이름의 별칭으로 설정합니다. 매핑된 이름을 지정하지 않으면 컨텍스트 내에서 센서 이름이 사용됩니다. 보안을 위해, 컨텍스트에서 어떤 센서가 사용되고 있는지를 컨텍스트 관리자에게 알리고 싶지 않을 수 있습니다. 또는 컨텍스트 컨피그레이션을 일반화하고자 할 수도 있습니다. 예를 들어, 모든 컨텍스트에서 "sensor1"과 "sensor2"라는 센서를 사용하도록 하려면 context A에서는 "highsec"과 "lowsec" 센서를 sensor1과 sensor2에 매핑하되 context B에서는 "medsec"과 "lowsec" 센서를 sensor1과 sensor2에 매핑할 수 있습니다.
sensor_name	AIP SSM에 구성된 센서 이름을 설정합니다. AIP SSM에 구성된 센서를 보려면 **allocate-ips ?**를 입력합니다. 사용 가능한 모든 센서가 나열됩니다. **show ips** 명령을 입력할 수도 있습니다. 시스템 실행 공간에서 **show ips** 명령을 실행하면 사용 가능한 모든 센서가 나열됩니다. 이 명령을 컨텍스트에서 입력할 경우 이미 컨텍스트에 할당된 센서가 표시됩니다. 아직 AIP SSM에 존재하지 않는 센서 이름을 지정하면 오류 메시지가 표시되지만 **allocate-ips** 명령은 있는 그대로 입력됩니다. AIP SSM에서 그 이름의 센서를 만들 때까지 컨텍스트는 해당 센서가 다운 상태라고 가정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

각 컨텍스트에 하나 이상의 IPS 가상 센서를 지정할 수 있습니다. 그러면 AIP SSM에 트래픽을 전송하도록 **ips** 명령을 사용하여 컨텍스트를 구성할 때 컨텍스트에 할당된 센서를 지정할 수 있습니다. 컨텍스트에 할당하지 않은 센서는 지정할 수 없습니다. 컨텍스트에 어떤 센서도 할당하지 않을 경우 AIP SSM에 구성된 기본 센서가 사용됩니다. 여러 컨텍스트에 동일한 센서를 할당할 수 있습니다.

참고 다중 컨텍스트 모드에서만 가상 센서를 사용할 수 있는 것은 아닙니다. 단일 모드에서도 서로 다른 트래픽 흐름에 대해 서로 다른 센서를 사용할 수 있습니다.

예

다음 예는 sensor1 및 sensor2를 context A에, sensor1 및 sensor3을 context B에 할당합니다. 두 컨텍스트 모두 센서 이름을 "ips1" 및 "ips2"에 매핑합니다. context A에서는 sensor1이 기본 센서로 설정되었지만, context B에서는 기본 센서가 설정되지 않았으므로 AIP SSM에 구성된 기본 센서가 사용됩니다.

```
ciscoasa(config-ctx)# context A
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)# allocate-ips sensor1 ips1 default
ciscoasa(config-ctx)# allocate-ips sensor2 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1
ciscoasa(config-ctx)# allocate-ips sensor3 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

관련 명령

명령	설명
context	시스템 컨피그레이션에서 보안 컨텍스트를 만들고 컨텍스트 컨피그레이션 모드를 시작합니다.
ips	검사받기 위해 트래픽을 AIP SSM로 전환합니다.
show context	컨텍스트의 목록(시스템 실행 영역) 또는 현재 컨텍스트에 대한 정보를 표시합니다.
show ips	AIP SSM에 구성된 가상 센서를 표시합니다.

allow-ssc-mgmt

ASA 5505의 인터페이스가 SSC 관리 인터페이스가 되도록 설정하려면 인터페이스 컨피그레이션 모드에서 **allow-ssc-mgmt** 명령을 사용합니다. 인터페이스 할당을 취소하려면 이 명령의 **no** 형식을 사용합니다.

allow-ssc-mgmt

no allow-ssc-mgmt

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

이 명령은 공장 기본 컨피그레이션에서 VLAN 1에 대해 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

SSC는 외부 인터페이스가 없습니다. VLAN을 관리 VLAN으로 구성함으로써 백플레인을 통해 내부 관리 IP 주소에 액세스하게 할 수 있습니다. 기본적으로 VLAN 1은 SSC 관리 주소에 대해 활성화되어 있습니다. 하나의 VLAN만 SSC 관리 VLAN으로 지정할 수 있습니다.

ASDM을 사용하여 액세스하려는 경우 관리 주소에 대해 NAT를 구성하지 마십시오. ASDM을 통한 초기 설정에서는 실제 주소에 액세스해야 합니다. (SSC에 비밀번호를 설정하는) 초기 설정 이후에는 NAT를 구성하고 SSC에 액세스할 때 ASDM에 변환된 주소를 제공할 수 있습니다.

예

다음 예에서는 VLAN 1에서 관리 액세스를 비활성화하고 VLAN 2에서는 활성화합니다.

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# no allow-ssc-mgmt
ciscoasa(config-if)# interface vlan 2
ciscoasa(config-if)# allow-ssc-mgmt
```

관련 명령

명령	설명
interface	인터페이스를 구성합니다.
ip address	브리지 그룹의 관리 IP 주소를 설정합니다.
nameif	인터페이스 이름을 설정합니다.
security-level	인터페이스 보안 레벨을 설정합니다.
hw-module module ip	SSC를 위한 관리 IP 주소를 구성합니다.
hw-module module allow-ip	관리 IP 주소에 액세스할 수 있는 호스트를 설정합니다.

always-on-vpn

AnyConnect Always-On-VPN 기능을 구성하려면 그룹 정책 컨피그레이션 모드에서 **always-on-vpn** 명령을 사용합니다.

always-on-vpn [profile-setting | disable]

구문 설명

disable	Always-On-VPN 기능을 끕니다.
profile-setting	AnyConnect 프로필에 구성된 **always-on-vpn** 설정을 사용합니다.

명령 기본값

Always-On-VPN 기능은 기본적으로 꺼져 있습니다.

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

사용 지침

AnyConnect 사용자에 대해 Always-On-VPN 기능을 활성화하려면 프로필 편집기에서 AnyConnect 프로필을 구성합니다. 그런 다음 알맞은 정책에 대한 그룹 정책 특성을 구성합니다.

예

다음 예에서는 VLAN 1에서 관리 액세스를 비활성화하고 VLAN 2에서는 활성화합니다.

```
ciscoasa(config)# group-policy <group policy> attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# always-on-vpn profile-setting
```

관련 명령

명령	설명
webvpn	WebVPN에 대한 그룹 정책을 구성합니다.

anyconnect ask

ASA에서 원격 SSL VPN 클라이언트 사용자에게 클라이언트 다운로드 프롬프트를 표시할 수 있게 하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect ask** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect ask {none | enable [default {webvpn | anyconnect} timeout *value*]}

no anyconnect ask none [default {webvpn | anyconnect}]

구문 설명

default anyconnect timeout *value*	원격 사용자에게 클라이언트 다운로드 프롬프트를 표시하거나 클라이언트리스 연결용 포털 페이지로 이동한 다음 *value*의 값만큼 기다렸다가 기본 작업, 즉 클라이언트 다운로드를 시작합니다.
default webvpn timeout *value*	원격 사용자에게 클라이언트 다운로드 프롬프트를 표시하거나 클라이언트리스 연결용 포털 페이지로 이동한 다음 *value*의 값만큼 기다렸다가 기본 작업을 수행합니다. 즉 WebVPN 포털 페이지를 표시합니다.
enable	원격 사용자에게 클라이언트 다운로드 프롬프트를 표시하거나 클라이언트리스 연결용 포털 페이지로 이동한 다음 사용자가 응답할 때까지 무한정 기다립니다.
none	즉시 기본 작업을 수행합니다.

기본값

이 명령의 기본값은 **anyconnect ask none default webvpn**입니다. ASA는 클라이언트리스 연결을 위한 포털 페이지를 즉시 표시합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

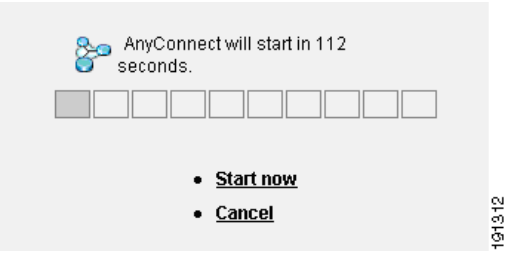
명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
8.4(1)	**anyconnect ask** 명령이 **svc ask** 명령을 대체했습니다.

사용 지침

그림 2-1 은 **default anyconnect timeout** *value* 명령 또는 **default webvpn timeout** *value* 명령이 구성되면 원격 사용자에게 프롬프트를 표시합니다.

그림 2-1 원격 사용자에게 표시되는 SSL VPN 클라이언트 다운로드 프롬프트



예

다음 예에서는 ASA에서 원격 사용자에게 클라이언트 다운로드 프롬프트를 표시하거나 포털 페이지로 이동한 다음 10초간 사용자 응답을 기다렸다가 클라이언트를 다운로드하도록 구성합니다.

```
ciscoasa(config-group-webvpn)# anyconnect ask enable default svc timeout 10
```

관련 명령

명령	설명
show webvpn anyconnect	설치된 SSL VPN 클라이언트에 대한 정보를 표시합니다.
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect image	ASA에서 원격 PC에 다운로드하기 위해 캐시 메모리에서 확장하는 클라이언트 패키지 파일을 지정합니다.

anyconnect df-bit-ignore

패킷에서 단편화가 필요한 DF 비트를 무시하려면 그룹 정책 webvpn 컨피그레이션 모드에서 **anyconnect-df-bit-ignore** 명령을 사용합니다. 단편화가 필요한 DF 비트를 인정하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect df-bit-ignore {enable | none}

no anyconnect df-bit-ignore {enable | none}

구문 설명

enable	AnyConnect 클라이언트에 대해 DF 비트 무시를 활성화합니다.
none	AnyConnect 클라이언트에 대해 DF 비트를 비활성화합니다.

기본값

기본적으로 이 옵션은 활성화되어 있지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	**svc df-bit-ignore** 명령을 도입했습니다.
8.4(3)	**anyconnect df-bit-ignore** 명령이 **svc df-bit-ignore** 명령을 대체했습니다.

예

```
vmb-5520(config-group-webvpn)# anyconnect routing-filtering-ignore ?

config-group-webvpn mode commands/options:
  enable  Enable Routing/Filtering for AnyConnect Client
  none    Disable Routing/Filtering for AnyConnect Client
```

anyconnect dpd-interval

ASA에서 DPD(Dead Peer Detection)를 활성화하고 원격 클라이언트 또는 ASA에서 SSL VPN 연결을 통해 DPD를 수행하는 빈도를 설정하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect dpd-interval** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

구문 설명

client none	클라이언트에서 수행하는 DPD를 비활성화합니다.
client *seconds*	클라이언트에서 DPD를 수행하는 빈도를 30초~3600초 범위에서 지정합니다.
gateway none	ASA에서 수행하는 DPD를 비활성화합니다.
gateway *seconds*	ASA에서 DPD를 수행하는 빈도를 30초~3600초 범위에서 지정합니다.

기본값

기본적으로 ASA(게이트웨이)와 클라이언트 모두에서 DPD가 활성화되어 있고 30초로 설정되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.
8.0(3)	ASA(게이트웨이) 및 클라이언트 모두에서 기본 설정을 비활성에서 30초로 변경했습니다.
8.4(1)	**anyconnect dpd-interval** 명령이 **svc dpd-interval** 명령을 대체했습니다.

예

다음 예에서는 *sales*라는 기존 그룹 정책에 대해 ASA(게이트웨이)에서 수행하는 DPD의 빈도를 3000초로, 클라이언트에서 수행하는 DPD 빈도는 1000초로 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect dpd-interval gateway 3000
ciscoasa(config-group-webvpn)# anyconnect dpd-interval client 1000
```

anyconnect dtls compression

특정 그룹 또는 사용자에 대해 저대역폭 링크에서의 압축을 활성화하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect dtls compression** 명령을 사용합니다. 그룹에서 컨피그레이션을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect dtls compression {lzs | none}

no anyconnect dtls compression {lzs | none}

구문 설명

lzs	무상태(stateless) 압축 알고리즘을 활성화합니다.
none	압축을 비활성화합니다.

기본값

기본적으로 AnyConnect 압축은 활성화되어 있지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(2)	**anyconnect dtls compression** 명령을 도입했습니다.

예

다음 예에서는 압축을 비활성화하는 시퀀스를 보여줍니다.

```
asa# config terminal
asa(config)# group-policy DfltGrpPolicy attributes
asa(config-group-policy)# webvpn
asa(config-group-webvpn)# anyconnect ssl compression none
asa(config-group-webvpn)# anyconnect dtls compression none
```

anyconnect enable

ASA에서 원격 컴퓨터에 AnyConnect 클라이언트를 다운로드하거나 AnyConnect 클라이언트(SSL 또는 IKEv2)를 사용하여 ASA와 연결할 수 있게 하려면 webvpn 컨피그레이션 모드에서 **anyconnect enable** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect enable

no anyconnect enable

기본값

이 명령은 기본적으로 비활성화되어 있습니다. ASA는 클라이언트를 다운로드하지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 **svc enable**로 도입했습니다.
8.4(1)	**anyconnect enable** 명령이 **svc enable** 명령을 대체했습니다.

사용 지침

no anyconnect enable 명령을 입력하더라도 활성 세션이 종료되지 않습니다.

anyconnect enable 명령은 **anyconnect image xyz** 명령으로 AnyConnect 이미지를 구성한 다음에 실행해야 합니다. AnyConnect 클라이언트 또는 AnyConnect weblaunch를 사용하려면 **anyconnect enable**을 실행해야 합니다. **anyconnect enable** 명령이 SSL 또는 IKEv2와 함께 실행되지 않을 경우 AnyConnect는 정상적으로 작동하지 않으며 IPsec VPN 연결 종료 오류와 함께 시간 초과됩니다. 따라서 **show webvpn svc** 명령이 SSL VPN 클라이언트가 활성화되었다고 간주하지 않고 설치된 AnyConnect 패키지도 등록하지 않습니다.

예

다음 예에서는 ASA에서 클라이언트 다운로드를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect enable
```

관련 명령

명령	설명
anyconnect image	ASA에서 원격 PC에 다운로드하기 위해 캐시 메모리에서 확장하는 AnyConnect SSL VPN 클라이언트 패키지 파일을 지정합니다.
anyconnect modules	AnyConnect SSL VPN 클라이언트에서 선택적 기능을 위해 필요로 하는 모듈의 이름을 지정합니다.
anyconnect profiles	ASA에서 Cisco AnyConnect SSL VPN 클라이언트에 다운로드하는 프로필을 저장하는 데 쓰이는 파일의 이름을 지정합니다.
show webvpn anyconnect	ASA에 설치되었고 원격 PC에 다운로드되기 위해 캐시 메모리에 로드된 SSL VPN 클라이언트에 대한 정보를 표시합니다.
anyconnect localization	Cisco AnyConnect VPN Client에 다운로드되는 현지화 파일을 저장하는 데 쓰이는 패키지 파일을 지정합니다.

anyconnect firewall-rule

공개를 설정하거나 ACL 방화벽을 제공하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect firewall-rule** 명령을 사용합니다.

anyconnect firewall-rule client interface {public | private} *ACL*

구문 설명

ACL	액세스 제어 목록 지정
client interface	클라이언트 인터페이스 지정
private	비공개 인터페이스 규칙 구성
public	공개 인터페이스 규칙 구성

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.
8.4(1)	**anyconnect firewall-rule** 명령이 **svc firewall-rule** 명령을 대체했습니다.
9.0(1)	명령의 ACL에 IPv4 및 IPv6 주소를 모두 지정할 수 있는 Unified Access Control 규칙을 사용할 수 있습니다.

사용 지침

이 명령이 정상적으로 작동하려면 AnyConnect 보안 모빌리티 클라이언트를 위한 AnyConnect Secure Mobility 라이센스를 지원하는 AsyncOS for Web version 7.0 릴리스가 필요합니다. 또한 AnyConnect Secure Mobility, ASA 8.3, ASDM 6.3을 지원하는 AnyConnect 릴리스도 필요합니다.

다음 참고 사항은 AnyConnect 클라이언트에서 방화벽을 사용하는 방식을 설명합니다.

- 소스 IP는 방화벽 규칙에 사용되지 않습니다. 클라이언트는 ASA에서 보낸 방화벽 규칙에서 소스 IP 정보를 무시합니다. 클라이언트는 그 규칙이 공개 또는 비공개인가에 따라 소스 IP를 결정합니다. 공개 규칙은 클라이언트의 모든 인터페이스에 적용됩니다. 비공개 규칙은 가상 어댑터에 적용됩니다.
- ASA는 ACL 규칙을 위해 여러 프로토콜을 지원합니다. 그러나 AnyConnect 방화벽 기능은 TCP, UDP, ICMP, IP만 지원합니다. 클라이언트가 다른 프로토콜의 규칙을 수신할 경우 이를 잘못된 방화벽 규칙으로 간주한 다음 보안을 위해 스플릿 터널링을 비활성화하고 완전한 터널링을 사용합니다.

운영 체제에 따라 다음과 같이 다르게 동작하므로 주의하십시오.

- Windows 컴퓨터는 Windows 방화벽에서 거부 규칙이 허용 규칙에 우선합니다. ASA가 AnyConnect 클라이언트에 허용 규칙을 푸시하지만 사용자가 이미 사용자 지정 거부 규칙을 만들었다면 AnyConnect 규칙은 적용되지 않습니다.
- Windows Vista에서는 방화벽 규칙이 생성될 때 Vista가 포트 번호 범위를 쉼표로 구분된 문자열(예: 1~300, 5000~5300)로 받습니다. 포트의 최대 개수는 300개입니다. 300개보다 많은 포트를 지정할 경우 방화벽 규칙은 처음 300개 포트에만 적용됩니다.
- 방화벽 서비스가 (시스템에서 자동으로 시작되지 않고) AnyConnect 클라이언트에 의해 시작되어야 하는 Windows 사용자는 VPN 연결 설정에 상당히 더 많은 시간이 걸리는 것을 느낄 수 있습니다.
- Mac 컴퓨터에서는 AnyConnect 클라이언트가 ASA에서 규칙을 적용하는 것과 동일한 순서로, 순차적으로 규칙을 적용합니다. 전역 규칙은 항상 마지막에 와야 합니다.
- 타사 방화벽의 경우, AnyConnect 클라이언트 방화벽과 타사 방화벽 모두 해당 트래픽 유형을 허용해야 트래픽이 전달됩니다. 타사 방화벽이 AnyConnect 클라이언트에서 허용하는 트래픽 유형을 차단할 경우 클라이언트는 해당 트래픽을 차단합니다.

로컬 인쇄 및 테더링 디바이스 지원을 위한 ACL 규칙의 예를 포함하여 AnyConnect 클라이언트 방화벽에 대한 자세한 내용은 *AnyConnect 관리자 설명서*를 참조하십시오.

예

다음 예에서는 ACL인 *AnyConnect_Client_Local_Print*를 공개 방화벽으로 활성화합니다.

```
ciscoasa(config)# group-policy example_group attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect firewall-rule client-interface public value
AnyConnect_Client_Local_Print
```

관련 명령

명령	설명
show webvpn anyconnect	설치된 SSL VPN 클라이언트에 대한 정보를 표시합니다.
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect image	ASA에서 원격 PC에 다운로드하기 위해 캐시 메모리에서 확장하는 클라이언트 패키지 파일을 지정합니다.

anyconnect image

AnyConnect 배포 패키지를 설치하거나 업그레이드하고 이를 실행 중인 컨피그레이션에 추가하려면 webvpn 컨피그레이션 모드에서 **anyconnect image** 명령을 사용합니다. 실행 중인 컨피그레이션에서 AnyConnect 배포 패키지를 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect image *path order* [**regex** *expression*]

no anyconnect image *path order* [**regex** *expression*]

구문 설명

order	여러 클라이언트 패키지 파일이 있을 경우 패키지 파일의 순서를 지정합니다. 1~65535입니다. ASA는 사용자가 지정한 순서대로 각 클라이언트의 일부를 원격 PC에 다운로드하면서 운영 체제와 매칭하는 것을 찾습니다.
path	AnyConnect 패키지의 경로와 파일 이름을 최대 255자로 지정합니다.
regex *expression*	ASA가 브라우저에서 전달한 user-agent 문자열과의 매칭에 사용할 문자열을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 **svc image**로 도입했습니다.
8.0(1)	**regex** 키워드를 추가했습니다.
8.4(1)	**anyconnect image** 명령이 **svc image** 명령을 대체했습니다.

사용 지침

패키지 파일에 번호를 부여함으로써 ASA에서 운영 체제와 매칭하는 것을 찾을 때까지 원격 PC에 그 일부를 다운로드하는 순서가 결정됩니다. 번호가 가장 낮은 패키지 파일을 맨 먼저 다운로드합니다. 따라서 원격 PC에서 사용하는 가장 자주 보이는 운영 체제와 매칭하는 패키지 파일에 가장 낮은 번호를 부여해야 합니다.

기본 순서는 1입니다. *order* 인수를 지정하지 않을 경우, **svc image** 명령을 입력할 때마다 앞서 1번이었던 이미지를 덮어쓰게 됩니다.

각 클라이언트 패키지 파일에 대한 **anyconnect image** 명령을 임의의 순서로 입력할 수 있습니다. 이를테면 어떤 패키지 파일을 두 번째로 다운로드하도록 지정한 다음(*order* 2) **anyconnect image** 명령을 입력하여 그 패키지 파일이 가장 먼저 다운로드하게끔 지정할 수 있습니다(*order* 1).

모바일 사용자를 위해 **regex** keyword를 사용하여 모바일 디바이스의 연결 시간을 단축할 수 있습니다. 브라우저가 ASA에 연결되면 HTTP 헤더에 user-agent 문자열을 포함합니다. ASA가 문자열을 수신하고 그 문자열이 이미지에 대해 구성된 표현식과 매칭할 경우, 나머지 클라이언트 이미지를 테스트하지 않고 즉시 그 이미지를 다운로드합니다.

참고 독립형 클라이언트를 사용할 때는 **regex** 명령이 무시됩니다. 이는 오로지 웹 브라우저에서 성능 향상을 위해 사용되며, regex 문자열은 독립형 클라이언트에서 제공하는 어떤 사용자 또는 에이전트와도 매칭되지 않습니다.

ASA는 AnyConnect 클라이언트 및 CSD(Cisco Secure Desktop) 패키지 파일 둘 다 캐시 메모리에 확장합니다. ASA에서 성공적으로 패키지 파일을 확장하려면 패키지 파일의 이미지와 파일을 저장하기에 충분한 캐시 메모리가 있어야 합니다.

ASA는 패키지를 확장하기에 캐시 메모리가 부족함을 알게 되면 콘솔에 오류 메시지를 표시합니다. 다음 예에서는 **svc image** 명령으로 패키지 파일의 설치를 시도한 다음 표시되는 오류 메시지를 보여줍니다.

```
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0520-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

패키지 파일을 설치할 때 이러한 오류가 발생할 경우 글로벌 컨피그레이션 모드에서 **dir cache:/** 명령을 사용하여 남아 있는 캐시 메모리의 양 및 이미 설치한 패키지가 있으면 그 크기를 확인합니다.

참고 ASA에 기본 내장형 플래시 메모리 또는 기본 DRAM(캐시 메모리용)의 용량만 있을 경우 여러 AnyConnect 클라이언트 패키지를 ASA에 저장하고 로드하면서 문제가 생길 가능성이 있습니다. 플래시 메모리에 패키지 파일을 수용하기에 충분한 공간이 있더라도 클라이언트 이미지의 압축을 풀고 로드하는 과정에서 ASA의 캐시 메모리가 부족해질 수 있습니다. AnyConnect 구축 시 ASA 메모리 요구 사항 및 ASA 만일의 메모리 업그레이드에 대한 자세한 내용은 Cisco ASA 5500 시리즈의 최신 릴리스 정보를 참조하십시오.

예

다음 예에서는 Windows, MAC, Linux를 위한 AnyConnect 클라이언트 패키지 파일을 이 순서대로 로드합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0527-k9.pkg 1
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-linux-3.0.0414-k9.pkg 3
ciscoasa(config-webvpn)
```

다음은 **show webvpn anyconnect** 명령의 샘플 출력입니다. 여기서는 로드된 AnyConnect 클라이언트 패키지와 그 순서를 보여줍니다.

```
ciscoasa(config-webvpn)# show webvpn anyconnect
1. disk0:/anyconnect-win-3.0.0527-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,0,0527
  Hostscan Version 3.0.0527
  Tue 10/19/2010 16:16:56.25

2. disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2 dyn-regex=/Intel Mac OS X/
  CISCO STC Darwin_i386
  3.0.0414
  Wed Oct 20 20:39:53 MDT 2010
```

```
3. disk0:/anyconnect-linux-3.0.0414-k9.pkg 3 dyn-regex=/Linux i[1-9]86/
  CISCO STC Linux
  3.0.0414
  Wed Oct 20 20:42:02 MDT 2010

3 AnyConnect Client(s) installed
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
anyconnect modules	AnyConnect SSL VPN 클라이언트에서 선택적 기능을 위해 필요로 하는 모듈의 이름을 지정합니다.
anyconnect profiles	ASA에서 Cisco AnyConnect SSL VPN 클라이언트에 다운로드하는 프로필을 저장하는 데 쓰이는 파일의 이름을 지정합니다.
show webvpn anyconnect	ASA에 설치되었고 원격 PC에 다운로드되기 위해 캐시 메모리에 로드된 SSL VPN 클라이언트에 대한 정보를 표시합니다.
anyconnect localization	Cisco AnyConnect VPN Client에 다운로드되는 현지화 파일을 저장하는 데 쓰이는 패키지 파일을 지정합니다.

anyconnect keep-installer

참고 이 명령은 AnyConnect 2.5 이후 버전에는 적용되지 않지만, 역호환성을 위해 아직 제공되고 있습니다. **anyconnect keep-installer** 명령을 구성하더라도 AnyConnect 3.0 이상에는 영향을 주지 않습니다.

원격 PC에 SSL VPN 클라이언트를 영구적으로 설치할 수 있게 하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect keep-installer** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect keep-installer {**installed** | **none**}

no anyconnect keep-installer {**installed** | **none**}

구문 설명

installed	클라이언트의 자동 제거 기능을 비활성화합니다. 클라이언트는 향후 연결을 위해 원격 PC에 계속 설치되어 있습니다.
none	활성 연결이 끝나면 원격 컴퓨터에서 클라이언트가 제거되도록 지정합니다.

기본값

기본적으로 클라이언트 영구 설치가 활성화됩니다. 클라이언트는 세션이 끝나더라도 원격 컴퓨터에 남아 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.
8.4(1)	**anyconnect keep-installer** 명령이 **svc keep-installer** 명령을 대체했습니다.

예

다음 예에서는 사용자가 그룹 정책 webvpn 컨피그레이션 모드를 시작하고 세션이 끝날 때 클라이언트를 제거하도록 그룹 정책을 구성합니다.

```
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)# anyconnect keep-installer none
ciscoasa(config-group-webvpn)#
```

관련 명령

명령	설명
show webvpn anyconnect	ASA에 설치되었고 원격 PC에 다운로드되기 위해 캐시 메모리에 로드된 AnyConnect 클라이언트에 대한 정보를 표시합니다.
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect enable	ASA에서 원격 PC에 AnyConnect 클라이언트 파일을 다운로드할 수 있게 합니다.
anyconnect image	ASA에서 원격 PC에 다운로드하기 위해 캐시 메모리에서 확장하는 AnyConnect 클라이언트 패키지 파일을 지정합니다.

anyconnect modules

AnyConnect SSL VPN 클라이언트에서 선택적 기능을 위해 필요로 할 모듈의 이름을 지정하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect modules** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect modules {none | value *string***}**

no anyconnect modules {none | value *string***}**

구문 설명

string	선택적 모듈의 이름이며 최대 256자입니다. 여러 문자열은 쉼표로 구분합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 **svc modules**로 도입했습니다.
8.4(1)	**anyconnect modules** 명령이 **svc modules** 명령을 대체했습니다.

사용 지침

클라이언트는 다운로드 시간을 최소화하기 위해 지원하는 각 기능에 필요한 모듈만 (ASA에서) 다운로드하도록 요청합니다. **anyconnect modules** 명령은 ASA에서 이 모듈을 다운로드할 수 있게 합니다.

다음 표에서는 AnyConnect Module을 나타내는 문자열 값을 보여줍니다.

AnyConnect 모듈을 가리키는 문자열	AnyConnect 모듈 이름
dart	AnyConnect DART(Diagnostics and Reporting Tool)
nam	AnyConnect Network Access Manager
vpngina	AnyConnect SBL(Start Before Logon)
websecurity	AnyConnect Web Security Module
telemetry	AnyConnect Telemetry Module
posture	AnyConnect Posture Module
none	**none**을 선택하면 ASA는 선택적 모듈 없이 필수 파일만 다운로드합니다. 기존 모듈은 그룹 정책에서 제거됩니다.

예

다음 예에서는 사용자가 그룹 정책 *PostureModuleGroup*에 대해 그룹 정책 특성 모드를 시작하고 이 그룹 정책에 대한 webvpn 컨피그레이션 모드를 시작한 다음 문자열 *posture*와 *telemetry*를 지정하여 ASA와 연결할 때 AnyConnect Posture Module과 AnyConnect Telemetry Module을 엔드포인트에 다운로드하게 합니다.

```
ciscoasa> en
Password:
ciscoasa# config t
ciscoasa(config)# group-policy PostureModuleGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect modules value posture,telemetry
ciscoasa(config-group-webvpn)# write mem
Building configuration...
Cryptochecksum: 40975338 b918425d 083b391f 9e5a5c69

22055 bytes copied in 3.440 secs (7351 bytes/sec)
[OK]
ciscoasa(config-group-webvpn)#
```

그룹 정책에서 모듈을 제거하려면 보존하려는 모듈 값만 지정하면서 명령을 재실행합니다. 이를테면 다음 명령은 telemetry 모듈을 제거합니다.

```
ciscoasa(config-group-webvpn)# anyconnect modules value posture
```

관련 명령

명령	설명
show webvpn anyconnect	ASA의 캐시 메모리에 로드되었고 다운로드 가능한 AnyConnect 패키지에 대한 정보를 표시합니다.
anyconnect enable	특정 그룹 또는 사용자에 대해 AnyConnect 클라이언트를 활성화합니다.
anyconnect image	ASA에서 원격 PC에 다운로드하기 위해 캐시 메모리에서 확장하는 AnyConnect 클라이언트 패키지 파일을 지정합니다.

anyconnect mtu

Cisco AnyConnect VPN Client에 의해 설정되는 SSL VPN 연결의 MTU 크기를 조정하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect mtu** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect mtu *size*

no anyconnect mtu *size*

구문 설명

size	MTU 크기는 바이트 단위이며, 범위는 256바이트~1406바이트입니다.

기본값

기본 크기는 1406바이트입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
8.4(1)	**anyconnect mtu** 명령이 **svc mtu** 명령을 대체했습니다.

사용 지침

이 명령은 AnyConnect 클라이언트에만 영향을 줍니다. Cisco SSL VPN 클라이언트는 여러 MTU 크기에 맞출 수 없습니다.

기본 그룹 정책에서 이 명령의 기본값은 **no svc mtu**입니다. MTU 크기는 연결에서 사용하는 인터페이스의 MTU에서 IP/UDP/DTLS 오버헤드를 뺀 값으로 자동 조정됩니다.

이 명령은 SSL 및 SSL with DTLS에서 설정된 AnyConnect 클라이언트 연결에만 적용됩니다.

IPv6 활성 인터페이스에서 허용되는 최소 MTU는 1280바이트입니다. 그러나 IPsec이 인터페이스에서 활성화된 경우, IPsec 암호화의 오버헤드 때문에 MTU가 1380보다 작은 값으로 설정되어야 합니다. 1380바이트보다 낮게 인터페이스를 설정하면 패킷이 폐기될 수 있습니다.

예

다음 예에서는 그룹 정책 *telecommuters*에 대해 MTU 크기를 500바이트로 구성합니다.

```
ciscoasa(config)# group-policy telecommuters attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect mtu 500
```

관련 명령

명령	설명
anyconnect keep-installer	클라이언트의 자동 제거 기능을 비활성화합니다. 최초로 다운로드한 후 연결이 종료하더라도 클라이언트가 원격 PC에 남아 있습니다.
anyconnect ssl dtls	SSL VPN 연결을 설정하여 DTLS for CVC를 활성화합니다.
show run webvpn	**anyconnect** 명령을 비롯하여 WebVPN에 대한 컨피그레이션 정보를 표시합니다.

anyconnect profiles(group-policy or username attributes)

Cisco AnyConnect VPN Client(CVC) 사용자에게 다운로드될 CVC 프로필 패키지를 지정하려면 그룹 정책 webvpn 또는 사용자 이름 특성 webvpn 컨피그레이션 모드에서 **anyconnect profiles** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect profiles {value *profile* **| none}**

no anyconnect profiles {value *profile* **| none } [type** *type***]**

구문 설명

value *profile*	프로필의 이름.
none	ASA에서 프로필을 다운로드하지 않습니다.
type *type*	표준 AnyConnect 프로필에 해당하는 사용자 또는 임의의 영숫자 값.

기본값

기본값은 none입니다. ASA에서 프로필을 다운로드하지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
8.3(1)	선택적 유형인 **value**를 도입했습니다.
8.4(1)	**anyconnect profiles** 명령이 **svc profiles** 명령을 대체했습니다.

사용 지침

그룹 정책 webvpn 또는 사용자 이름 특성 webvpn 컨피그레이션 모드에서 이 명령을 입력하면 ASA는 그룹 정책 또는 사용자 이름에 따라 CVC 사용자에게 프로필을 다운로드할 수 있습니다. 모든 CVC 사용자에게 CVC 프로필을 다운로드하려면 webvpn 컨피그레이션 모드에서 이 명령을 사용합니다.

CVC 프로필은 CVC가 CVC 사용자 인터페이스에 나타날 연결 엔트리를 구성하기 위해 사용하는 컨피그레이션 매개변수의 그룹입니다. 여기에는 호스트 컴퓨터의 이름 및 주소도 포함됩니다. CVC 사용자 인터페이스를 통해 프로필을 만들고 저장할 수 있습니다. 또한 텍스트 편집기로 이 파일을 편집하고 사용자 인터페이스에서 제공하지 않는 고급 매개변수를 설정할 수도 있습니다.

CVC 설치에는 하나의 프로필 템플릿(cvcprofile.xml)이 포함되어 있는데, 이를 수정하고 기반으로 활용하여 다른 프로필 파일을 만들 수 있습니다. CVC 프로필 편집에 대한 자세한 내용은 *Cisco AnyConnect VPN Client 관리자 설명서*를 참조하십시오.

예

다음 예에서는 사용자가 **anyconnect profiles value** 명령을 입력합니다. 그러면 사용 가능한 프로필이 표시됩니다.

```
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

그런 다음 사용자는 CVC 프로필 sales를 사용하도록 그룹 정책을 구성합니다.

```
ciscoasa(config-group-webvpn)# anyconnect profiles sales
```

관련 명령

명령	설명
show webvpn anyconnect	설치된 AnyConnect 클라이언트에 대한 정보를 표시합니다.
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect image	ASA에서 원격 PC에 다운로드하기 위해 캐시 메모리에서 확장하는 AnyConnect 클라이언트 패키지 파일을 지정합니다.

anyconnect profiles(webvpn)

어떤 파일을 ASA에서 캐시 메모리에 로드하고 CVC 사용자의 그룹 정책 및 사용자 이름 특성에 사용할 수 있도록 제공하는 프로필 패키지로 지정하려면 webvpn 컨피그레이션 모드에서 **anyconnect profiles** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하고 ASA의 캐시 메모리에서 패키지 파일의 로드를 취소하게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect profiles {*profile path*}

no anyconnect profiles {*profile path*}

구문 설명

path	ASA의 플래시 메모리에 있는 프로필 파일의 경로 및 파일 이름
profile	캐시 메모리에 만들 프로필의 이름

기본값

기본값은 none입니다. ASA는 캐시 메모리에 프로필 패키지를 로드하지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
8.4(1)	**anyconnect profiles** 명령이 **svc profiles** 명령을 대체했습니다.

사용 지침

CVC 프로필은 CVC가 CVC 사용자 인터페이스에 나타날 연결 엔트리를 구성하기 위해 사용하는 컨피그레이션 매개변수의 그룹입니다. 여기에는 호스트 컴퓨터의 이름 및 주소도 포함됩니다. CVC 사용자 인터페이스를 통해 프로필을 만들고 저장할 수 있습니다.

또한 텍스트 편집기로 이 파일을 편집하고 사용자 인터페이스에서 제공하지 않는 고급 매개변수를 설정할 수도 있습니다. CVC 설치에는 하나의 프로필 템플릿(cvcprofile.xml)이 포함되어 있는데, 이를 수정하고 기반으로 활용하여 다른 프로필 파일을 만들 수 있습니다. CVC 프로필 편집에 대한 자세한 내용은 *Cisco AnyConnect VPN Client 관리자 설명서*를 참조하십시오.

새 CVC 프로필을 만들고 플래시 메모리에 업로드한 다음 XML 파일을 ASA에 프로필로 식별합니다. 이를 위해 webvpn 컨피그레이션 모드에서 **anyconnect profiles** 명령을 사용합니다. 이 명령을 입력하면 파일이 ASA의 캐시 메모리에 로드됩니다. 그러면 그룹 정책 webvpn 컨피그레이션 또는 사용자 이름 특성 컨피그레이션 모드에서 **anyconnect profiles** 명령을 사용하여 그룹 또는 사용자에 대해 이 프로필을 지정할 수 있습니다.

예

다음 예에서는 사용자가 CVC 설치 시 제공된 cvcprofile.xml 파일로 2개의 새 프로필 파일(sales_hosts.xml, engineering_hosts.xml)을 이미 만들었고 ASA의 플래시 메모리에 업로드한 상태입니다.

이제 사용자는 ASA에 이 파일을 CVC 프로필로 식별하면서 *sales* 및 *engineering*이라는 이름을 지정합니다.

```
ciscoasa(config-webvpn)# anyconnect profiles sales disk0:sales_hosts.xml
ciscoasa(config-webvpn)# anyconnect profiles engineering disk0:engineering_hosts.xml
```

dir cache:stc/profiles 명령을 입력하면 캐시 메모리에 로드되었던 프로필을 표시합니다.

```
ciscoasa(config-webvpn)# dir cache:stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg

2428928 bytes total (18219008 bytes free)
ciscoasa(config-webvpn)#
```

이 프로필은 그룹 정책 webvpn 컨피그레이션 또는 사용자 이름 특성 컨피그레이션 모드에서 **svc profiles** 명령에 사용할 수 있습니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

관련 명령

명령	설명
show webvpn anyconnect	설치된 AnyConnect 클라이언트에 대한 정보를 표시합니다.
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect image	ASA에서 원격 PC에 다운로드하기 위해 캐시 메모리에서 확장하는 AnyConnect 패키지 파일을 지정합니다.

anyconnect ssl compression

특정 그룹 또는 사용자에 대해 SSL VPN 연결을 통한 http 데이터의 압축을 활성화하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect ssl compression** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect ssl compression {deflate | lzs | none}

no anyconnect ssl compression {deflate | lzs | none}

구문 설명

deflate	deflate 압축 알고리즘을 활성화합니다.
lzs	무상태(stateless) 압축 알고리즘을 활성화합니다.
none	압축을 비활성화합니다.

기본값

기본적으로 압축은 none(비활성)으로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(2)	**anyconnect compression** 명령을 도입했습니다.

사용 지침

SSL VPN 연결에서는 webvpn 컨피그레이션 모드에서 구성된 **compression** 명령이 그룹 정책 및 사용자 이름 webvpn 모드에서 구성된 **anyconnect ssl compression** 명령을 재정의합니다.

예

다음 예에서는 그룹 정책 sales에 대해 SVC 압축이 비활성화됩니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl compression none
```

관련 명령

명령	설명
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect keepalive	원격 컴퓨터의 클라이언트가 SSL VPN 연결을 통해 ASA에 keepalive 메시지를 보내는 빈도를 지정합니다.
anyconnect keep-installer	클라이언트의 자동 제거 기능을 비활성화합니다. 클라이언트는 향후 연결을 위해 원격 PC에 계속 설치되어 있습니다.
anyconnect rekey	클라이언트가 SSL VPN 연결에 대해 rekey를 수행할 수 있게 합니다.
compression	모든 SSL, WebVPN, IPsec VPN 연결에 대해 압축을 활성화합니다.
show webvpn anyconnect	설치된 SSL VPN 클라이언트에 대한 정보를 표시합니다.

anyconnect ssl df-bit-ignore

특정 그룹 또는 사용자에 대해 SSL VPN 연결에서 패킷의 강제 단편화를 활성화하려면(패킷이 터널을 통과할 수 있게 함) 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect ssl df-bit-ignore** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect ssl df-bit-ignore {enable | disable}

no anyconnect ssl df-bit-ignore

구문 설명

enable	AnyConnect(SSL)에 대해 DF 비트 무시를 활성화합니다.
disable	AnyConnect(SSL)에 대해 DF 비트를 비활성화합니다.

기본값

DF 비트 무시는 *disabled*로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령의 **anyconnect ssl df-bit-ignore** 형식이 **svc df-bit-ignore**를 대체했습니다.

사용 지침

이 기능을 DF 비트가 설정된 패킷의 강제 단편화를 허용하여 이 패킷이 터널을 통과할 수 있게 합니다. 예를 들면, 네트워크에서 TCP MSS 협상에 제대로 응답하지 않는 서버에 사용할 수 있습니다.

예

다음 예에서는 그룹 정책 sales에 대해 DF 비트 무시가 활성화됩니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl df-bit-ignore enable
```

관련 명령

명령	설명
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect keepalive	원격 컴퓨터의 클라이언트가 SSL VPN 연결을 통해 ASA에 keepalive 메시지를 보내는 빈도를 지정합니다.
anyconnect keep-installer	클라이언트의 자동 제거 기능을 비활성화합니다. 클라이언트는 향후 연결을 위해 원격 PC에 계속 설치되어 있습니다.
anyconnect rekey	클라이언트가 SSL VPN 연결에 대해 rekey를 수행할 수 있게 합니다.

anyconnect ssl dtls enable

Cisco AnyConnect VPN Client로 SSL VPN 연결을 설정하는 특정 그룹 또는 사용자에 대해 인터페이스에서 DTLS(Datagram Transport Layer Security) 연결을 활성화하려면 그룹 정책 webvpn 또는 사용자 이름 특성 webvpn 컨피그레이션 모드에서 **anyconnect ssl dtls enable** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect ssl dtls enable *interface*

no anyconnect ssl dtls enable *interface*

구문 설명

interface	인터페이스의 이름

기본값

기본값은 enabled입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
8.4(1)	**anyconnect ssl dtls** 명령이 **svc dtls** 명령을 대체했습니다.

사용 지침

DTLS를 활성화하면 SSL VPN 연결을 설정하는 AnyConnect 클라이언트에서 2개의 동시 터널, 즉 SSL 터널과 DTLS 터널을 사용할 수 있게 됩니다. DTLS를 사용하면 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제가 방지되며, 패킷 지연에 민감한 실시간 애플리케이션의 성능이 향상됩니다.

DTLS를 활성화하지 않을 경우 SSL VPN 연결을 설정하는 AnyConnect 클라이언트 사용자는 SSL 터널로만 연결합니다.

이 명령은 특정 그룹 또는 사용자에 대해 DTLS를 활성화합니다. 모든 AnyConnect 클라이언트 사용자에게 DTLS를 활성화하려면 webvpn 컨피그레이션 모드에서 **anyconnect ssl dtls enable** 명령을 사용합니다.

예

다음 예에서는 그룹 정책 *sales*에 대해 그룹 정책 webvpn 컨피그레이션 모드를 시작하고 DTLS를 활성화합니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl dtls enable
```

관련 명령

명령	설명
dtls port	DTLS를 위한 UDP 포트를 지정합니다.
anyconnect dtls	SSL VPN 연결을 설정하는 그룹 또는 사용자를 위해 DTLS를 활성화합니다.
vpn-tunnel-protocol	SSL을 비롯하여 ASA에서 원격 액세스에 허용하는 VPN 프로토콜을 지정합니다.

anyconnect ssl keepalive

원격 클라이언트가 SSL VPN 연결을 통해 ASA에 보내는 keepalive 메시지의 빈도를 구성하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect ssl keepalive** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하고 그 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect ssl keepalive {**none** | *seconds*}

no anyconnect ssl keepalive {**none** | *seconds*}

구문 설명

none	keepalive 메시지를 비활성화합니다.
seconds	keepalive 메시지를 활성화하고 메시지의 빈도를 15초~600초의 범위에서 지정합니다.

기본값

기본값은 20초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.
8.0(3)	기본 설정을 disabled에서 20초로 변경했습니다.
8.4(1)	**anyconnect ssl keepalive** 명령이 **svc keepalive** 명령을 대체했습니다.

사용 지침

Cisco SVC(SSL VPN Client)와 Cisco AnyConnect VPN Client 모두 ASA와 SSL VPN 연결을 설정할 때 keepalive 메시지를 보낼 수 있습니다.

keepalive 메시지의 빈도(초 단위로 지정)를 조정하여 프록시, 방화벽 또는 NAT 디바이스를 지나는 SSL VPN 연결이 디바이스에서 연결의 유휴 시간을 제한하더라도 계속 유지되게 할 수 있습니다.

또한 이 빈도를 조정함으로써 원격 사용자가 소켓 기반 애플리케이션(예: Microsoft Outlook, Microsoft Internet Explorer)을 능동적으로 실행하고 있지 않을 때 클라이언트의 연결이 끊겼다가 다시 연결되는 현상을 방지할 수 있습니다.

참고 Keepalive는 기본적으로 활성화되어 있습니다. keepalive를 비활성화할 경우 장애 조치 상황에서 SSL VPN 클라이언트 세션이 스탠바이 디바이스에 전달되지 않습니다.

예

다음 예에서는 사용자가 기존 그룹 정책인 *sales*에 대해 ASA를 구성하여 클라이언트에서 300초(5분)의 빈도로 keepalive 메시지를 보낼 수 있게 합니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl keepalive 300
```

관련 명령

명령	설명
anyconnect	특정 그룹 또는 사용자에 대해 SSL VPN 클라이언트를 활성화하거나 요구합니다.
anyconnect dpd-interval	ASA에서 DPD(Dead Peer Detection)를 활성화하고 클라이언트 또는 ASA에서 DPD를 수행하는 빈도를 설정합니다.
anyconnect keep-installer	클라이언트의 자동 제거 기능을 비활성화합니다. 클라이언트는 향후 연결을 위해 원격 PC에 계속 설치되어 있습니다.
anyconnect ssl rekey	클라이언트에서 세션에 대해 rekey를 수행할 수 있게 합니다.

anyconnect ssl rekey

원격 클라이언트가 SSL VPN 연결에 대해 rekey를 수행할 수 있게 하려면 그룹 정책 webvpn 또는 사용자 이름 webvpn 컨피그레이션 모드에서 **anyconnect ssl rekey** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect ssl rekey {method {ssl | new-tunnel} | time *minutes* **| none}**

no anyconnect ssl rekey {method {ssl | new-tunnel} | time *minutes* **| none}**

구문 설명

method ssl	클라이언트가 rekey 과정에서 새 터널을 설정하게 합니다.
method new-tunnel	클라이언트가 rekey 과정에서 새 터널을 설정하게 합니다.
method none	rekey를 비활성화합니다.
time *minutes*	세션 시작부터 rekey가 수행될 때까지의 시간(분)을 지정합니다. 범위는 4분~10080분(1주)입니다.

기본값

기본값은 none(비활성)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
그룹 정책 webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 **svc rekey**로 도입했습니다.
8.0(2)	"man in the middle" 공격의 가능성을 방지하기 위해 **svc rekey method ssl** 명령의 동작을 **svc rekey method new-tunnel** 명령의 동작으로 변경했습니다.
8.4(1)	**anyconnect ssl rekey** 명령이 **svc rekey** 명령을 대체했습니다.

사용 지침

Cisco AnyConnect Secure Mobility Client는 ASA과의 SSL VPN 연결에 대해 rekey를 수행할 수 있습니다. rekey 방식을 **ssl** 또는 **new-tunnel**로 구성하면 rekey 과정에서 SSL 재협상이 일어나지 않고 클라이언트가 새 터널을 설정합니다.

예

다음 예에서는 사용자가 그룹 정책 *sales*에 속하는 원격 클라이언트가 rekey 과정에서 SSL과 재협상하고 세션 시작 30분 후에 rekey가 수행되도록 지정합니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anycoanynnect ssl rekey method ssl
ciscoasa(config-group-webvpn)# anyconnect ssl rekey time 30
```

관련 명령

명령	설명
anyconnect enable	특정 그룹 또는 사용자에 대해 AnyConnect Secure Mobility Client를 활성화하거나 요구합니다.
anyconnect dpd-interval	ASA에서 DPD(Dead Peer Detection)를 활성화하고 AnyConnect Secure Mobility Client 또는 ASA에서 DPD를 수행하는 빈도를 설정합니다.
anyconnect keepalive	원격 컴퓨터의 AnyConnect Secure Mobility Client가 ASA에 keepalive 메시지를 보내는 빈도를 지정합니다.
anyconnect keep-installer	원격 컴퓨터에 AnyConnect Secure Mobility Client를 영구 설치할 수 있게 합니다.

anyconnect-custom(버전 9.0~9.2)

사용자 지정 특성의 값을 설정하거나 업데이트하려면 anyconnect-custom-attr 컨피그레이션 모드에서 **anyconnect-custom** 명령을 사용합니다. 사용자 지정 특성의 값을 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect-custom *attr-name* **value** *attr-value*

anyconnect-custom *attr-name* **none**

no anyconnect-custom *attr-name*

구문 설명

attr-name	현재 그룹 정책에 속한 특성의 이름이며, **anyconnnect-custom-attr** 명령에 의해 정의됩니다.
none	즉시 기본 작업을 수행합니다.
value *attr-value*	특성 값을 포함하는 문자열. 연결 설정 과정에서 이 값이 특성 이름과 연관되어 클라이언트에 전달됩니다. 최대 길이는 450자입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
anyconnect-custom-attr 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 그룹 정책에서 사용자 지정 특성의 값을 설정합니다. *AnyConnect 관리자 설명서*에서는 해당 릴리스에 적용되는 사용자 지정 특성에 유효한 값의 목록을 제공합니다. 사용자 지정 특성은 **anyconnect-custom-attr** 명령으로 생성합니다.

이 명령은 다중 인스턴스가 지원되므로 하나의 특성에 여러 값을 구현할 수 있습니다. 어떤 특성 이름과 관련된 모든 데이터는 CLI에 입력되는 순서대로 클라이언트에 전달됩니다. 여러 행으로 된 값의 각 행은 제거할 수 없습니다.

이 명령의 **no** 형식은 **value** 또는 **none** 키워드를 허용하지 않습니다.

어떤 특성 이름과 관련된 데이터가 여러 CLI 행으로 입력되면 이는 하나로 연결되고 뉴라인 문자(\n)에 의해 구분되는 문자열로 엔드포인트에 보내집니다 .

예

다음 예에서는 AnyConnect Deferred Update를 위한 사용자 지정 특성을 구성합니다.

```
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed true
```

관련 명령

명령	설명
show run webvpn	**anyconnect** 명령을 비롯하여 WebVPN에 대한 컨피그레이션 정보를 표시합니다.
show run group-policy	현재 그룹 정책에 대한 컨피그레이션 정보를 표시합니다.
anyconnect-custom-attr	사용자 지정 특성을 만듭니다.

anyconnect-custom(버전 9.3 이상)

사용자 지정 특성의 값을 설정하거나 업데이트하려면 group-policy 또는 dynamic-access-policy-record 컨피그레이션 모드에서 **anyconnect-custom** 명령을 사용합니다. 사용자 지정 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect-custom *attr-type* **value** *attr-name*

anyconnect-custom *attr-type* **none**

no anyconnect-custom *attr-type*

구문 설명

attr-type	**anyconnnect-custom-attr** 명령에 의해 정의된 사용자 지정 특성의 유형.
none	이 사용자 지정 특성이 해당 정책에서 명시적으로 제외됩니다.
value *attr-name*	**anyconnect-custom-data** 명령에 의해 정의된 사용자 지정 특성 값의 이름. 사용자 지정 특성 유형 및 명명된 값은 연결 설정 과정에서 클라이언트에 전달됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
group-policy 또는 dynamic-access-policy-record	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 새롭게 정의했습니다.

사용 지침

이 명령은 그룹 정책 또는 DAP에서 사용자 지정 특성의 값을 설정합니다.

*AnyConnect 관리자 설명서*에서는 해당 릴리스에 적용되는 사용자 지정 특성에 유효한 값의 목록을 제공합니다. 사용자 지정 특성은 **anyconnect-custom-attr** 및 **anyconnect-custom-data** 명령으로 생성됩니다.

이 명령의 **no** 형식은 **none** 키워드를 허용하지 않습니다.

예

다음 예에서는 AnyConnect Deferred Update를 위한 사용자 지정 특성을 구성합니다.

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
ciscoasa(config-webvpn)# exit
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed def-allowed
```

관련 명령

명령	설명
show run webvpn	**anyconnect** 명령을 비롯하여 WebVPN에 대한 컨피그레이션 정보를 표시합니다.
show run group-policy	현재 그룹 정책에 대한 컨피그레이션 정보를 표시합니다.
show running-config dynamic-access-policy-record	DAP 정책에 쓰이는 사용자 지정 특성을 표시합니다.
anyconnect-custom-attr	이 명령에 쓰이는 사용자 지정 특성 유형을 만듭니다.
anyconnect-custom-data	이 명령에 쓰이는 사용자 지정 특성의 명명된 값을 생성합니다.

anyconnect-custom-attr(버전 9.0~9.2)

사용자 지정 특성을 만들려면 Anyconnect-custom-attr 컨피그레이션 모드에서 **anyconnect-custom-attr** 명령을 사용합니다. 사용자 지정 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

[no] anyconnect-custom-attr *attr-name* **[description** *description***]**

구문 설명

attr-name	특성의 이름. 이 이름은 그룹 정책 구문 및 종합 인증 프로토콜 메시지에서 참조합니다. 최대 길이는 32자입니다.
description *description*	특성의 용도에 대한 자유 형식의 설명. 그룹 정책 특성 컨피그레이션 모드에서 이 사용자 지정 특성을 참조할 때 명령 도움말에 이 텍스트가 나타납니다. 최대 길이는 128자입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Anyconnect-custom-attr 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 특수한 AnyConnect 기능을 지원하기 위해 사용자 지정 특성을 만듭니다. 특정 기능을 위한 사용자 지정 특성을 만든 다음 그룹 정책에 추가합니다. 그러면 이 기능이 VPN 클라이언트에 적용될 수 있습니다. 이 명령은 정의된 모든 특성 이름이 고유함을 보장합니다.

일부 AnyConnect 버전에서는 기능을 구성하는 데 사용자 지정 특성을 사용합니다. 각 버전의 릴리스 정보 및 *AnyConnect 관리자 설명서*에서 사용자 지정 특성을 필요로 하는 기능의 목록을 제공합니다.

그룹 정책에서 사용 중인 특성의 정의를 제거하려 하면 오류 메시지가 표시되고 해당 작업은 실패합니다. 사용자가 이미 사용자 지정 특성으로 존재하는 특성을 추가하려 할 경우, 그 설명에 대한 변경 사항은 모두 반영되지만 명령 자체는 무시됩니다.

이 명령은 다중 인스턴스가 지원되므로 하나의 특성에 여러 값을 구현할 수 있습니다. 어떤 특성 이름과 관련된 모든 데이터는 CLI에 입력되는 순서대로 클라이언트에 전달됩니다. 여러 행으로 된 값의 각 행은 제거할 수 없습니다.

예

다음 예에서는 AnyConnect Deferred Update를 위한 사용자 지정 특성을 구성합니다.

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

관련 명령

명령	설명
show run webvpn	**anyconnect** 명령을 비롯하여 WebVPN에 대한 컨피그레이션 정보를 표시합니다.
show run group-policy	현재 그룹 정책에 대한 컨피그레이션 정보를 표시합니다.
anyconnect-custom	사용자 지정 특성 유형 및 명명된 값을 그룹 정책 또는 동적 액세스 정책과 연결합니다.

anyconnect-custom-attr(버전 9.3 이상)

사용자 지정 특성 유형을 만들려면 config-webvpn 컨피그레이션 모드에서 **anyconnect-custom-attr** 명령을 사용합니다. 사용자 지정 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

[no] anyconnect-custom-attr *attr-type* **[description** *description***]**

구문 설명

attr-type	특성의 유형. 이 유형은 그룹 정책 구문 및 DAP 정책 구문 그리고 종합 인증 프로토콜 메시지에서도 참조합니다. 최대 길이는 32자입니다.
description *description*	특성의 용도에 대한 자유 형식의 설명. 그룹 정책 특성 컨피그레이션 모드에서 이 사용자 지정 특성을 참조할 때 명령 도움말에 이 텍스트가 나타납니다. 최대 길이는 자입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
config-webvpn	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 새롭게 정의했습니다.

사용 지침

이 명령은 특수한 AnyConnect 기능을 지원하기 위해 사용자 지정 특성을 만듭니다. 어떤 기능을 위한 사용자 지정 특성을 만든 다음 그에 대한 값을 정의하고 그룹 정책에 추가합니다. 그러면 관련 기능이 VPN 클라이언트에 적용될 수 있습니다. 이 명령은 정의된 모든 특성 이름이 고유함을 보장합니다.

일부 AnyConnect 버전에서는 기능을 구성하는 데 사용자 지정 특성을 사용합니다. 각 버전의 릴리스 정보 및 *AnyConnect 관리자 설명서*에서 사용자 지정 특성을 필요로 하는 기능의 목록을 제공합니다.

그룹 정책에서 사용 중인 특성의 정의를 제거하려 하면 오류 메시지가 표시되고 해당 작업은 실패합니다. 사용자가 이미 사용자 지정 특성으로 존재하는 특성을 추가하려 할 경우, 그 설명에 대한 변경 사항은 모두 반영되지만 명령 자체는 무시됩니다.

예

다음 예에서는 AnyConnect Deferred Update를 위한 사용자 지정 특성을 구성합니다.

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
```

관련 명령

명령	설명
show run webvpn	**anyconnect** 명령을 비롯하여 WebVPN에 대한 컨피그레이션 정보를 표시합니다.
show run group-policy	현재 그룹 정책에 대한 컨피그레이션 정보를 표시합니다.
show running-config dynamic-access-policy-record	DAP 정책에 쓰이는 사용자 지정 특성을 표시합니다.
anyconnect-custom	정책에 사용할 사용자 지정 특성의 값을 설정합니다.
anyconnect-custom-data	사용자 지정 특성의 명명된 값을 생성합니다.

anyconnect-custom-data

사용자 지정 특성의 명명된 값을 생성하려면 글로벌 컨피그레이션 모드에서 **anyconnect-custom-data** 명령을 사용합니다. 사용자 지정 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect-custom-data *attr-type attr-name attr-value*

no anyconnect-custom-data *attr-type attr-name*

구문 설명

attr-type	**anyconnect-custom-attr**을 사용하여 이미 정의한 특성의 유형.
attr-name	지정된 값을 갖는 특성의 이름. 이는 group-policy 및 dynamic-access-policy-record 컨피그레이션 모드에서 참조할 수 있습니다.
attr-value	특성 값을 포함하는 문자열. 최대 길이는 420자입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 특수한 AnyConnect 기능을 지원하기 위해 사용자 지정 특성의 명명된 값을 정의합니다. 어떤 기능을 위한 사용자 지정 특성을 만든 다음 그에 대한 값을 정의하고 DAP 또는 그룹 정책에 추가합니다. 그러면 관련 기능이 VPN 클라이언트에 적용될 수 있습니다.

일부 AnyConnect 버전에서는 기능을 구성하는 데 사용자 지정 특성을 사용합니다. 각 버전의 릴리스 정보 및 *AnyConnect 관리자 설명서*에서 사용자 지정 특성을 필요로 하는 기능의 목록을 제공합니다.

그룹 정책에서 사용 중인 특성의 명명된 값을 제거하려 하면 오류 메시지가 표시되고 해당 작업은 실패합니다.

이 명령은 다중 인스턴스가 지원되므로 하나의 특성에 여러 값을 구현할 수 있습니다. 어떤 특성 이름과 관련된 모든 데이터는 CLI에 입력되는 순서대로 클라이언트에 전달됩니다. 여러 행으로 된 값의 각 행은 제거할 수 없습니다.

예

다음 예에서는 AnyConnect Deferred Update를 위한 사용자 지정 특성을 구성합니다.

```
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

관련 명령

명령	설명
show run webvpn	**anyconnect** 명령을 비롯하여 WebVPN에 대한 컨피그레이션 정보를 표시합니다.
show run group-policy	현재 그룹 정책에 대한 컨피그레이션 정보를 표시합니다.
show running-config dynamic-access-policy-record	DAP 정책에 쓰이는 사용자 지정 특성을 표시합니다.
show run anyconnect-custom-data	모든 정의된 사용자 지정 특성의 명명된 값을 표시합니다.
anyconnect-custom	사용자 지정 특성 유형 및 값을 그룹 정책 또는 DAP와 연결합니다.
anyconnect-custom-attr	사용자 지정 특성을 만듭니다.

anyconnect-essentials

ASA에서 AnyConnect Essentials를 활성화하려면 그룹 정책 webvpn 컨피그레이션 모드에서 **anyconnect-essentials** 명령을 사용합니다. AnyConnect Essentials의 사용을 비활성화하고 그 대신 프리미엄 AnyConnect 클라이언트를 활성화하려면 이 명령의 **no** 형식을 사용합니다.

anyconnect-essentials

no anyconnect-essentials

기본값

AnyConnect Essentials가 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

전 기능 AnyConnect 클라이언트 라이센스가 설치되었다는 가정 하에 전 기능 AnyConnect SSL VPN Client 사용과 AnyConnect Essentials SSL VPN Client 사용으로 전환하려면 이 명령을 사용합니다. AnyConnect Essentials는 별도의 라이센스가 제공되는 SSL VPN 클라이언트로서 전적으로 ASA에서 구성되며, 다음 예외와 함께 프리미엄 AnyConnect 기능을 제공합니다.

- CSD(HostScan/Vault/Cache Cleaner 포함) 없음
- 클라이언트리스 SSL VPN 없음

AnyConnect Essentials 클라이언트는 Microsoft Windows Vista, Windows Mobile, Windows XP, Windows 2000, Linux 또는 Macintosh OS X을 실행하는 원격 최종 사용자가 Cisco SSL VPN Client의 이점을 누릴 수 있게 합니다.

AnyConnect Essentials 라이센스는 **anyconnect-essentials** 명령으로 활성화하거나 비활성화합니다. 이 명령은 ASA에 AnyConnect Essentials 라이센스를 설치한 후에 사용 가능합니다. 이 라이센스가 없으면 이 명령은 다음 오류 메시지를 반환합니다.

```
ERROR: Command requires AnyConnect Essentials license
```

참고 이 명령은 AnyConnect Essentials 사용을 활성화하거나 비활성화하는 기능만 담당합니다. AnyConnect Essentials *라이센스* 자체는 **anyconnect-essentials** 명령의 설정으로부터 영향을 받지 않습니다.

AnyConnect Essentials 라이센스가 활성화되면 AnyConnect 클라이언트는 Essentials 모드를 사용하며 클라이언트리스 SSL VPN 액세스는 비활성화됩니다. AnyConnect Essentials 라이센스가 비활성화되면 AnyConnect 클라이언트는 전 기능 AnyConnect SSL VPN Client 라이센스를 사용합니다.

참고 이 명령은 ASAv에서는 지원되지 않습니다. 자세한 내용은 라이센스 설명서를 참조하십시오.

활성 상태의 클라이언트리스 SSL VPN 연결이 있는 상태에서 AnyConnect Essentials 라이센스를 활성화할 경우 모든 연결이 로그오프되며 다시 설정되어야 합니다.

예 다음 예에서는 사용자가 webvpn 컨피그레이션 모드를 시작하고 AnyConnect Essentials VPN 클라이언트를 활성화합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect-essentials
```

apcf

Application Profile Customization Framework 프로필을 활성화하려면 webvpn 컨피그레이션 모드에서 **apcf** 명령을 사용합니다. 특정 APCF 스크립트를 비활성화하려면 이 명령의 **no** 형식을 사용합니다. 모든 APCF 스크립트를 비활성화하려면 이 명령의 **no** 형식을 인수 없이 사용합니다.

apcf URL/filename.ext

no apcf [URL/filename.ext]

구문 설명

filename.extension	APCF 사용자 지정 스크립트의 이름을 지정합니다. 이 스크립트는 항상 XML 형식입니다. 확장자는 .xml, .txt, .doc, 기타 여러 확장자가 가능합니다.
URL	ASA에 로드하고 사용할 APCF 프로필의 위치를 지정합니다. URL http://, https://, tftp://, ftp://, flash:/, disk#:/' 중 하나를 사용합니다. URL이 서버, 포트, 경로를 포함할 수 있습니다. 파일 이름만 제공할 경우 기본 URL은 flash:/입니다. **copy** 명령을 사용하여 APCF 프로필을 플래시 메모리에 복사할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표는 명령을 입력하는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

apcf 명령은 ASA에서 비표준 웹 애플리케이션 및 웹 리소스를 처리하면서 WebVPN 연결을 통해 올바르게 렌더링할 수 있게 해줍니다. APCF 프로필은 하나의 스크립트로 구성되는데, 이는 특정 애플리케이션을 위해 언제(pre, post), 어디서(header, body, request, response), 어떤 데이터를 변환할지 지정합니다.

ASA에서 여러 APCF 프로필을 사용할 수 있습니다. 그러면 ASA는 오래된 것부터 시작하여 각 프로필을 적용합니다.

APCF 명령은 Cisco TAC의 지원을 받을 때만 사용하는 것이 좋습니다.

예

다음 예에서는 플래시 메모리의 /apcf에 위치한 apcf1이라는 APCF를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf flash:/apcf/apcf1.xml
ciscoasa(config-webvpn)#
```

이 예에서는 apcf2.xml이라는 APCF를 활성화하는 방법을 보여줍니다. 이 파일은 myserver라는 HTTPS 서버에 있으며 포트는 1440, 경로는 /apcf입니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
proxy-bypass	특정 애플리케이션을 위해 최소한의 콘텐츠 재작성을 구성합니다.
rewrite	트래픽이 ASA를 지날지 여부를 지정합니다.
show running config webvpn apcf	APCF 컨피그레이션을 표시합니다.

appl-acl

어떤 세션에 적용할, 이미 구성된 웹 타입 ACL을 식별하려면 dap webvpn 컨피그레이션 모드에서 **appl-acl** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 모든 웹 타입 ACL을 제거하려면 이 명령의 **no** 형식을 인수 없이 사용합니다.

appl-acl [*identifier***]**

no appl-acl [*identifier***]**

구문 설명

identifier	이미 구성된 웹 타입 ACL의 이름. 최대 길이는 240자입니다.

기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Dap webvpn 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

웹 타입 ACL을 구성하려면 글로벌 컨피그레이션 모드에서 **access-list webtype** 명령을 사용합니다.

DAP 정책에 둘 이상의 웹 타임 ACL을 적용하려면 **appl-acl** 명령을 여러 번 사용합니다.

예

다음 예에서는 newacl이라는 이미 구성된 웹 타입 ACL을 동적 액세스 정책에 적용하는 방법을 보여줍니다.

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# appl-acl newacl
```

관련 명령

명령	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
access-list_webtype	웹 타입 ACL을 만듭니다.

application-access

인증된 WebVPN 사용자에게 표시되는 WebVPN Home 페이지의 Application Access 필드 및 사용자가 애플리케이션을 선택할 때 시작하는 Application Access 창을 사용자 지정하려면 사용자 지정 컨피그레이션 모드에서 **application-access** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

구문 설명

message	Application Access 필드의 제목 아래 표시되는 메시지를 변경합니다.
style	Application Access 필드의 스타일을 변경합니다.
text	Application Access 필드의 텍스트를 변경합니다.
title	Application Access 필드의 제목을 변경합니다.
value	표시되는 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자).
window	Application Access 창을 변경합니다.

기본값

Application Access 필드의 기본 제목 텍스트는 "Application Access"입니다.

Application Access 필드의 기본 제목 스타일은

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase입니다.

Application Access 필드의 기본 메시지 텍스트는 "Start Application Client"입니다.

Application Access 필드의 기본 메시지 스타일은

background-color:#99CCCC;color:maroon;font-size:smaller입니다.

Application Access 창의 기본 창 텍스트는

"Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications."입니다.

Application Access 창의 기본 창 스타일은

background-color:#99CCCC;color:black;font-weight:bold입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 **webvpn** 명령 또는 **tunnel-group webvpn-attributes** 명령을 사용하여 액세스합니다.

style 옵션은 유효한 CSS 매개변수로 나타냅니다. 이 매개변수에 대한 설명은 본 설명서의 범위에 속하지 않습니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹 사이트(www.w3.org)의 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F는 편리한 CSS 매개변수 목록을 포함하고 있으며 www.w3.org/TR/CSS21/propidx.html에서 이용할 수 있습니다.

다음 팁은 WebVPN 페이지에서 가장 자주 바꾸는 페이지 색상을 변경할 때 유용합니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 (HTML에서 인식된다면) 색상의 이름을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며, 각 색상(빨강, 녹색, 파랑)을 나타내는 0~255 범위의 10진수입니다. 쉼표로 구분하여 입력한 값은 해당 강도의 각 색상이 나머지 색상과 조합되는 것을 의미합니다.
- HTML 형식은 #000000이며, 6자리의 16진수입니다. 1번째와 2번째 자리는 빨강을, 3번째와 4번째 자리는 녹색을, 5번째와 6번째는 파랑을 나타냅니다.

참고 손쉽게 WebVPN 페이지를 사용자 지정하려면 ASDM을 사용하는 것이 좋습니다. 색 견본, 미리 보기 등 스타일 요소를 편리하게 구성할 수 있는 기능을 제공합니다.

예

다음 예에서는 Application Access 필드의 배경색을 RGB 16진수 값 66FFFF, 즉 연한 녹색으로 사용자 지정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

관련 명령

명령	설명
application-access hide-details	Application Access 창에서 애플리케이션 세부정보의 표시를 활성화하거나 비활성화합니다.
browse-networks	WebVPN Home 페이지의 Browse Networks 필드를 사용자 지정합니다.
file-bookmarks	WebVPN Home 페이지의 File Bookmarks 제목 또는 링크를 사용자 지정합니다.
web-applications	WebVPN Home 페이지의 Web Application 필드를 사용자 지정합니다.
web-bookmarks	WebVPN Home 페이지의 Web Bookmarks 제목 또는 링크를 사용자 지정합니다.

application-access hide-details

WebVPN Applications Access 창에 표시되는 애플리케이션 세부정보를 숨기려면 사용자 지정 컨피그레이션 모드에서 **application-access hide-details** 명령을 사용합니다. 이 모드는 **webvpn** 명령 또는 **tunnel-group webvpn-attributes** 명령으로 액세스할 수 있습니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

application-access hide-details {**enable** | **disable**}

no application-access [**hide-details** {**enable** | **disable**}]

구문 설명

disable	Application Access 창에서 애플리케이션 세부정보를 숨기지 않습니다.
enable	Application Access 창에서 애플리케이션 세부정보를 숨깁니다.

기본값

기본값은 disabled입니다. Application Access 창에 애플리케이션 세부정보가 나타납니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

예

다음 예에서는 애플리케이션 세부정보의 표시를 비활성화합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access hide-details disable
```

관련 명령

명령	설명
application-access	WebVPN Home 페이지의 Application Access 필드를 사용자 지정합니다.
browse-networks	WebVPN Home 페이지의 Browse Networks 필드를 사용자 지정합니다.
web-applications	WebVPN Home 페이지의 Web Application 필드를 사용자 지정합니다.

3 장

area ~ auto-update timeout 명령

area

OSPF v2 또는 OSPFv3 영역을 만들려면 라우터 컨피그레이션 모드에서 **area** 명령을 사용합니다. 영역을 제거하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id*

no area *area_id*

구문 설명

area_id	생성하는 영역의 ID. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—
IPv6 라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	OSPFv3 지원을 추가했습니다.

사용 지침

생성하는 영역은 어떤 매개변수도 설정되어 있지 않습니다. 영역 매개변수를 설정하려면 해당 **area** 명령을 사용합니다.

예

다음 예에서는 영역 ID가 1인 OSPF 영역을 만드는 방법을 보여줍니다.

```
ciscoasa(config-router)# area 1
ciscoasa(config-router)#
```

관련 명령

명령	설명
area nssa	이 영역을 not-so-stubby 영역으로 정의합니다.
area stub	이 영역을 스텁 영역으로 정의합니다.
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area authentication

OSPFv2 영역에 대한 인증을 활성화하려면 라우터 컨피그레이션 코드에서 **area authentication** 명령을 사용합니다. 영역 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **authentication [message-digest]**

no area *area_id* **authentication [message-digest]**

구문 설명

area_id	인증을 활성화할 영역의 식별자. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
message-digest	(선택 사항) *area_id*에 의해 지정된 영역에 대해 MD5(Message Digest 5) 인증을 활성화합니다.

기본값

영역 인증은 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

지정된 OSPFv2 영역이 없을 경우 이 명령이 입력될 때 생성됩니다. **area authentication** 명령을 **message-digest** 키워드 없이 입력하여 단순 비밀번호 인증을 활성화할 수 있습니다. **message-digest** 키워드를 포함하여 MD5 인증이 활성화됩니다.

예

다음 예에서는 area 1에 대해 MD5 인증을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config-router)# area 1 authentication message-digest
ciscoasa(config-router)#
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area default-cost

스텁 또는 NSSA에 보낸 기본 요약 경로의 비용을 지정하려면 라우터 컨피그레이션 모드 또는 IPv6 라우터 컨피그레이션 모드에서 **area default-cost** 명령을 사용합니다. 비용의 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost** *cost*

구문 설명

area_id	기본 비용을 변경하는 스텁 또는 NSSA의 식별자. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
cost	스텁 또는 NSSA에 사용되는 기본 요약 경로의 비용을 지정합니다. 유효한 값의 범위는 0~65535입니다.

기본값

*cost*의 기본값은 1입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—
IPv6 라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 및 OSPFv3가 지원됩니다.

사용 지침

지정된 영역이 아직 **area** 명령으로 정의되지 않았다면 이 명령은 지정된 매개변수로 영역을 만듭니다.

예

다음 예에서는 스텁 또는 NSSA에 보낸 요약 경로의 기본 비용을 지정하는 방법을 보여줍니다.

```
ciscoasa(config-router)# area 1 default-cost 5
ciscoasa(config-router)#
```

관련 명령

명령	설명
area nssa	이 영역을 not-so-stubby 영역으로 정의합니다.
area stub	이 영역을 스텁 영역으로 정의합니다.
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area filter-list prefix

ABR의 OSPFv2 영역 간에 Type 3 LSA를 통해 광고된 접두사를 필터링하려면 라우터 컨피그레이션 모드에서 **area filter-list prefix** 명령을 사용합니다. 필터를 변경하거나 취소하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **filter-list prefix** *list_name* **{in | out}**

no area *area_id* **filter-list prefix** *list_name* **{in | out}**

구문 설명

area_id	필터링이 구성되는 영역을 식별합니다. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
in	지정된 영역에 인바운드로 광고되는 접두사에 구성된 접두사 목록을 적용합니다.
list_name	접두사 목록의 이름을 지정합니다.
out	지정된 영역에서 아웃바운드로 광고되는 접두사에 구성된 접두사 목록을 적용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

지정된 영역이 아직 **area** 명령으로 정의되지 않았다면 이 명령은 지정된 매개변수로 영역을 만듭니다.

유형 3 LSA만 필터링할 수 있습니다. 사설 네트워크에서 ASBR이 구성된 경우 Type 5 LSA(사설 네트워크를 설명함)를 보냅니다. 이는 공개 영역을 포함한 전체 AS에 플러딩됩니다.

예

다음 예에서는 다른 모든 영역에서 area 1로 보내지는 접두사를 필터링합니다.

```
ciscoasa(config-router)# area 1 filter-list prefix-list AREA_1 in
ciscoasa(config-router)#
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area nssa

어떤 영역을 NSSA로 구성하려면 라우터 컨피그레이션 모드 또는 IPv6 라우터 컨피그레이션 모드에서 **area nssa** 명령을 사용합니다. 영역에서 NSSA 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **nssa [no-redistribution] [default-information-originate [metric-type {1 | 2}] [metric** *value*]] **[no-summary]**

no area *area_id* **nssa [no-redistribution] [default-information-originate [metric-type {1 | 2}] [metric** *value*]] **[no-summary]**

구문 설명

area_id	NSSA로 지정되는 영역을 식별합니다. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
default-information-originate	NSSA 영역에 Type 7 기본 설정을 생성하는 데 사용합니다. 이 키워드는 NSSA ABR 또는 NSSA ASBR에만 적용됩니다.
metric *metric_value*	(선택 사항) OSPF 기본 메트릭 값을 지정합니다. 유효한 값의 범위는 0~16777214입니다.
metric-type {**1** | **2**}	(선택 사항) 기본 경로의 OSPF 메트릭 유형. 유효한 값은 다음과 같습니다. • **1**—type 1 • **2**—type 2 기본값은 2입니다.
no-redistribution	(선택 사항) 라우터가 NSSA ABR일 때 **redistribute** 명령을 사용하여 NSSA 영역이 아닌 일반 영역에만 경로를 가져오려는 경우에 사용합니다.
no-summary	(선택 사항) not-so-stubby 영역이 될 수 있으나 요약 경로는 삽입할 수 없게 합니다.

기본값

기본 설정은 다음과 같습니다.

- NSSA 영역이 정의되지 않습니다.
- **metric-type**은 2입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	• 예	—
IPv6 라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 콘텐츠 모드 및 OSPFv3가 지원됩니다.

사용 지침

지정된 영역이 아직 **area** 명령으로 정의되지 않았다면 이 명령은 지정된 매개변수로 영역을 만듭니다.

어떤 영역에 대해 옵션을 구성하고 나중에 다른 옵션을 지정할 경우 둘 다 설정됩니다. 이를테면 다음 두 명령을 각각 입력할 경우 컨피그레이션에서는 두 옵션이 모두 설정된 하나의 명령이 됩니다.

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area area_id nssa default-information-originate
```

예

다음 예에서는 두 옵션을 각각 설정했을 때 컨피그레이션에서 하나의 명령이 되는 것을 보여줍니다.

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area 1 nssa default-information-originate
ciscoasa(config-rtr)# exit
ciscoasa(config-rtr)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

관련 명령

명령	설명
area stub	이 영역을 스텁 영역으로 정의합니다.
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area range(OSPFv2)

영역 경계에서 경로를 통합하고 요약하려면 라우터 컨피그레이션 모드에서 **area range** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **range** *address mask* **[advertise | not-advertise]**

no area *area_id* **range** *address mask* **[advertise | not-advertise]**

구문 설명

address	서브넷 범위의 IP 주소.
advertise	(선택 사항) Type 3 요약 LSA(link-state advertisement)를 광고하고 생성하기 위해 주소 범위 상태를 설정합니다.
area_id	범위가 구성되는 영역을 식별합니다. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
mask	IP 주소 서브넷 마스크.
not-advertise	(선택 사항) 주소 범위 상태를 DoNotAdvertise로 설정합니다. Type 3 요약 LSA가 억제되고, 구성 요소 네트워크는 다른 네트워크에 숨겨진 상태로 유지됩니다.

기본값

주소 범위 상태는 advertise로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

지정된 영역이 아직 **area** 명령으로 정의되지 않았다면 이 명령은 지정된 매개변수로 영역을 만듭니다.

area range 명령은 오로지 ABR과 함께 어떤 영역에 대해 경로를 통합하거나 요약하는 데 사용합니다. 그러면 단일 요약 경로가 ABR에 의해 다른 영역에 광고됩니다. 라우팅 정보는 영역 경계에서 압축됩니다. 영역의 외부에서는 단일 경로가 각 주소 범위에 광고됩니다. 이러한 동작을 *경로 요약*이라고 합니다. 하나의 영역에 대해 여러 **area range** 명령을 구성할 수 있습니다. 이런 방법으로 OSPF는 각기 다른 여러 주소 범위 세트에 대해 주소를 요약할 수 있습니다.

no area *area_id* **range** *ip_address netmask* **not-advertise** 명령은 **not-advertise** 선택적 키워드만 제거합니다.

예

다음 예에서는 네트워크 10.0.0.0의 모든 서브넷 및 네트워크 192.168.110.0의 모든 호스트에서 단일 요약 경로가 ABR에 의해 다른 영역에 광고되도록 지정합니다.

```
ciscoasa(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
ciscoasa(config-router)# area 0 range 192.168.110.0 255.255.255.0
ciscoasa(config-router)#
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area range(OSPFv3)

영역 경계에서 OSPFv3 경로를 통합하고 요약하려면 IPv6 라우터 컨피그레이션 모드에서 **area range** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **range** *ipv6-prefix*/*prefix-length* **[advertise | not-advertise] [cost** *cost***]**

no area *area_id* **range** *ipv6-prefix*/*prefix-length* **[advertise | not-advertise] [cost** *cost***]**

구문 설명

advertise	(선택 사항) Type 3 요약 LSA를 광고하고 생성하기 위해 범위 상태를 설정합니다.
area_id	경로가 요약될 영역의 식별자를 지정합니다. 이 식별자는 십진수 또는 IPv6 접두사로 지정할 수 있습니다.
cost *cost*	(선택 사항) 목적지까지의 최단 경로를 결정하는 OSPF SPF 계산 과정에 사용되는 이 요약 경로의 메트릭 또는 비용을 지정합니다. 유효한 값의 범위는 0~16777215입니다.
ipv6-prefix	IPv6 접두사를 지정합니다.
not-advertise	(선택 사항) 범위 상태를 DoNotAdvertise로 설정합니다. Type 3 요약 LSA가 억제되고, 구성 요소 네트워크는 다른 네트워크에 숨겨진 상태로 유지됩니다.
prefix-length	IPv6 접두사 길이를 지정합니다.

기본값

기본적으로 범위 상태는 advertise로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
IPv6 라우터 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

지정된 영역이 아직 **area** 명령으로 정의되지 않았다면 이 명령은 지정된 매개변수로 영역을 만듭니다.

area range 명령은 오로지 ABR과 함께 사용합니다. 어떤 영역에 대해 경로를 통합하거나 요약하는 데 쓰입니다. 그러면 단일 요약 경로가 ABR에 의해 다른 영역에 광고됩니다. 라우팅 정보는 영역 경계에서 압축됩니다. 영역의 외부에서는 단일 경로가 각 IPv6 접두사 및 접두사 길이에 대해 광고됩니다. 이러한 동작을 *경로 요약*이라고 합니다. 하나의 영역에 대해 여러 **area range** 명령을 구성할 수 있습니다. 이런 방법으로 OSPFv3는 각기 다른 여러 IPv6 접두사 및 접두사 길이 세트에 대해 경로를 요약할 수 있습니다.

예

다음 예에서는 IPv6 접두사 2000:0:0:4::2, 접두사 길이 2001::/64:에 대해 ABR가 단일 요약 경로를 다른 영역에 광고하도록 지정합니다.

```
ciscoasa(config-router)# area 1 range 2000:0:0:4::2/2001::/64
ciscoasa(config-router)#
```

관련 명령

명령	설명
ipv6 router ospf	OSPFv3의 IPv6 라우터 컨피그레이션 모드를 시작합니다.
show running-config ipv6 router	전역 라우터 컨피그레이션에서 IPv6 명령을 표시합니다.

area stub

어떤 영역을 스텁 영역으로 정의하려면 라우터 컨피그레이션 모드 또는 IPv6 라우터 컨피그레이션 모드에서 **area stub** 명령을 사용합니다. 스텁 영역을 제거하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **stub [no-summary]**

no area *area_id* **stub [no-summary]**

구문 설명

area_id	스텁 영역을 식별합니다. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
no-summary	ABR에서 스텁 영역에 요약 링크 광고를 보내지 못하게 합니다.

기본값

기본 동작은 다음과 같습니다.

- 스텁 영역이 정의되지 않습니다.
- 요약 링크 광고가 스텁 영역에 보내집니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
라우터 컨피그레이션	• 예	—	• 예	—	—
IPv6 라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	OSPFv3 지원을 추가했습니다.

사용 지침

이 명령은 스텁 또는 NSSA에 연결된 ABR에서만 사용합니다.

2개의 스텁 영역 라우터 컨피그레이션 명령이 있습니다. **area stub** 명령과 **area default-cost** 명령입니다. 스텁 영역에 연결된 모든 라우터 및 액세스 서버에서 **area stub** 명령을 통해 이 영역이 스텁 영역으로 구성되어야 합니다. 스텁 영역에 연결된 ABR에서만 **area default-cost** 명령을 사용합니다. **area default-cost** 명령은 ABR에 의해 스텁 영역에 생성된 요약 기본 경로에 대한 메트릭을 제공합니다.

예

다음 예에서는 지정된 영역을 스텁 영역으로 구성합니다.

```
ciscoasa(config-rtr)# area 1 stub
ciscoasa(config-rtr)#
```

관련 명령

명령	설명
area default-cost	스텁 또는 NSSA에 보내진 기본 요약 경로의 비용을 지정합니다.
area nssa	이 영역을 not-so-stubby 영역으로 정의합니다.
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area virtual-link(OSPFv2)

OSPF 가상 링크를 정의하려면 라우터 컨피그레이션 모드에서 **area virtual-link** 명령을 사용합니다. 옵션을 재설정하거나 가상 링크를 제거하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **virtual-link** *router_id* **[authentication [message-digest | null]] [hello-interval** *seconds*] **[retransmit-interval seconds] [transmit-delay** *seconds*] **[dead-interval** *seconds* **[[[[authentication-key[0 | 8]** *key* **] | [message-digest-key** *key_id* **md5 [0 | 8]** *key* **]]]]**

no area *area_id* **virtual-link** *router_id* **[authentication [message-digest | null]] [hello-interval** *seconds*] **[retransmit-interval seconds] [transmit-delay** *seconds*] **[dead-interval** *seconds* **[[[[authentication-key [0 | 8]** *key* **] | [message-digest-key** *key_id* **md5 [0 | 8]** *key* **]]]]**

구문 설명

area_id	가상 링크를 위한 트랜짓 영역의 ID. 이 식별자는 십진수 또는 IP 주소로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
authentication	(선택 사항) 인증 유형을 지정합니다.
authentication-key [0 | 8]*key*	(선택 사항) 인접한 라우팅 디바이스에서 사용할 OSPF 인증 비밀번호를 지정합니다.
dead-interval *seconds*	(선택 사항) 어떤 hello 패킷도 수신되지 않을 경우 인접한 라우팅 디바이스가 다운 상태임을 선언하기 전의 간격을 지정합니다. 유효한 값은 1초~65535초입니다.
hello-interval *seconds*	(선택 사항) 인터페이스에서 보내지는 hello 패킷의 간격을 지정합니다. 유효한 값은 1초~65535초입니다.
md5 [0 | 8] *key*	(선택 사항) 최대 16바이트의 영숫자 키를 지정합니다.
message-digest	(선택 사항) 메시지 다이제스트 인증이 사용되도록 지정합니다.
message-digest-key *key_id*	(선택 사항) MD5 인증을 활성화하고 숫자 인증 키 ID 번호를 지정합니다. 유효한 값은 1~255입니다.
0	암호화되지 않은 비밀번호가 뒤따르도록 지정합니다.
8	암호화된 비밀번호가 뒤따르도록 지정합니다.
null	(선택 사항) 어떤 인증도 사용하지 않도록 지정합니다. OSPF 영역에 대해 구성될 경우 비밀번호 또는 메시지 다이제스트 인증을 재정의합니다.
retransmit-interval *seconds*	(선택 사항) 해당 인터페이스에 속하는 인접 라우터를 위한 LSA 재전송의 간격을 지정합니다. 유효한 값은 1초~65535초입니다.
router_id	가상 링크 네이버의 라우터 ID. 이 라우터 ID는 내부적으로 각 라우터에 의해 인터페이스 IP 주소로부터 파생됩니다. 이 값은 IP 주소의 형식으로 입력해야 합니다. 기본값이 없습니다.
transmit-delay *seconds*	(선택 사항) OSPF에서 토폴로지 변경을 수신한 시점부터 SPF(shortest path first) 계산을 시작하는 시점까지의 지연 시간을 0초~65535초 범위에서 지정합니다. 기본값은 5초입니다.

참고 1자리 비밀번호 및 숫자로 시작하고 그 다음에 공백이 오는 비밀번호는 더 이상 지원되지 않습니다.

기본값

기본 설정은 다음과 같습니다.

- *area_id*: 어떤 영역 ID도 미리 정의되지 않습니다.
- *router_id*: 어떤 라우터 ID도 미리 정의되지 않습니다.
- **hello-interval** *seconds*: 10초.
- **retransmit-interval** *seconds*: 5초.
- **transmit-delay** *seconds*: 1초.
- **dead-interval** *seconds*: 40초.
- **authentication-key [0 | 8]** *key*: 어떤 키도 미리 정의되지 않습니다.
- **message-digest-key** *key_id* **md5 [0 | 8]** *key*: 어떤 키도 미리 정의되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

OSPF에서는 모든 영역이 백본 영역에 연결되어야 합니다. 백본과의 연결이 끊길 경우 가상 링크를 설정하여 복구할 수 있습니다.

hello 간격이 짧을수록 토폴로지 변경 사항이 더 빨리 탐지되지만 더 많은 라우팅 트래픽이 발생합니다.

재전송 간격은 신중하게 설정해야 합니다. 그렇지 않으면 불필요한 재전송이 일어납니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.

전송 지연 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다.

지정된 인증 키는 **area** *area_id* **authentication** 명령을 통해 백본에 대해 인증이 활성화된 경우에만 사용됩니다.

단순 텍스트와 MD5 인증의 두 인증 체계는 동시에 사용할 수 없습니다. 둘 중 하나만 지정하거나 둘 다 지정하지 않아야 합니다. **authentication-key [0 | 8]** *key* 또는 **message-digest-key** *key_id* **md5[0 | 8]** *key* 다음에 키워드와 인수를 지정하더라도 무시됩니다. 따라서 선택적 인수는 키워드-인수 조합의 앞에 지정합니다.

인터페이스에 대해 인증 유형이 지정되지 않을 경우 인터페이스는 해당 영역에 대해 지정된 인증 유형을 사용합니다. 영역에 대해 어떤 인증 유형도 지정되지 않은 경우 영역의 기본 설정은 null 인증입니다.

참고 각 가상 링크 네이버는 트랜짓 영역 ID 및 해당 가상 링크 네이버 라우터 ID를 포함해야 가상 링크가 제대로 구성됩니다. 라우터 ID를 설정하려면 **show ospf** 명령을 사용합니다.

예

다음 예에서는 MD5 인증으로 가상 링크를 설정합니다.

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 8
sa5721bk47
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show ospf	OSPF 라우팅 프로세스에 대한 일반적인 정보를 표시합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

area virtual-link(OSPFv3)

OSPFv3 가상 링크를 정의하려면 IPv6 라우터 컨피그레이션 모드에서 **area virtual-link** 명령을 사용합니다. 옵션을 재설정하거나 가상 링크를 제거하려면 이 명령의 **no** 형식을 사용합니다.

area *area_id* **virtual-link** *router_id* **[hello-interval** *seconds***] [retransmit-interval** *seconds***] [transmit-delay** *seconds***] [dead-interval** *seconds* **[ttl-security hops** *hop-count***]**

no area *area_id* **virtual-link** *router_id* **[hello-interval** *seconds***] [retransmit-interval** *seconds***] [transmit-delay** *seconds***] [dead-interval** *seconds***] [ttl-security hops** *hop-count***]**

구문 설명

area_id	가상 링크를 위한 트랜짓 영역의 ID를 지정합니다. 이 식별자는 십진수 또는 유효한 IPv6 접두사로 지정할 수 있습니다. 유효한 십진수 값의 범위는 0~4294967295입니다.
dead-interval *seconds*	(선택 사항) 네이버에서 라우터가 다운 상태임을 선언하기 전에 hello 패킷이 인식되지 않는 기간(초)을 지정합니다. Dead 간격은 무부호 정수입니다. hello 간격과 마찬가지로 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~8192입니다.
hello-interval *seconds*	(선택 사항) ASA가 인터페이스에서 보내는 hello 패킷의 간격(초)을 지정합니다. Hello 간격은 hello 패킷에 광고되는 무부호 정수입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~8192초입니다.
retransmit-interval *seconds*	(선택 사항) 인터페이스에 속하는 인접 라우터에 대해 LSA를 재전송하는 간격(초)을 지정합니다. 재전송 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간입니다. 이 값이 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1~8192초입니다.
router_id	가상 링크 네이버와 연결된 라우터 ID를 지정합니다. 라우터 ID는 **show ipv6 ospf** 또는 **show ipv6 display** 명령에 나타납니다.
transmit-delay *seconds*	(선택 사항) 인터페이스에서 링크 상태 업데이트 패킷을 보내는 데 필요한 예상 시간(초)을 지정합니다. 이 정수 값은 0보다 커야 합니다. 업데이트 패킷의 LSA에는 전송 전에 이 키워드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 유효한 값의 범위는 1~8192초입니다.
ttl-security hops *hop-count*	(선택 사항) 가상 링크에서 TTL(time-to-live) 보안을 구성합니다. 유효한 hop count 범위는 1~254입니다.

참고 1자리 비밀번호 및 숫자로 시작하고 그 다음에 공백이 오는 비밀번호는 더 이상 지원되지 않습니다.

기본값

기본 설정은 다음과 같습니다.

- *area_id*: 어떤 영역 ID도 미리 정의되지 않습니다.
- *router_id*: 어떤 라우터 ID도 미리 정의되지 않습니다.
- **hello-interval**: 10초.
- **retransmit-interval**: 5초.
- **transmit-delay**: 1초.
- **dead-interval**: 40초.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
IPv6 라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

OSPFv3에서는 모든 영역이 백본 영역에 연결되어야 합니다. 백본과의 연결이 끊길 경우 가상 링크를 설정하여 복구할 수 있습니다.

hello 간격이 짧을수록 토폴로지 변경 사항이 더 빨리 탐지되지만 더 많은 라우팅 트래픽이 발생합니다.

재전송 간격은 신중하게 설정해야 합니다. 그렇지 않으면 불필요한 재전송이 일어납니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다.

전송 지연 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다.

참고 각 가상 링크 네이버는 트랜짓 영역 ID 및 해당 가상 링크 네이버 라우터 ID를 포함해야 가상 링크가 제대로 구성됩니다. 라우터 ID를 설정하려면 **show ipv6 ospf** 명령을 사용합니다.

예

다음 예에서는 OSPFv3에서 가상 링크를 설정합니다.

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello interval 5
```

관련 명령i

명령	설명
ipv6 router ospf	OSPFv3의 라우터 컨피그레이션 모드를 시작합니다.
show ipv6 ospf	OSPFv3 라우팅 프로세스에 대한 일반적인 정보를 표시합니다.
show running-config ipv6 router	전역 라우터 컨피그레이션에서 IPv6 명령을 표시합니다.

arp

ARP 테이블에 고정 ARP 엔트리를 추가하려면 글로벌 컨피그레이션 모드에서 **arp** 명령을 사용합니다. 고정 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

arp *interface_name ip_address mac_address* **[alias]**

no arp *interface_name ip_address mac_address*

구문 설명

alias	(선택 사항) 이 매핑을 위한 프록시 ARP를 활성화합니다. ASA에서 지정된 IP 주소에 대한 ARP 요청을 받을 경우 ASA MAC 주소로 응답합니다. ASA에서 해당 IP 주소의 호스트로 갈 트래픽을 수신할 경우 ASA는 이 명령으로 지정한 호스트 MAC 주소에 트래픽을 전달합니다. 이 키워드는 이를테면 ARP를 수행하지 않는 디바이스가 있을 경우 유용합니다. 투명 방화벽 모드에서는 이 키워드가 무시됩니다. ASA가 프록시 ARP를 수행하지 않습니다.
interface_name	호스트 네트워크에 연결된 인터페이스.
ip_address	호스트 IP 주소입니다.
mac_address	호스트 MAC 주소입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

호스트에서 IP 주소로 패킷 목적지를 식별하긴 하지만, 이더넷에서 패킷이 실제 전달되는 것은 이더넷 MAC 주소에 달려 있습니다. 라우터 또는 호스트에서 패킷을 직접 연결된 디바이스에 전달하려는 경우, IP 주소와 연관된 MAC 주소를 묻는 ARP 요청이 전송되며 그 후 ARP 응답에 따라 패킷이 MAC 주소에 전달됩니다. 호스트 또는 라우터에서는 ARP 테이블을 보관하므로, 모든 패킷을 전달할 때마다 ARP 요청을 보내지 않아도 됩니다. ARP 테이블은 ARP 응답이 네트워크로 전송될 때마다 동적으로 업데이트되며, 일정 기간 동안 사용되지 않는 항목이 있으면 해당 항목은 시간 제한으로 만료됩니다. 항목이 잘못된 경우(예: 제공된 IP 주소의 MAC 주소가 변경된 경우), 해당 항목은 업데이트되기 전에 시간 제한으로 만료됩니다.

고정 ARP 엔트리는 IP 주소에 MAC 주소를 매핑하고 호스트에 연결하기 위해 지날 인터페이스를 식별합니다. 고정 ARP 엔트리는 시간 초과가 없으며, 네트워킹 문제 해결에 도움이 될 수 있습니다. 투명 방화벽 모드에서는 고정 ARP 테이블을 ARP 검사와 함께 사용합니다(**arp-inspection** 명령 참조).

참고 투명 방화벽 모드에서는 관리 트래픽과 같이 ASA에서 나오고 들어가는 트래픽에 동적 ARP 엔트리를 사용합니다.

예

다음 예에서는 외부 인터페이스에서 MAC 주소가 0009.7cbe.2100인 10.1.1.1을 위해 고정 ARP를 만듭니다.

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

관련 명령

명령	설명
arp timeout	ASA에서 ARP 테이블을 재작성할 때까지의 시간을 설정합니다.
arp-inspection	투명 방화벽 모드에서 ARP 스푸핑을 방지하기 위해 ARP 패킷을 검사합니다.
show arp	ARP 테이블을 표시합니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config arp	ARP 시간 초과의 현재 컨피그레이션을 표시합니다.

arp permit-nonconnected

ARP 캐시가 직접 연결되지 않은 서브넷도 포함할 수 있게 하려면 글로벌 컨피그레이션 모드에서 **arp permit-nonconnected** 명령을 사용합니다. 비 연결 서브넷을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

arp permit-nonconnected

no arp permit-nonconnected

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(5), 9.0(1)	이 명령을 도입했습니다.

사용 지침

ASA ARP 캐시에는 기본적으로 직접 연결된 서브넷의 항목만 포함됩니다. 이 명령을 사용하면 ARP 캐시에 직접 연결되지 않은 서브넷도 포함할 수 있습니다. 그러나 보안 위험을 잘 숙지하고 있지 않다면 이 기능은 사용하지 않는 것이 좋습니다. 이 기능은 ASA에 대한 DoS(서비스 거부 시도) 공격을 촉진할 수 있습니다. 즉, 임의의 인터페이스에서 사용자가 다량의 ARP 응답을 전송하고 ASA ARP 테이블에 false 항목이 오버로드되도록 할 수 있습니다.

다음을 사용하는 경우 이 기능을 사용할 수 있습니다.

- 보조 서브넷
- 트래픽 전달을 지원하는 인접 경로의 프록시 ARP

예

다음 예에서는 비 연결 서브넷을 활성화합니다.

```
ciscoasa(config)# arp permit non-connected
```

관련 명령

명령	설명
arp	고정 ARP 항목을 추가합니다.

arp-inspection

투명 방화벽 모드에서 ARP 검사를 활성화하려면 글로벌 컨피그레이션 모드에서 **arp-inspection** 명령을 사용합니다. ARP 검사를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

arp-inspection *interface_name* **enable [flood | no-flood]**

no arp-inspection *interface_name* **enable**

구문 설명

enable	ARP 검사를 활성화합니다.
flood	(기본값) 고정 ARP 항목의 모든 요소와 일치하지 않는 패킷은 해당 패킷이 시작된 인터페이스를 제외한 모든 인터페이스에 플러딩됩니다. MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 ASA에서는 패킷을 누락시킵니다. **참고** 관리 전용 인터페이스가 있다면 이 매개변수가 플러딩을 실행하도록 설정된 경우에도 패킷이 플러딩되지 않습니다 .
interface_name	ARP 검사를 활성화하려는 인터페이스.
no-flood	(선택 사항) 고정 ARP 엔트리와 정확하게 일치하지 않는 패킷은 삭제됩니다.

기본값

기본적으로 ARP 검사는 모든 인터페이스에서 비활성화됩니다. 즉 모든 ARP 패킷이 ASA를 지나도록 허용됩니다. ARP 검사를 활성화할 경우 기본 설정은 불일치 ARP 패킷을 플러딩하는 것입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ARP 검사를 활성화하기 전에 **arp** 명령을 사용하여 고정 ARP 엔트리를 구성합니다.

ARP 검사에서는 고정 ARP 엔트리와 비교하여 모든 ARP 패킷을 확인하고(**arp** 명령 참조) 불일치 패킷을 차단합니다. 이 기능으로 ARP 스푸핑을 방지합니다.

ARP 검사를 활성화할 경우 ASA에서는 MAC 주소, IP 주소, 모든 ARP 패킷의 소스 인터페이스를 ARP 테이블의 고정 항목과 비교하고 다음과 같은 조치를 취합니다.

- IP 주소, MAC 주소, 소스 인터페이스가 ARP 항목과 일치하면 패킷이 통과됩니다.
- MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 ASA에서는 패킷을 누락시킵니다.

- ARP 패킷이 고정 ARP 테이블의 어느 항목과도 일치하지 않으면 ASA를 설정하여 패킷을 모든 인터페이스로 전달(플러딩)하거나 패킷이 누락되도록 합니다.

참고 전용 관리 인터페이스가 있다면 이 매개변수가 플러딩을 실행하도록 설정된 경우에도 패킷이 플러딩되지 않습니다.

ARP 검사 기능은 악의적인 사용자가 다른 호스트 또는 라우터로 위장(ARP 스푸핑이라고도 함)하는 것을 방지합니다. ARP 스푸핑은 "끼어들기" 공격을 활성화할 수 있습니다. 예를 들어, 호스트에서 ARP 요청을 게이트웨이 라우터에 전송할 경우 해당 게이트웨이 라우터는 게이트웨이 라우터 MAC 주소에 응답합니다. 그러나 공격자는 라우터 MAC 주소가 아닌 공격자 MAC 주소가 포함된 다른 ARP 응답을 호스트에 전송합니다. 이제 공격자는 라우터에 트래픽이 전달되기 전에 모든 호스트 트래픽을 가로챌 수 있게 됩니다.

ARP 검사 기능은 고정 ARP 테이블에 올바른 MAC 주소와 관련 IP 주소를 입력하기만 하면 공격자가 공격자 MAC 주소가 포함된 ARP 응답을 보낼 수 없도록 합니다.

참고 투명 방화벽 모드에서는 관리 트래픽과 같이 ASA에서 나오고 들어가는 트래픽에 동적 ARP 엔트리를 사용합니다.

예

다음 예에서는 외부 인터페이스에서 ARP 검사를 활성화하고 ASA에서 공정 ARP 엔트리와 일치하지 않는 모든 ARP 패킷을 삭제하도록 설정합니다.

```
ciscoasa(config)# arp outside 209.165.200.225 0009.7cbe.2100
ciscoasa(config)# arp-inspection outside enable no-flood
```

관련 명령

명령	설명
arp	고정 ARP 항목을 추가합니다.
clear configure arp-inspection	ARP 검사 컨피그레이션을 지웁니다.
firewall transparent	방화벽 모드를 투명 모드로 설정합니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config arp	ARP 시간 초과의 현재 컨피그레이션을 표시합니다.

arp timeout

ASA에서 ARP 테이블을 재작성할 때까지의 시간을 설정하려면 글로벌 컨피그레이션 모드에서 **arp timeout** 명령을 사용합니다. 시간 초과의 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

arp timeout *seconds*

no arp timeout *seconds*

구문 설명

seconds	ARP 테이블 재작성 간격(초)이며 범위는 60초~4294967초입니다.

기본값

기본값은 14,400초(4시간)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ARP 테이블을 재구성하면 새 호스트 정보가 자동으로 업데이트되고 기존 호스트 정보가 제거됩니다. 호스트 정보는 자주 변경되므로 시간 제한 값을 낮출 수 있습니다.

예

다음 예에서는 ARP 시간 초과를 5,000초로 변경합니다.

```
ciscoasa(config)# arp timeout 5000
```

관련 명령

명령	설명
arp	고정 ARP 항목을 추가합니다.
arp-inspection	투명 방화벽 모드에서 ARP 스푸핑을 방지하기 위해 ARP 패킷을 검사합니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config arp timeout	ARP 시간 초과의 현재 컨피그레이션을 표시합니다.

as-path access-list

정규식을 사용하여 자율 시스템 경로 필터를 구성하려면 글로벌 컨피그레이션 모드에서 **as-path access-list** 명령을 사용합니다. 자율 시스템 경로 필터를 삭제하고 실행 중인 컨피그레이션 파일에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

as-path access-list *acl-name* **{permit | deny}** *regexp*

no as-path access-list *acl-name*

구문 설명

acl-name	AS-path 액세스 목록을 지정하는 이름.
permit	매칭 조건에 따라 광고를 허용합니다.
deny	매칭 조건에 따라 광고를 거부합니다.
regexp	AS-path 필터를 정의하는 정규식. 자율 시스템 번호는 1~65535 범위로 표현됩니다. 자율 시스템 번호 형식에 대한 자세한 내용은 **router bgp** 명령을 참조하십시오. **참고** 정규식 컨피그레이션에 대한 자세한 내용은 *Cisco IOS Terminal Services 컨피그레이션 가이드*의 " 정규식 " 부록을 참조하십시오 .

기본값

자율 시스템 경로 필터가 생성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

자율 시스템 경로 필터를 구성하려면 **as-path access-list** 명령을 사용합니다. 인바운드 및 아웃바운드 BGP 경로 모두에 자율 시스템 경로 필터를 적용할 수 있습니다. 각 필터는 정규식을 통해 정의됩니다. 정규식이 ASCII 문자열로 표시된 경로의 자율 시스템 경로와 일치할 경우 **permit** 또는 **deny** 조건이 적용됩니다. 자율 시스템 경로는 논리적 자율 시스템 번호를 포함해서는 안 됩니다.

Cisco가 구현한 4바이트 자율 시스템 번호에서는 asplain(예: 65538)을 자율 시스템 번호를 위한 기본 정규식 매칭 및 출력 표시 형식으로 사용하지만, 4바이트 자율 시스템 번호를 asplain 형식 및 asdot 형식(예: RFC 5396에 설명된) 모두로 구성할 수 있습니다. 4바이트 자율 시스템 번호의 기본 정규식 매칭 및 출력 표시를 asdot 형식으로 변경하려면 **bgp asnotation dot** 명령을 사용합니다. asdot 형식이 기본 설정으로 활성화되면 4바이트 자율 시스템 번호와 일치하는 모든 정규식은 asdot 형식으로 작성해야 합니다. 그렇지 않으면 정규식 매칭에서 실패합니다.

예

다음 예에서는 ASA가 자율 시스템 65535를 지나거나 여기서 나오는 어떤 경로도 네이버인 10.20.2.2에 광고하지 않도록 구성하기 위해 자율 시스템 경로 액세스 목록(번호 500)을 정의합니다.

```
ciscoasa(config)# as-path access-list as-path-acl deny _65535_
ciscoasa(config)# as-path access-list as-path-acl deny ^65535$
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-fmaily ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.1 remote-as 65535
ciscoasa(config-router-af)# neighbor 10.20.2.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 10.20.2.2 filter-list as-path-acl out
```

asdm disconnect

활성 ASDM 세션을 종료하려면 특별 권한 EXEC 모드에서 **asdm disconnect** 명령을 사용합니다.

asdm disconnect *session*

구문 설명

session	종료할 활성 ASDM 세션의 세션 ID

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**pdm disconnect** 명령을 **asdm disconnect** 명령으로 변경했습니다.

사용 지침

활성 ASDM 세션 및 그 세션 ID의 목록을 표시하려면 **show asdm sessions** 명령을 사용합니다. 특정 세션을 종료하려면 **asdm disconnect** 명령을 사용합니다.

ASDM 세션을 종료할 경우 남아 있는 활성 ASDM 세션은 해당 세션 ID를 계속 유지합니다. 예를 들어, 세션 ID가 0, 1, 2인 3개의 활성 ASDM 세션이 있을 경우 세션 1을 종료하면 나머지 ASDM 세션은 세션 ID 0과 2를 유지합니다. 이 예에서 다음 신규 ASDM 세션에는 세션 ID 1이 부여되며 그 다음의 신규 세션에는 세션 ID 3부터 지정됩니다.

예

다음 예에서는 세션 ID가 0인 ASDM 세션을 종료합니다. **show asdm sessions** 명령은 **asdm disconnect** 명령을 입력하기 전후에 활성 ASDM 세션을 표시합니다.

```
ciscoasa# show asdm sessions

0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm sessions

1 192.168.1.2
```

관련 명령

명령	설명
show asdm sessions	활성 ASDM 세션과 그 세션 ID의 목록을 표시합니다.

asdm disconnect log_session

활성 ASDM 로깅 세션을 종료하려면 특별 권한 EXEC 모드에서 **asdm disconnect log_session** 명령을 사용합니다.

asdm disconnect log_session *session*

구문 설명

session	종료할 활성 ASDM 로깅 세션의 세션 ID

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

활성 ASDM 로깅 세션 및 그 세션 ID의 목록을 표시하려면 **show asdm log_sessions** 명령을 사용합니다. 특정 로깅 세션을 종료하려면 **asdm disconnect log_session** 명령을 사용합니다.

각 활성 ASDM 세션은 하나 이상의 ASDM 로깅 세션을 갖습니다. ASDM에서는 ASA에서 syslog 메시지를 검색하는 데 로깅 세션을 사용합니다. 로그 세션을 종료할 경우 활성 ASDM 세션에 불리하게 작용할 수 있습니다. 불필요한 ASDM 세션을 종료하려면 **asdm disconnect** 명령을 사용합니다.

참고 각 ASDM 세션이 하나 이상의 ASDM 로깅 세션을 가지므로 **show asdm sessions** 및 **show asdm log_sessions**의 출력이 동일할 수도 있습니다.

ASDM 로깅 세션을 종료할 경우 남아 있는 활성 ASDM 로깅 세션은 해당 세션 ID를 계속 유지합니다. 예를 들어, 세션 ID가 0, 1, 2인 3개의 활성 ASDM 로깅 세션이 있을 경우 세션 1을 종료하면 나머지 ASDM 로깅 세션은 세션 ID 0과 2를 유지합니다. 이 예에서 다음 신규 ASDM 로깅 세션에는 세션 ID 1이 부여되며 그 다음의 신규 세션에는 세션 ID 3부터 지정됩니다.

예

다음 예에서는 세션 ID가 0인 ASDM 세션을 종료합니다. **show asdm log_sessions** 명령은 **asdm disconnect log_sessions** 명령을 입력하기 전후에 활성 ASDM 세션을 표시합니다.

```
ciscoasa# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm log_sessions

1 192.168.1.2
```

관련 명령

명령	설명
show asdm log_sessions	활성 ASDM 로깅 세션과 그 세션 ID의 목록을 표시합니다.

asdm history enable

ASDM 기록 추적을 활성화하려면 글로벌 컨피그레이션 모드에서 **asdm history enable** 명령을 사용합니다. ASDM 기록 추적을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

asdm history enable

no asdm history enable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**pdm history enable** 명령을 **asdm history enable** 명령으로 변경했습니다.

사용 지침

ASDM 기록 추적을 활성화하여 얻은 정보는 ASDM 기록 버퍼에 저장됩니다. **show asdm history** 명령을 사용하여 이 정보를 볼 수 있습니다. 기록 정보는 ASDM에서 디바이스 모니터링에 사용합니다.

예

다음 예에서는 ASDM 기록 추적을 활성화합니다.

```
ciscoasa(config)# asdm history enable
ciscoasa(config)#
```

관련 명령

명령	설명
show asdm history	ASDM 기록 버퍼의 내용을 표시합니다.

asdm image

플래시 메모리에 있는 ASDM 소프트웨어 이미지의 위치를 지정하려면 글로벌 컨피그레이션 모드에서 **asdm image** 명령을 사용합니다. 이미지 위치를 제거하려면 이 명령의 **no** 형식을 사용합니다.

asdm image *url*

no asdm image [*url*]

구문 설명

url	플래시 메모리에 있는 ASDM 이미지의 위치를 설정합니다. 다음 URL 구문을 참조하십시오. • **disk0:/**[*path*/]*filename* ASA 5500 시리즈에서는 이 URL이 내부 플래시 메모리를 가리킵니다. **flash**를 **disk0** 대신 사용할 수 있습니다. 서로 별칭입니다. • **disk1:/**[*path*/]*filename* ASA 5500 시리즈에서는 이 URL이 외부 플래시 메모리 카드를 가리킵니다. • **flash:/**[*path*/]*filename* 이 URL이 내부 플래시 메모리를 가리킵니다.

기본값

시작 컨피그레이션에 이 명령을 포함하지 않을 경우 ASA는 시작 시 처음으로 발견한 ASDM 이미지를 사용합니다. 내부 플래시 메모리의 루트 디렉토리와 외부 플래시 메모리를 차례로 검색합니다. 그런 다음 ASA는 이미지를 발견하면 실행 중인 컨피그레이션에 **asdm image** 명령을 삽입합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

플래시 메모리에 둘 이상의 ASDM 소프트웨어 이미지를 저장할 수 있습니다. 활성 ASDM 세션이 있는 상태에서 새 ASDM 소프트웨어 이미지를 지정하기 위해 **asdm image** 명령을 입력할 경우 새 명령이 활성 세션을 중단하지 않습니다. 활성 ASDM 세션에서는 시작할 때 사용했던 ASDM 소프트웨어를 계속 사용합니다. 새 ASDM 세션에서는 새 소프트웨어 이미지를 사용합니다. **no asdm image** 명령을 입력하면 이 명령이 컨피그레이션에서 제거됩니다. 그러나 마지막으로 구성되었던 이미지 위치를 사용하여 계속 ASA에서 ASDM에 액세스할 수 있습니다.

시작 컨피그레이션에 이 명령을 포함하지 않을 경우 ASA는 시작 시 처음으로 발견한 ASDM 이미지를 사용합니다. 내부 플래시 메모리의 루트 디렉토리와 외부 플래시 메모리를 차례로 검색합니다. 그런 다음 ASA는 이미지를 발견하면 실행 중인 컨피그레이션에 **asdm image** 명령을 삽입합니다. 반드시 **write memory** 명령을 사용하여 실행 중인 컨피그레이션을 시작 컨피그레이션으로 저장해야 합니다. **asdm image** 명령을 시작 컨피그레이션에 저장하지 않으면 재부팅할 때마다 ASA에서 ASDM 이미지를 검색하고 **asdm image** 명령을 실행 중인 컨피그레이션에 삽입하게 됩니다. 자동 업데이트를 사용하는 경우 시작 시 이 명령이 자동으로 추가되어 ASA의 컨피그레이션이 자동 업데이트 서버의 컨피그레이션과 일치하지 않게 됩니다. 이러한 불일치 때문에 ASA에서 자동 업데이트 서버에서 컨피그레이션을 다운로드합니다. 불필요한 자동 업데이트 활동을 방지하기 위해 **asdm image** 명령을 시작 컨피그레이션에 저장하십시오.

예

다음 예에서는 ASDM 이미지를 asdm.bin으로 설정합니다.

```
ciscoasa(config)# asdm image flash:/asdm.bin
ciscoasa(config)#
```

관련 명령

명령	설명
show asdm image	현재 ASDM 이미지 파일을 표시합니다.
boot	소프트웨어 이미지 및 시작 컨피그레이션 파일을 설정합니다.

asdm location

주의 이 명령을 수동으로 구성하지 마십시오. ASDM은 실행 중인 컨피그레이션에 **asdm location** 명령을 추가하고 이를 내부 통신에 사용합니다. 이 명령은 단지 참조용으로 설명서에 포함되었습니다.

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

구문 설명

if_name	최상위 보안 인터페이스의 이름. 여러 인터페이스가 최상위 보안 상태에 있을 경우 임의의 인터페이스 이름이 선택됩니다. 이 인터페이스 이름은 사용되지 않지만 필수 매개변수입니다.
ip_addr	ASDM이 네트워크 토폴로지를 정의하기 위해 내부에서 사용하는 IP 주소.
ipv6_addr/prefix	ASDM이 네트워크 토폴로지를 정의하기 위해 내부에서 사용하는 IPv6 주소 및 접두사.
netmask	*ip_addr*의 서브넷 마스크.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**pdm location** 명령을 **asdm location** 명령으로 변경했습니다.

사용 지침

이 명령을 직접 구성하거나 제거하지 마십시오.

asp load-balance per-packet

멀티코어 ASA의 경우 로드 밸런싱 동작을 변경하려면 글로벌 컨피그레이션 모드에서 **asp load-balance per-packet** 명령을 사용합니다. 로드 밸런싱 메커니즘의 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

asp load-balance per-packet [auto]

no asp load-balance per-packet

구문 설명

auto	각 인터페이스 수신 링에서 패킷별로 ASP 로드 밸런싱을 자동으로 켜고 끕니다. 기본값은 disabled입니다.

명령 기본값

asp load-balance per-packet 명령에서는 로드 밸런싱 메커니즘이 기본적으로 다중 인터페이스를 선호합니다. **asp load-balance per-packet auto** 명령에서는 기본적으로 한 번에 하나의 코어에서만 인터페이스 수신 링에서 패킷을 받을 수 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.1(1)	이 명령을 도입했습니다.
9.3(1)	네트워크 조건에 따라 ASP 로드 밸런싱을 자동으로 켜고 끌 수 있도록 **auto** 옵션을 추가했습니다.

사용 지침

이 기본 동작은 패킷이 모든 인터페이스 링에서 고르지 않게 수신되는 시나리오를 위해 최적화되었습니다. 이 패킷별 동작은 인터페이스 수신 링에서 트래픽이 비대칭적으로 분포하는 시나리오를 위해 최적화되었습니다. 멀티코어 ASA의 성능은 프로세서 수, 인터페이스 수신 링 수, 지나는 트래픽의 특성에 따라 달라질 수 있습니다. **asp load-balance per-packet** 명령을 사용하면 여러 코어가 단일 인터페이스 수신 링크로부터 받은 패킷에 동시에 작업할 수 있습니다. 이 명령은 수신 패킷이 여러 독립적인 연결에 분산된 경우에 병렬 처리를 가능하게 합니다. 이 명령을 사용하면 동일한 연결 및 연관된 연결에서 나온 패킷이 추가적인 큐잉 오버헤드를 겪을 수 있습니다. 하나의 코어에서 이 패킷을 처리하기 때문입니다.

시스템에서 패킷을 폐기하고 **show cpu** 명령 출력이 100%보다 훨씬 적은 경우, 패킷이 관련 없는 다수의 연결에 속한 것이라면 이 명령으로 처리량을 늘릴 수 있습니다. CPU 사용량은 실제로 몇 개의 코어가 사용되고 있는지 보여주는 유용한 지표입니다.

예를 들어, 8코어의 ASA 5580-40에서 2개 코어가 사용되는 경우 **show cpu** 명령의 출력은 25%가 됩니다. 4코어는 50%, 6코어는 75%가 됩니다.

auto 옵션을 사용하면 ASA에서 비대칭 트래픽이 유입되었는지 여부를 탐지할 수 있습니다. 로드 밸런싱이 필요할 경우 인터페이스 수신 링과 코어 간의 일대일 잠금이 해제됩니다. 이러한 적응형 ASP 로드 밸런싱 메커니즘으로 다음과 같은 문제를 방지할 수 있습니다.

- 흐름에서 산발적인 트래픽 급증으로 인한 오버런
- 특정 인터페이스 수신 링에 초과 유입되는 대량 흐름에 의한 오버런
- 비교적 과부하 상태인 인터페이스 수신 링으로 인한 오버런. 단일 코어에서 부하를 수용할 수 없음

참고 자동 모드에서는 패킷별 ASP 로드 밸런싱이 모든 인터페이스 수신 링이 아니라 과부하 상태의 인터페이스 수신 링에서만 활성화됩니다. 업그레이드 과정에서 패킷별 ASP 로드 밸런싱이 활성화되었거나 비활성화되었을 때 실행 중이던 모드를 유지해야 합니다. 명시적으로 자동 모드를 구성해야 합니다.

자동 모드에서는 각 인터페이스 수신 링이 대기 시간을 유지합니다. 인터페이스 수신 링이 busy 상태로 간주되고 많은 트래픽 때문에 패킷별 ASP 로드 밸런싱이 자동으로 활성화될 때 인터페이스 수신 링은 대기 시간(기본값은 200밀리초) 동안 패킷별 ASP 로드 밸런싱을 자동 활성 상태로 유지합니다. 인터페이스 수신 링의 부하가 감소하지만 200밀리초 내에 다시 트래픽이 많아질 경우 인터페이스 수신 링은 busy 상태로 간주되고 대기 시간은 최대 6400밀리초 범위에서 2배로 늘어납니다. 인터페이스 수신 링에서 과다 트래픽을 지속적으로 겪지 않을 경우 대기 시간은 200밀리초로 유지됩니다. 이러한 메커니즘으로 패킷별 ASP 로드 밸런싱이 활성 상태와 비활성 상태를 바쁘게 오가는 것이 줄어듭니다. 그러면 서로 다른 시간 범위 내 오버런을 방지할 수 있습니다.

auto 옵션이 활성화된 경우 과부하 상태가 아닌 링에서는 일대일 잠금이 유지됩니다. 이 링은 멀티코어 처리가 필요하지 않기 때문입니다. 또한 과부하 링에서는 일대일 잠금이 유지되지 않습니다. 이 부하를 처리하기 위해 멀티코어 지원이 필요하기 때문입니다.

과부하 링의 총 개수가 일정 한도를 넘어서면 이 기능은 자동으로 꺼집니다.

ASA 5585-X 및 ASASM에서만 이 명령을 사용할 수 있습니다.

예

다음 예에서는 기본 로드 밸런싱 동작을 변경하는 방법을 보여줍니다.

```
ciscoasa(config)# asp load-balance per-packet
```

다음 예에서는 패킷별 로드 밸런싱의 자동 켜기/끄기를 활성화합니다.

```
ciscoasa(config)# asp load-balance per-packet auto
```

관련 명령

명령	설명
clear asp load-balance history	패킷별 ASP 로드 밸런싱 기록 통계를 생성하고 재설정합니다.
show asp load-balance	로드 밸런서 큐 크기를 히스토그램으로 표시합니다.
show asp load-balance per-packet	현재 상태, 상위/하위 워터마크, 전역 임계값을 표시합니다.
show asp load-balance per-packet history	현재 상태, 상위/하위 워터마크, 전역 임계값, 최근 재설정 후 패킷별 ASP 로드 밸런싱을 켜고 끈 횟수, 패킷별 ASP 로드 밸런싱 기록(타임스탬프 포함), 켜고 끈 사유를 표시합니다.

asp rule-engine transactional-commit

규칙 엔진의 트랜잭션 커밋 모델을 활성화하거나 비활성화하려면 **asp rule-engine transactional-commit** 명령을 사용합니다.

asp rule-engine transactional-commit *option*

no asp rule-engine transactional-commit *option*

구문 설명

option	선택된 정책에 대해 규칙 엔진의 트랜잭션 커밋 모델을 활성화합니다. 선택 가능한 옵션: • **access-group**—전역에 또는 인터페이스에 적용되는 액세스 규칙 • **nat**—네트워크 주소 변환 규칙

명령 기본값

기본적으로 트랜잭션 커밋 모델은 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(5)	이 명령을 도입했습니다.
9.3(1)	**nat** 키워드를 추가했습니다.

사용 지침

기본적으로 규칙 기반 정책(예: 액세스 규칙)을 바꾸면 그 변경 사항이 즉시 적용됩니다. 하지만 이와 같은 신속성이 다소 성능에 영향을 미칩니다. 이 성능 문제는 초당 연결 수가 많은 환경에서 매우 큰 규칙 목록을 사용할 때 더욱 두드러집니다. 예를 들면, ASA에서 초당 18,000건의 연결을 처리하는 동안 25,000개의 규칙이 포함된 정책을 변경하는 경우입니다.

규칙 엔진이 규칙 조회 속도를 높이고자 규칙을 컴파일하면서 성능에 영향을 줍니다. 기본적으로 이 시스템은 연결 시도를 평가할 때 새로운 규칙을 적용할 수 있도록 컴파일되지 않은 규칙도 검색합니다. 규칙이 컴파일되지 않았으므로 검색 시간이 늘어납니다.

규칙 엔진에서 규칙 변경을 구현할 때 트랜잭션 모델을 사용함으로써 새 규칙이 컴파일되어 사용 가능해질 때까지 기존 규칙을 계속 사용하도록 위 동작을 변경할 수 있습니다. 트랜잭션 모델을 사용하면 규칙 컴파일 과정에서 성능이 저하되지 않습니다. 다음 표에서 동작의 차이점을 확인할 수 있습니다.

모델	컴파일 전	컴파일 과정	컴파일 후
기본값	기존 규칙에 매칭합니다.	새 규칙에 매칭합니다. (초당 연결 수 감소)	새 규칙에 매칭합니다.
트랜잭션	기존 규칙에 매칭합니다.	기존 규칙에 매칭합니다. (초당 연결 수에 영향을 주지 않음)	새 규칙에 매칭합니다.

트랜잭션 모델의 또 다른 이점은 인터페이스에서 ACL을 대체할 때 기존 ACL을 삭제하는 시점과 새 ACL을 적용하는 시점 사이에 공백이 없다는 것입니다. 이 기능 덕분에 작업 과정에서 적합한 연결이 폐기될 가능성이 줄어듭니다.

팁 규칙 유형에 대해 트랜잭션 모델을 활성화하면 컴파일의 시작과 끝을 알리는 syslog 메시지가 생성됩니다. 이 메시지의 번호는 780001부터 시작합니다.

예

다음 예에서는 액세스 그룹에 대해 트랜잭션 커밋 모델을 활성화합니다.

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

관련 명령

명령	설명
clear conf asp rule-engine transactional-commit	규칙 엔진의 트랜잭션 커밋 컨피그레이션을 지웁니다.
show run asp rule-engine transactional-commit	규칙 엔진에 대해 실행 중인 컨피그레이션을 표시합니다.

asr-group

비대칭 라우팅 인터페이스 그룹 ID를 지정하려면 인터페이스 컨피그레이션 모드에서 **asr-group** 명령을 사용합니다. ID를 제거하려면 이 명령의 **no** 형식을 사용합니다.

asr-group *group_id*

no asr-group *group_id*

구문 설명

group_id	비대칭 라우팅 그룹 ID. 유효한 값은 1~32입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

액티브/액티브 장애 조치가 활성화된 경우, 로드 밸런싱 때문에 아웃바운드 연결의 반환 트래픽이 (아웃바운드 연결의 컨텍스트가 스탠바이 그룹에 있는) 피어 유닛의 활성 컨텍스트를 통해 라우팅될 때가 있습니다.

asr-group 명령은 수신 인터페이스의 플로우를 찾을 수 없을 경우 수신 패킷이 동일한 ASR 그룹의 인터페이스로 재분류되게 합니다. 재분류를 통해 다른 인터페이스의 플로우를 찾고 해당 컨텍스트가 스탠바이 상태에 있으면 패킷은 활성 유닛으로 전달되어 처리됩니다.

이 명령이 실행되려면 상태 기반 장애 조치가 활성화되어야 합니다.

show interface detail 명령으로 ASR 통계를 볼 수 있습니다. 이 통계에는 인터페이스에서 보내고 받고 삭제한 ASR 패킷의 수가 포함됩니다.

참고 같은 ASR 그룹의 같은 컨텍스트에서 2개의 인터페이스를 구성할 수 없습니다.

예

다음 예에서는 선택된 인터페이스를 비대칭 라우팅 그룹 1로 지정합니다.

Context ctx1 컨피그레이션:

```
ciscoasa/ctx1(config)# interface Ethernet2
ciscoasa/ctx1(config-if)# nameif outside
ciscoasa/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
ciscoasa/ctx1(config-if)# asr-group 1
```

Context ctx2 컨피그레이션:

```
ciscoasa/ctx2(config)# interface Ethernet3
ciscoasa/ctx2(config-if)# nameif outside
ciscoasa/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
ciscoasa/ctx2(config-if)# asr-group 1
```

관련 명령

명령	설명
interface	인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스 통계를 표시합니다.

assertion-consumer-url

보안 디바이스가 어설션 사용자 서비스에 연결하기 위해 액세스하는 URL을 식별하려면 해당 SAML-type SSO 서버의 webvpn 컨피그레이션 모드에서 **assertion-consumer-url** 명령을 사용합니다. 어설션에서 URL을 제거하려면 이 명령의 **no** 형식을 사용합니다.

assertion-consumer-url *url*

no assertion-consumer-url [*url*]

구문 설명

url	SAML-type SSO 서버에서 사용하는 어설션 사용자 서비스의 URL을 지정합니다. URL은 http:// 또는 https://로 시작하고 영숫자 255자 미만이어야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

WebVPN에서만 가능한 SSO(single sign-on) 지원 덕분에 사용자가 사용자 이름과 비밀번호를 2번 이상 입력하지 않고도 여러 서버의 여러 보안 서비스에 액세스할 수 있습니다. ASA는 현재 SAML POST-type SSO 서버와 SiteMinder-type of SSO 서버를 지원합니다.

이 명령은 SAML-type SSO 서버에만 적용됩니다.

URL이 HTTPS로 시작할 경우 어설션 사용자 서비스 SSL 인증서의 루트 인증서를 설치해야 합니다.

예

다음 예에서는 SAML-type SSO 서버에 대해 어설션 사용자 URL을 지정합니다.

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
ciscoasa(config-webvpn-sso-saml#
```

관련 명령

명령	설명
issuer	SAML-type SSO 서버 보안 디바이스 이름을 지정합니다.
request-timeout	실패한 SSO 인증 시도가 시간 초과할 때까지의 시간(초)을 지정합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버의 운영 통계를 표시합니다.
sso-server	WebVPN SSO 서버를 만듭니다.
trustpoint	SAML-type 브라우저 어설션에 서명하는 데 사용할 인증서가 포함된 신뢰 지점 이름을 지정합니다.

attribute

ASA에서 DAP 특성 데이터베이스에 기록하는 특성 값 쌍을 지정하려면 dap 테스트 특성 모드에서 **attribute** 명령을 입력합니다.

attribute *name value*

구문 설명

name	잘 알려진 특성 이름 또는 "label" 태그를 포함하는 특성을 지정합니다. label 태그는 DAP 레코드에서 파일, 레지스트리, 프로세스, 안티바이러스, 안티스파이웨어, 개인 방화벽 엔드포인트 특성에 구성하는 엔드포인트 ID에 해당합니다.
value	AAA 특성에 지정되는 값.

명령 기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
DAP 특성 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

여러 특성 값 쌍을 입력하려면 이 명령을 여러 번 사용합니다.

일반적으로 ASA는 AAA 서버에서 사용자 권한 부여 특성을 검색하고 Cisco Secure Desktop, Host Scan, CNA 또는 NAC에서 엔드포인트 특성을 검색합니다. 이 특성 모드에서 테스트 명령에 대해 사용자 권한 부여 및 엔드포인트 특성을 지정합니다. ASA에서는 DAP 레코드에 대한 AAA 선택 특성 및 엔드포인트 선택 특성을 평가할 때 DAP 하위 시스템에서 참조하는 특성 데이터베이스에 이를 기록합니다.

예

다음 예에서는 인증 사용자가 SAP 그룹의 멤버이고 엔드포인트 시스템에 안티바이러스 소프트웨어가 설치된 경우 ASA에서 2개의 DAP 레코드를 선택한다고 가정합니다. 안티바이러스 소프트웨어 엔드포인트 규칙을 위한 엔드포인트 ID는 *nav*입니다.

DAP 레코드는 다음 정책 특성을 갖습니다.

DAP Record 1	DAP Record 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
—	url-entry = enable

```
ciscoasa # test dynamic-access-policy attributes
ciscoasa(config-dap-test-attr)# attribute aaa.ldap.memberof SAP
ciscoasa(config-dap-test-attr)# attribute endpoint.av.nav.exists true
ciscoasa(config-dap-test-attr)# exit

ciscoasa # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

ciscoasa #
```

관련 명령I

명령	설명
display	현재 특성 목록을 표시합니다.
dynamic-access-policy-record	DAP 레코드를 생성합니다.
test dynamic-access-policy attributes	특성을 입력합니다.
test dynamic-access-policy execute	DAP를 생성하고 그 결과 액세스 정책을 콘솔에 표시하는 로직을 실행합니다.

auth-cookie-name

인증 쿠키의 이름을 지정하려면 aaa-server 호스트 컨피그레이션 모드에서 **auth-cookie-name** 명령을 사용합니다. 이는 HTTP Forms 명령을 사용하는 SSO입니다.

auth-cookie-name

구문 설명

name	인증 쿠키의 이름. 이름은 최대 128자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

ASA의 WebVPN 서버는 SSO 서버에 SSO 인증 요청을 보내는 데 HTTP POST 요청을 사용합니다. 인증에 성공하면 인증 웹 서버가 클라이언트 브라우저에 인증 쿠키를 보내줍니다. 클라이언트 브라우저는 그 인증 쿠키를 제시하면서 SSO 도메인의 다른 웹 서버에 인증합니다. **auth-cookie-name** 명령은 ASA에서 SSO에 사용할 인증 쿠키의 이름을 구성합니다.

인증 쿠키의 일반적인 형식은 *cookie name*=*cookie value* [;*cookie attributes*]입니다. 다음 인증 쿠키 예에서는 SMSESSION이 **auth-cookie-name** 명령으로 구성될 이름입니다.

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o
88uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma
5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;
Path=/
```

예

다음 예에서는 example.com이라는 웹 서버로부터 받은 인증 쿠키에 대해 SMSESSION이라는 이름을 지정합니다.

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# auth-cookie-name SMSESSION
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
action-uri	SSO 인증을 위한 사용자 이름 및 비밀번호를 받을 웹 서버 URI를 지정합니다.
hidden-parameter	인증 웹 서버와 교환할 숨겨진 매개변수를 만듭니다.
password-parameter	SSO 인증을 위해 사용자 비밀번호를 전송해야 하는 HTTP POST 요청 매개변수의 이름을 지정합니다.
start-url	로그인 전 쿠키를 검색할 URL을 지정합니다.
user-parameter	SSO 인증에 사용할 HTTP POST 요청에 사용자 이름 매개변수를 포함시켜 보내도록 지정합니다.

authenticated-session-username

이중 인증이 활성화된 경우 해당 세션에 어떤 인증 사용자 이름을 연결할지 지정하려면 tunnel-group general-attributes 모드에서 **authenticated-session-username** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

authenticated-session-username {primary | secondary}

no authenticated-session-username

구문 설명

primary	기본 인증 서버의 사용자 이름을 사용합니다.
secondary	보조 인증 서버의 사용자 이름을 사용합니다.

기본값

기본값은 **primary**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 이중 인증이 활성화된 경우에 사용할 수 있습니다. **authenticated-session-username** 명령은 ASA에서 세션의 사용자 이름을 추출할 인증 서버를 선택합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 remotegrp라는 IPsec 원격 액세스 터널 그룹을 만들고 보조 인증 서버의 사용자 이름을 연결에 사용하도록 지정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authenticated-session-username secondary
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

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

authentication-attr-from-server

이중 인증이 활성화된 경우 어떤 인증 서버 권한 부여 특성을 연결에 적용할지 지정하려면 tunnel-group general-attributes 모드에서 **authentication-attr-from-server** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

authentication-attr-from-server {primary | secondary}

no authentication-attr-from-server

구문 설명

primary	기본 인증 서버를 사용합니다.
secondary	보조 인증 서버를 사용합니다.

기본값

기본값은 **primary**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 이중 인증이 활성화된 경우에 사용할 수 있습니다. **authentication-attr-from-server** 명령은 ASA에서 연결에 적용할 권한 부여 특성을 추출하는 인증 서버를 선택합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 remotegrp라는 IPsec 원격 액세스 터널 그룹을 만들고 연결에 적용할 권한 부여 특성을 보조 인증 서버에서 얻도록 지정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-attr-from-server secondary
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

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

authentication-certificate

연결을 설정하는 WebVPN 클라이언트에서 인증서를 요청하려면 webvpn 컨피그레이션 모드에서 **authentication-certificate** 명령을 사용합니다. 클라이언트 인증서 요구 사항을 취소하려면 이 명령의 **no** 형식을 사용합니다.

authentication-certificate *interface-name*

no authentication-certificate [*interface-name***]**

구문 설명

interface-name	연결 설정에 사용하는 인터페이스의 이름. 사용 가능한 인터페이스 이름: • **inside** 인터페이스 GigabitEthernet0/1의 이름 • **outside** 인터페이스 GigabitEthernet0/0의 이름

기본값

authentication-certificate 명령을 생략하면 클라이언트 인증서 인증이 비활성화됩니다. **authentication-certificate** 명령에서 인터페이스 이름을 지정하지 않으면 기본 인터페이스 이름은 **inside**가 됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

이 명령이 적용되려면 먼저 해당 인터페이스에서 WebVPN이 활성화되어야 합니다. **interface**, **IP address**, **nameif** 명령으로 인터페이스가 구성되고 명명됩니다.

이 명령은 WebVPN 클라이언트 연결에만 적용됩니다. 그러나 **http authentication-certificate** 명령을 사용하여 관리 연결을 위한 클라이언트 인증서 인증을 지정하는 기능은 WebVPN을 지원하지 않는 플랫폼을 포함한 모든 플랫폼에서 사용 가능합니다.

ASA는 PKI 신뢰 지점을 사용하여 인증서를 검증합니다. 인증서가 검증을 통과하지 못하면 다음 중 하나가 수행됩니다.

조건:	결과:
ASA에 포함된 로컬 CA가 활성화되지 않았습니다.	ASA는 SSL 연결을 종료합니다.
로컬 CA가 활성화되었고 AAA 인증은 활성화되지 않았습니다.	ASA는 로컬 CA가 인증서를 얻을 수 있도록 클라이언트를 인증서 등록 페이지에 리디렉션합니다.
로컬 CA와 AAA 인증 모두 활성화됩니다.	클라이언트가 AAA 인증 페이지에 리디렉션됩니다. 구성된 경우 클라이언트는 로컬 CA 등록 페이지의 링크도 받습니다.

예

다음 예에서는 외부 인터페이스의 WebVPN 사용자 연결을 위해 인증서 인증을 구성합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
authentication(tunnel-group webvpn 컨피그레이션 모드)	터널 그룹의 멤버가 인증에 반드시 디지털 인증서를 사용하도록 지정합니다.
http authentication-certificate	ASA와의 ASDM 관리 연결에 인증서를 사용하여 인증하도록 지정합니다.
interface	연결 설정에 사용할 인터페이스를 구성합니다.
show running-config ssl	구성된 SSL 명령의 현재 세트를 표시합니다.
ssl trust-point	SSL 인증서 신뢰 지점을 구성합니다.

authentication-exclude

최종 사용자가 클라이언트리스 SSL VPN에 로그인하지 않고 구성된 링크로 이동할 수 있게 하려면 webvpn 컨피그레이션 모드에서 **authentication-exclude** 명령을 입력합니다. 여러 사이트에 대한 액세스를 허용하려면 이 명령을 여러 번 사용합니다.

authentication-exclude *url-fnmatch*

구문 설명

url-fnmatch	클라이언트리스 SSL VPN 로그인 요구 사항을 면제할 링크를 식별합니다.

명령 기본값

비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

이 기능은 일부 내부 리소스를 SSL VPN을 통해 공개적으로 사용해야 하는 경우에 유용합니다.

링크에 대한 정보를 SSL VPN-mangled 형식으로 최종 사용자에게 배포해야 합니다. 이를테면 SSL VPN을 사용하여 이 리소스로 이동한 다음 그 결과 URL을 배포할 링크 정보에 복사합니다.

예

다음 예에서는 2개 사이트를 인증 요구 사항에서 제외하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-exclude http://www.example.com/public/*
ciscoasa(config-webvpn)# authentication-exclude *example.html
ciscoasa(config-webvpn)# ciscoasa #
```

authentication

WebVPN 및 이메일 프록시의 인증 방법을 구성하려면 여러 모드에서 **authentication** 명령을 사용합니다. 기본 방법을 복원하려면 이 명령의 **no** 형식을 사용합니다. ASA는 사용자의 신원을 확인하기 위해 사용자를 인증합니다.

authentication {[aaa] [certificate] [mailhost] [piggyback]}

no authentication [**aaa**] [**certificate**] [**mailhost**] [**piggyback**]

구문 설명

aaa	ASA에서 이전에 구성된 AAA 서버로 확인할 사용자 이름 및 비밀번호를 제공합니다.
certificate	SSL 협상 과정에서 인증서를 제공합니다.
mailhost	SMTPS에 한해 원격 메일 서버를 통해 인증합니다. IMAP4S 및 POP3S는 메일호스트 인증이 필수이므로 구성 가능한 옵션으로 표시되지 않습니다.
piggyback	HTTPS WebVPN 세션이 이미 있어야 합니다. 피기백 인증은 이메일 프록시에만 사용할 수 있습니다.

기본값

다음 표는 WebVPN 및 이메일 프록시를 위한 기본 인증 방법을 보여줍니다.

프로토콜	기본 인증 방법
IMAP4S	메일호스트(필수)
POP3S	메일호스트(필수)
SMTPS	AAA
WebVPN	AAA

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
7.1(1)	이 명령을 webvpn 컨피그레이션 모드에서 더 이상 사용하지 않으며 WebVPN의 tunnel-group webvpn-attributes 컨피그레이션 모드로 이동했습니다.
8.0(2)	인증서 인증 요구 사항의 변경을 반영하여 이 명령을 수정했습니다.

사용 지침

하나 이상의 인증 방법이 필요합니다. 예를 들어, WebVPN에서는 AAA 인증, 인증서 인증 또는 둘 다 지정할 수 있습니다. 이 명령은 어떤 순서로도 입력할 수 있습니다.

WebVPN 인증서 인증에서는 각 인터페이스의 HTTP 사용자 인증서가 필요합니다. 즉 이 선택이 적용되려면 인증서 인증을 지정하기 전에 **authentication-certificate** 명령에서 인터페이스를 지정해야 합니다.

webvpn 컨피그레이션 모드에서 이 명령을 입력하면 tunnel-group webvpn-attributes 컨피그레이션 모드의 동일한 명령으로 변환됩니다.

WebVPN에서는 AAA 인증과 인증서 인증을 모두 요구할 수 있습니다. 그러면 사용자는 인증서, 사용자 이름과 비밀번호를 모두 제공해야 합니다. 이메일 프록시 인증에서는 둘 이상의 인증 방법을 요구할 수 있습니다. 이 명령을 다시 지정하면 기존 컨피그레이션을 덮어씁니다.

예

다음 예에서는 WebVPN 사용자가 인증을 위해 인증서를 제공하도록 요구하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication certificate
```

관련 명령

명령	설명
authentication-certificate	연결을 설정하는 WebVPN 클라이언트에 인증서를 요청합니다.
show running-config	현재 터널 그룹 컨피그레이션을 표시합니다.
clear configure aaa	구성된 AAA 값을 제거하거나 재설정합니다.
show running-config aaa	AAA 컨피그레이션을 표시합니다.

authentication eap-proxy

L2TP over IPsec 연결의 경우, EAP를 활성화하고 ASA에서 외부 RADIUS 인증 서버와의 PPP 인증 프로세스를 프록시하게 하려면 tunnel-group ppp-attributes 컨피그레이션 모드에서 **authentication eap-proxy** 명령을 사용합니다. 명령을 기본 설정으로 되돌리려면(CHAP 및 MS-CHAP 허용), 이 명령의 **no** 형식을 사용합니다.

authentication eap-proxy

no authentication eap-proxy

구문 설명

이 명령은 키워드 또는 인수가 없습니다.

기본값

기본적으로 EAP는 허용되는 인증 프로토콜이 아닙니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

L2TP over IPsec 터널 그룹 유형에만 이 특성을 적용할 수 있습니다.

예

config-ppp 컨피그레이션 모드에서 입력한 다음 예에서는 ppremotegrp라는 터널 그룹에 대해 PPP 연결을 위한 EAP를 허용합니다.

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication eap
ciscoasa(config-ppp)#
```

관련 명령

명령	설명
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	지정된 인증서 맵 엔트리를 표시합니다.
tunnel-group-map default-group	**crypto ca certificate map** 명령으로 생성된 인증서 맵 엔트리를 터널 그룹과 연결합니다.

authentication key eigrp

EIGRP 패킷의 인증을 활성화하고 인증 키를 지정하려면 인터페이스 컨피그레이션 모드에서 **authentication key eigrp** 명령을 사용합니다. EIGRP 인증을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

authentication key eigrp *as-number key* **key-id** *key-id*

no authentication key eigrp *as-number*

구문 설명

as-number	인증되는 EIGRP 프로세스의 자율 시스템 번호. EIGRP 라우팅 프로세스에 대해 구성된 것과 동일한 값이어야 합니다.
key	EIGRP 업데이트를 인증하기 위한 키. 키는 최대 16자를 포함할 수 있습니다.
key-id *key-id*	키 식별 값. 유효한 값의 범위는 1~255입니다.

기본값

EIGRP 인증이 비활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

EIGRP 메시지 인증을 활성화하려면 인터페이스에서 **authentication mode eigrp** 및 **authentication key eigrp** 명령을 모두 구성해야 합니다. 인터페이스에서 구성된 **authentication** 명령을 보려면 **show running-config interface** 명령을 사용합니다.

예

다음 예에서는 인터페이스 GigabitEthernet0/3에 구성된 EIGRP 인증을 보여줍니다.

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# authentication mode eigrp md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

관련 명령

명령	설명
authentication mode eigrp	EIGRP 인증에 사용할 인증의 유형을 지정합니다.

authentication mode eigrp

EIGRP 인증에 사용할 인증의 유형을 지정하려면 인터페이스 컨피그레이션 모드에서 **authentication mode eigrp** 명령을 사용합니다. 기본 인증 방법을 복원하려면 이 명령의 **no** 형식을 사용합니다.

authentication mode eigrp *as-num* **md5**

no authentication mode eigrp *as-num* **md5**

구문 설명

as-num	EIGRP 라우팅 프로세스의 자율 시스템 번호.
md5	EIGRP 메시지 인증에 MD5를 사용합니다.

기본값

기본적으로 어떤 인증도 제공하지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

EIGRP 메시지 인증을 활성화하려면 인터페이스에서 **authentication mode eigrp** 및 **authentication key eigrp** 명령을 모두 구성해야 합니다. 인터페이스에서 구성된 **authentication** 명령을 보려면 **show running-config interface** 명령을 사용합니다.

예

다음 예에서는 인터페이스 GigabitEthernet0/3에 구성된 EIGRP 인증을 보여줍니다.

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# authentication mode eigrp 100 md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

관련 명령

명령	설명
authentication key eigrp	EIGRP 패킷의 인증을 활성화하고 인증 키를 지정합니다.

authentication ms-chap-v1

L2TP over IPsec 연결의 경우 PPP를 위한 Microsoft CHAP, Version 1 인증을 활성화하려면 tunnel-group ppp-attributes 컨피그레이션 모드에서 **authentication ms-chap-v1** 명령을 사용합니다. 이 명령을 기본 설정으로 되돌리려면(CHAP 및 MS-CHAP 허용) 이 명령의 **no** 형식을 사용합니다. Microsoft CHAP, Version 1을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

authentication ms-chap-v1

no authentication ms-chap-v1

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

L2TP over IPsec 터널 그룹 유형에만 이 특성을 적용할 수 있습니다. 이 프로토콜은 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. 이 프로토콜에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.

관련 명령

명령	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 지정된 터널 그룹만 지웁니다.
show running-config tunnel-group	지정된 터널 그룹 또는 모든 터널 그룹에 대해 현재 실행 중인 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group	IPsec 및 WebVPN 터널을 위해 연결 관련 레코드의 데이터베이스를 만들고 관리합니다.

authentication ms-chap-v2

L2TP over IPsec 연결의 경우 PPP를 위한 Microsoft CHAP, Version 2 인증을 활성화하려면 tunnel-group ppp-attributes 컨피그레이션 모드에서 **authentication ms-chap-v1** 명령을 사용합니다. 명령을 기본 설정으로 되돌리려면(CHAP 및 MS-CHAP 허용), 이 명령의 **no** 형식을 사용합니다.

authentication ms-chap-v2

no authentication ms-chap-v2

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

L2TP over IPsec 터널 그룹 유형에만 이 특성을 적용할 수 있습니다.

이 프로토콜은 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. 이 프로토콜에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.

관련 명령

명령	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 지정된 터널 그룹만 지웁니다.
show running-config tunnel-group	지정된 터널 그룹 또는 모든 터널 그룹에 대해 현재 실행 중인 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group	IPsec 및 WebVPN 터널을 위해 연결 관련 레코드의 데이터베이스를 만들고 관리합니다.

authentication pap

L2TP over IPsec 연결에서 PPP를 위한 PAP 인증을 허용하려면 tunnel-group ppp-attributes 컨피그레이션 모드에서 **authentication pap** 명령을 사용합니다. 명령을 기본 설정으로 되돌리려면(CHAP 및 MS-CHAP 허용), 이 명령의 **no** 형식을 사용합니다.

authentication pap

no authentication pap

구문 설명

이 명령은 키워드 또는 인수가 없습니다.

기본값

기본적으로 PAP는 허용되는 인증 프로토콜이 아닙니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

L2TP over IPsec 터널 그룹 유형에만 이 특성을 적용할 수 있습니다.

이 프로토콜은 인증 과정에서 일반 텍스트 사용자 이름과 비밀번호를 전달하므로 안전하지 않습니다.

예

config-ppp 컨피그레이션 모드에서 입력한 다음 예에서는 ppremotegrp라는 터널 그룹에 대해 PPP 연결을 위한 PAP를 허용합니다.

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication pap
ciscoasa(config-ppp)#
```

관련 명령

명령	설명
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	지정된 인증서 맵 엔트리를 표시합니다.
tunnel-group-map default-group	**crypto ca certificate map** 명령으로 생성된 인증서 맵 엔트리를 터널 그룹과 연결합니다.

authentication-certificate

연결을 설정하는 WebVPN 클라이언트에서 인증서를 요청하려면 webvpn 컨피그레이션 모드에서 **authentication-certificate** 명령을 사용합니다. 클라이언트 인증서 요구 사항을 취소하려면 이 명령의 **no** 형식을 사용합니다.

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

구문 설명

interface-name	연결 설정에 사용하는 인터페이스의 이름. 사용 가능한 인터페이스 이름: • **inside** 인터페이스 GigabitEthernet0/1의 이름 • **outside** 인터페이스 GigabitEthernet0/0의 이름

기본값

authentication-certificate 명령을 생략하면 클라이언트 인증서 인증이 비활성화됩니다. **authentication-certificate** 명령에서 인터페이스 이름을 지정하지 않으면 기본 인터페이스 이름은 **inside**가 됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

이 명령이 적용되려면 먼저 해당 인터페이스에서 WebVPN이 활성화되어야 합니다. **interface**, **IP address**, **nameif** 명령으로 인터페이스가 구성되고 명명됩니다.

이 명령은 WebVPN 클라이언트 연결에만 적용됩니다. 그러나 **http authentication-certificate** 명령을 사용하여 관리 연결을 위한 클라이언트 인증서 인증을 지정하는 기능은 WebVPN을 지원하지 않는 플랫폼을 포함한 모든 플랫폼에서 사용 가능합니다.

ASA는 PKI 신뢰 지점을 사용하여 인증서를 검증합니다. 인증서가 검증을 통과하지 못하면 다음 중 하나가 수행됩니다.

조건:	결과:
ASA에 포함된 로컬 CA가 활성화되지 않았습니다.	ASA는 SSL 연결을 종료합니다.
로컬 CA가 활성화되었고 AAA 인증은 활성화되지 않았습니다.	ASA는 로컬 CA가 인증서를 얻을 수 있도록 클라이언트를 인증서 등록 페이지에 리디렉션합니다.
로컬 CA와 AAA 인증 모두 활성화됩니다.	클라이언트가 AAA 인증 페이지에 리디렉션됩니다. 구성된 경우 클라이언트는 로컬 CA 등록 페이지의 링크도 받습니다.

예

다음 예에서는 외부 인터페이스의 WebVPN 사용자 연결을 위해 인증서 인증을 구성합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
authentication(tunnel-group webvpn 컨피그레이션 모드)	터널 그룹의 멤버가 인증에 반드시 디지털 인증서를 사용하도록 지정합니다.
http authentication-certificate	ASA와의 ASDM 관리 연결에 인증서를 사용하여 인증하도록 지정합니다.
interface	연결 설정에 사용할 인터페이스를 구성합니다.
show running-config ssl	구성된 SSL 명령의 현재 세트를 표시합니다.
ssl trust-point	SSL 인증서 신뢰 지점을 구성합니다.

authentication-port

이 호스트의 RADIUS 인증에 사용할 포트 번호를 지정하려면 aaa-server 호스트 컨피그레이션 모드에서 **authentication-port** 명령을 사용합니다. 인증 포트 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

authentication-port *port*

no authentication-port

구문 설명

port	RADIUS 인증을 위한 1-65535 범위의 포트 번호

기본값

기본적으로 디바이스는 포트 1645에서 RADIUS를 수신합니다(RFC 2058). 포트가 지정되지 않으면 RADIUS 인증의 기본 포트 번호(1645)가 사용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	RADIUS 서버를 포함하는 서버 그룹을 위해 호스트별 서버 포트 지정을 지원하도록 명령의 의미를 변경했습니다.

사용 지침

이 명령은 인증 기능을 지정할 원격 RADIUS 서버 호스트의 목적지 TCP/UDP 포트 번호를 지정합니다. RADIUS 인증 서버에서 1645이 아닌 포트를 사용할 경우, RADIUS 서비스를 시작하기에 앞서 **aaa-server** 명령을 사용하여 ASA에서 알맞은 포트를 구성합니다.

이 명령은 RADIUS를 위해 구성된 서버 그룹에서만 유효합니다.

예

다음 예에서는 호스트 "1.2.3.4"에서 "srvgrp1"이라는 RADIUS AAA 서버를 구성하고 시간 초과를 9초로, 재시도 간격을 7초로 설정하고 인증 포트 1650를 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-interval 7
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
aaa authentication	**aaa-server** 명령에 의해 또는 ASDM 사용자 인증에 의해 지정된 서버에서 LOCAL, TACACS+ 또는 RADIUS 사용자 인증을 활성화하거나 비활성화합니다.
aaa-server host	AAA 서버 호스트 컨피그레이션 모드를 시작합니다. 그러면 호스트에 특화된 AAA 서버 매개변수를 구성할 수 있습니다.
clear configure aaa-server	모든 AAA 명령문을 컨피그레이션에서 제거합니다.
show running-config aaa-server	특정 서버 그룹, 특정 그룹에 속한 특정 서버 또는 특정 프로토콜에 대해 모든 AAA 서버의 AAA 서버 통계를 표시합니다.

authentication-server-group(imap4s, pop3s, smtps, config-mdm-proxy)

이메일 프록시 및 MDM 프록시에 사용할 인증 서버의 집합을 지정하려면 다양한 모드에서 **authentication-server-group** 명령을 사용합니다. 인증 서버를 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

authentication-server-group *group_tag*

no authentication-server-group

구문 설명

group_tag	이미 구성된 인증 서버 또는 서버 그룹을 식별합니다.

기본값

기본적으로 어떤 인증 서버도 구성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Imap4s 컨피그레이션	• 예	—	• 예	—	—
Pop3s 컨피그레이션	• 예	—	• 예	—	—
Smtps 컨피그레이션	• 예	—	• 예	—	—
config-mdm-proxy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.3(1)	이 명령은 이제 config-mdm-proxy 모드에서 사용할 수 있습니다.

사용 지침

ASA는 사용자의 신원을 확인하기 위해 사용자를 인증합니다.

AAA 인증을 구성할 경우 이 특성도 구성해야 합니다. 그렇지 않으면 인증이 실패합니다.

인증 서버를 구성하려면 **aaa-server** 명령을 사용합니다.

예

다음 예에서는 "IMAP4SSVRS"라는 인증 서버 집합을 사용하기 위해 IMAP4S 이메일 프록시를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# authentication-server-group IMAP4SSVRS
```

다음 예에서는 "MDMSRVGRP"라는 권한 부여 서버 집합을 사용하기 위해 MDM 이메일 프록시를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-pop3s)# authentication-server-group MDMSRVGRP
```

관련 명령

명령	설명
aaa-server host	인증, 권한 부여, 어카운팅 서버를 구성합니다.

authentication-server-group(tunnel-group general-attributes)

터널 그룹의 사용자 인증에 사용할 AAA 서버 그룹을 지정하려면 tunnel-group general-attributes 컨피그레이션 모드에서 **authentication-server-group** 명령을 사용합니다. 이 특성을 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]

no authentication-server-group [(*interface_name*)] *server_group*

구문 설명

interface_name	(선택 사항) IPsec 터널이 종료할 인터페이스를 지정합니다.
LOCAL	(선택 사항) 서버 그룹의 모든 서버가 통신 장애로 비활성화된 경우 로컬 사용자 데이터베이스로 인증하도록 요구합니다.
server_group	이미 구성된 인증 서버 또는 서버 그룹을 식별합니다.

기본값

이 명령에서 server-group의 기본 설정은 **LOCAL**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	이 명령은 webvpn 컨피그레이션 모드에서 더 이상 사용되지 않으며 tunnel-group general-attributes 컨피그레이션 모드로 이동했습니다.
8.0(2)	IPSec 연결에 대해 인터페이스별 인증을 허용하도록 이 명령을 개선했습니다.

사용 지침

이 특성을 모든 터널 그룹 유형에 적용할 수 있습니다.

aaa-server 명령을 사용하여 인증 서버를 구성하고, **aaa-server-host** 명령을 사용하여 이미 구성된 AAA 서버 그룹에 서버를 추가합니다.

예

config-general 컨피그레이션 모드에서 입력한 다음 예에서는 remotegrp라는 IPsec 원격 액세스 터널 그룹을 위해 aaa-server456이라는 인증 서버 그룹을 구성합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)#
```

관련 명령

명령	설명
aaa-server	AAA 서버 그룹을 만들고 그룹 특정 및 모든 그룹 호스트 공통 AAA 서버 매개변수를 구성합니다.
aaa-server host	이미 구성된 AAA 서버 그룹에 서버를 추가하고 호스트별 AAA 서버 매개변수를 구성합니다.
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹의 터널 그룹 컨피그레이션을 표시합니다.

authorization-required

연결에 앞서 사용자의 권한 부여가 성공하도록 요구하려면 여러 모드에서 **authorization-required** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

authorization-required

no authorization-required

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Imap4s 컨피그레이션	• 예	—	• 예	—	—
Pop3s 컨피그레이션	• 예	—	• 예	—	—
Smtps 컨피그레이션	• 예	—	• 예	—	—
Tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	이 명령은 webvpn 컨피그레이션 모드에서 더 이상 사용되지 않으며 tunnel-group general-attributes 컨피그레이션 모드로 이동했습니다.
7.2(1)	webvpn 컨피그레이션 모드를 imap4s, pop3s, smtps 컨피그레이션 모드로 대체했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 remotegrp라는 원격 액세스 터널 그룹을 통해 연결하는 사용자에게 전체 DN 기반의 권한 부여를 요구합니다. 첫 번째 명령은 remotegrp라는 원격 그룹에 대해 터널 그룹 유형을 ipsec_ra(IPsec 원격 액세스)로 구성합니다. 두 번째 명령은 지정된 터널 그룹의 tunnel-group general-attributes 컨피그레이션 모드를 시작합니다. 마지막 명령은 명명된 터널 그룹에 대해 권한 부여가 필요하도록 지정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-required
ciscoasa(config-tunnel-general)#
```

관련 명령

명령	설명
authorization-dn-attributes	권한 부여를 위한 사용자 이름으로 사용할 기본 및 보조 주체 DN 필드를 지정합니다.
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	지정된 인증서 맵 엔트리를 표시합니다.
tunnel-group general-attributes	명명된 터널 그룹의 일반 특성을 지정합니다.

authorization-server-group

WebVPN 및 이메일 프록시와 함께 사용할 권한 부여 서버의 집합을 지정하려면 여러 모드에서 **authorization-server-group** 명령을 사용합니다. 권한 부여 서버를 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

authorization-server-group *group_tag*

no authorization-server-group

구문 설명

group_tag	이미 구성된 권한 부여 서버 또는 서버 그룹을 식별합니다. 권한 부여 서버를 구성하려면 **aaa-server** 명령을 사용합니다.

기본값

기본적으로 어떤 권한 부여 서버도 구성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Imap4s 컨피그레이션	• 예	—	• 예	—	—
Pop3s 컨피그레이션	• 예	—	• 예	—	—
Smtps 컨피그레이션	• 예	—	• 예	—	—
Tunnel-group general-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	이 명령은 webvpn 컨피그레이션 모드에서 더 이상 사용되지 않으며 tunnel-group general-attributes 컨피그레이션 모드로 이동했습니다.

사용 지침

ASA에서는 사용자에게 허용된 네트워크 리소스에 대한 액세스 레벨을 검증하는 데 권한 부여를 사용합니다.

webvpn 컨피그레이션 모드에서 이 명령을 입력하면 tunnel-group general-attributes 모드의 동일한 명령으로 변환됩니다.

VPN 권한 부여가 LOCAL로 정의되면 기본 그룹 정책 DfltGrpPolicy에 구성된 특성이 적용됩니다.

예

다음 예에서는 "POP3Spermit"라는 권한 부여 서버 집합을 사용하기 위해 POP3S 이메일 프록시를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# authorization-server-group POP3Spermit
```

tunnel-general 컨피그레이션 모드에서 입력한 다음 예에서는 "remotegrp"라는 IPsec 원격 액세스 터널 그룹을 위해 "aaa-server78"이라는 권한 부여 서버 그룹을 구성합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

관련 명령

명령	설명
aaa-server host	인증, 권한 부여, 어카운팅 서버를 구성합니다.
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹의 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group general-attributes	명명된 터널 그룹의 일반 특성을 지정합니다.

auth-prompt

through-the-ASA 사용자 세션을 위해 AAA 챌린지를 지정하거나 변경하려면 글로벌 컨피그레이션 모드에서 **auth-prompt** 명령을 사용합니다. 인증 챌린지 텍스트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

구문 설명

accept	텔넷을 통한 사용자 인증이 승인되면 *string* 프롬프트를 표시합니다.
prompt	이 키워드 다음에 AAA 챌린지 프롬프트 문자열이 옵니다.
reject	텔넷을 통한 사용자 인증이 거부되면 *string* 프롬프트를 표시합니다.
string	최대 235자의 영숫자 또는 31단어(두 한도 중 먼저 해당되는 것 적용)로 된 문자열입니다. 특수 문자, 공백, 구두점이 허용됩니다. 물음표를 입력하거나 **Enter** 키를 눌러 문자열을 종료합니다. 물음표는 문자열에 표시됩니다.

기본값

인증 프롬프트를 지정하지 않을 경우

- FTP 사용자에게는 `FTP authentication`이 표시됩니다.
- HTTP 사용자에게는 `HTTP Authentication`이 표시됩니다.
- 텔넷 사용자에게는 어떤 챌린지 텍스트도 표시되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	명령의 의미를 약간 변경했습니다.

사용 지침

auth-prompt 명령을 사용하면 TACACS+ 또는 RADIUS 서버의 사용자 인증이 필요할 때 ASA를 지나는 HTTP, FTP, 텔넷 액세스를 위한 AAA 챌린지 텍스트를 지정할 수 있습니다. 이 텍스트는 기본적으로 장식의 용도이며, 사용자가 로그인할 때 사용자 이름과 비밀번호 프롬프트 위에 표시됩니다.

텔넷 사용자 인증의 경우 **accept** 및 **reject** 옵션을 사용하여 AAA 서버에 의해 인증 시도가 승인되었거나 거부되었음을 알리는 여러 상태 프롬프트를 표시할 수 있습니다.

AAA 서버가 사용자를 인증하면 ASA는 **auth-prompt accept** 텍스트(지정된 경우)를 사용자에게 표시합니다. 그렇지 않으면 **reject** 텍스트(지정된 경우)를 표시합니다. HTTP 및 FTP 세션 인증은 프롬프트에서 챌린지 텍스트만 표시합니다. **accept** 및 **reject** 텍스트가 나타나지 않습니다.

참고 Microsoft Internet Explorer에서는 인증 프롬프트에 최대 37자를 표시합니다. 텔넷 및 FTP는 인증 프롬프트에 최대 235자를 표시합니다.

예

다음 예에서는 인증 프롬프트를 "Please enter your username and password."라는 문자열로 설정합니다.

```
ciscoasa(config)# auth-prompt prompt Please enter your username and password
```

이 문자열이 컨피그레이션에 추가되면 사용자에게 다음 메시지가 표시됩니다.

```
Please enter your username and password
User Name:
Password:
```

텔넷 사용자의 경우 다음과 같이 ASA에서 인증 시도를 승인하거나 거부할 때를 알리는 별도의 메시지를 제공할 수도 있습니다.

```
ciscoasa(config)# auth-prompt reject Authentication failed. Try again.
ciscoasa(config)# auth-prompt accept Authentication succeeded.
```

다음 예에서는 성공적인 인증에 대한 인증 프롬프트를 "You’re OK."라는 문자열로 설정합니다.

```
ciscoasa(config)# auth-prompt accept You’re OK.
```

성공적으로 인증하면 사용자에게는 다음 메시지가 표시됩니다.

```
You’re OK.
```

관련 명령

명령	설명
clear configure auth-prompt	이전에 지정한 인증 프롬프트 챌린지 텍스트를 제거하고 기본값이 있다면 되돌립니다.
show running-config auth-prompt	현재 인증 프롬프트 챌린지 텍스트를 표시합니다.

auto-signon

ASA에서 클라이언트리스 SSL VPN 연결을 위한 사용자 로그인 자격 증명을 내부 서버에 자동으로 전달하도록 구성하려면 webvpn 컨피그레이션, webvpn 그룹 컨피그레이션 또는 webvpn 사용자 이름 컨피그레이션 모드 중 하나에서 **auto-signon** 명령을 사용합니다. 특정 서버에 대한 자동 로그인을 비활성화하려면 이 명령의 **no** 형식을 원래의 **ip**, **uri**, **auth-type** 인수와 함께 사용합니다. 모든 서버에 대한 자동 로그인을 비활성화하려면 이 명령의 **no** 형식을 인수 없이 사용합니다.

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type {basic | ftp | ntlm | all}**

no auto-signon [**allow {ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type {basic | ftp | ntlm | all}**]

구문 설명

all	NTLM 및 HTTP Basic 인증 방법을 모두 지정합니다.
allow	특정 서버에 대한 인증을 활성화합니다.
auth-type	인증 방법을 선택할 수 있게 합니다.
basic	HTTP Basic 인증 방법을 지정합니다.
ftp	ftp 및 cifs 인증 유형.
ip	IP 주소 및 마스크로 인증할 서버를 식별하게 합니다.
ip-address	*ip-mask*와 함께 사용하면서 인증할 서버의 IP 주소 범위를 식별합니다.
ip-mask	*ip-address*와 함께 사용하면서 인증할 서버의 IP 주소 범위를 식별합니다.
ntlm	NTLMv1 인증 방법을 지정합니다.
resource-mask	인증할 서버의 URI 마스크를 식별합니다.
uri	URI 마스크로 인증할 서버를 식별하게 합니다.

기본값

기본적으로 이 기능은 모든 서버에 대해 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Webvpn 컨피그레이션(글로벌)	• 예	—	• 예	—	—
Webvpn 그룹 정책 컨피그레이션	• 예	—	• 예	—	—
Webvpn 사용자 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.
8.0(1)	NTLMv2 지원을 추가했습니다. **ntlm** 키워드가 NTLMv1과 NTLMv2를 모두 포함합니다.

사용 지침

auto-signon 명령은 클라이언트리스 SSL VPN 사용자를 위한 SSO 방법입니다. NTLM 인증, HTTP Basic 인증 또는 둘 다를 사용하는 인증을 위해 로그인 자격 증명(사용자 이름, 비밀번호)을 내부 서버에 전달합니다. 여러 자동 로그인 명령을 입력할 수 있으며, 이는 입력 순서에 따라 처리됩니다. 즉 먼저 입력된 명령이 우선합니다.

자동 로그온 기능은 webvpn 컨피그레이션 그룹 정책, webvpn 컨피그레이션 또는 webvpn 사용자 이름 컨피그레이션 모드의 3가지 모드에서 사용할 수 있습니다. 일반적인 우선 순위 동작이 적용됩니다. 즉 사용자 이름이 그룹에, 그룹이 전역에 우선합니다. 선택하는 모드는 원하는 인증 범위에 따라 달라집니다.

모드	범위
Webvpn 컨피그레이션	모든 WebVPN 사용자
Webvpn 그룹 컨피그레이션	그룹 정책에 의해 정의되는 WebVPN 사용자의 하위 그룹
Webvpn 사용자 컨피그레이션	개별 WebVPN 사용자

예

다음 예에서는 모든 클라이언트리스 사용자를 위해 자동 로그인을 구성합니다. NTLM 인증을 사용하며, 서버의 주소 범위는 10.1.1.0~10.1.1.255입니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

다음 예에서는 모든 클라이언트리스 사용자를 위해 자동 로그인을 구성합니다. HTTP Basic 인증을 사용하며 서버는 URI 마스크 https://*.example.com/*에 의해 정의됩니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

다음 예에서는 ExamplePolicy 그룹 정책의 클라이언트리스 사용자를 위해 자동 로그인을 구성합니다. HTTP Basic 또는 NTLM 인증을 사용하며 서버는 URI 마스크 https://*.example.com/*에 의해 정의됩니다.

```
ciscoasa(config)# group-policy ExamplePolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

다음 예에서는 Anyuser라는 사용자를 위해 자동 로그인을 구성합니다. HTTP Basic 인증을 사용하며, 서버의 주소 범위는 10.1.1.0~10.1.1.255입니다.

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
basic
```

관련 명령

명령	설명
show running-config webvpn auto-signon	실행 중인 컨피그레이션의 자동 로그인 지정을 표시합니다.

auto-summary

서브넷 경로를 네트워크 레벨 경로로 자동 요약할 수 있게 하려면 라우터 컨피그레이션 모드에서 **auto-summary** 명령을 사용합니다. 경로 요약을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

auto-summary

no auto-summary

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

RIP Version 1, RIP Version 2, EIGRP에 대해 경로 요약이 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
8.0(2)	EIGRP 지원을 추가했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

경로를 요약하면 라우팅 테이블에서 라우팅 정보의 양이 줄어듭니다.

RIP Version 1은 항상 자동 요약을 사용합니다. RIP Version 1에서는 자동 요약을 비활성화할 수 없습니다.

RIP Version 2를 사용할 경우 **no auto-summary** 명령으로 자동 요약을 끌 수 있습니다. 연결되지 않은 서브넷 간의 라우팅을 수행해야 하는 경우 자동 요약을 비활성화합니다. 자동 요약이 비활성화되면 서브넷이 광고됩니다.

EIGRP 요약 경로는 관리 거리의 값이 5입니다. 이 값은 구성할 수 없습니다.

이 명령의 **no** 형식만 실행 중인 컨피그레이션에 나타납니다.

예

다음 예에서는 RIP 경로 요약을 비활성화합니다.

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
ciscoasa(config-router)# no auto-summary
```

다음 예에서는 자동 EIGRP 경로 요약을 비활성화합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# no auto-summary
```

관련 명령

명령	설명
clear configure router	실행 중인 컨피그레이션에서 모든 **router** 명령 및 라우터 컨피그레이션 모드 명령을 지웁니다.
router eigrp	EIGRP 라우팅 프로세스를 활성화하고 EIGRP 라우터 컨피그레이션 모드로 들어갑니다.
router rip	RIP 라우팅 프로세스를 활성화하고 RIP 라우터 컨피그레이션 모드로 들어갑니다.
show running-config router	실행 중인 컨피그레이션의 **router** 명령 및 라우터 컨피그레이션 모드 명령을 표시합니다.

auto-update device-id

자동 업데이트 서버에 사용할 ASA 디바이스 ID를 구성하려면 글로벌 컨피그레이션 모드에서 **auto-update device-id** 명령을 사용합니다. 디바이스 ID를 제거하려면 이 명령의 **no** 형식을 사용합니다.

auto-update device-id [hardware-serial | hostname | ipaddress [*if_name***] | mac-address [***if_name***] | string** *text***]**

no auto-update device-id [hardware-serial | hostname | ipaddress [*if_name***] | mac-address [***if_name***] | string** *text***]**

구문 설명

hardware-serial	디바이스를 고유하게 식별하기 위해 ASA의 하드웨어 일련 번호를 사용합니다.
hostname	디바이스를 고유하게 식별하기 위해 ASA의 호스트 이름을 사용합니다.
ipaddress [*if_name*]	ASA의 IP 주소를 사용하여 ASA를 고유하게 식별합니다. 기본적으로 ASA에서는 자동 업데이트 서버와의 통신에 쓰이는 인터페이스를 사용합니다. 다른 IP 주소를 사용하려면 *if_name* 옵션을 지정합니다.
mac-address [*if_name*]	ASA의 MAC 주소를 사용하여 ASA를 고유하게 식별합니다. 기본적으로 ASA에서는 자동 업데이트 서버와의 통신에 쓰이는 인터페이스의 MAC 주소를 사용합니다. 다른 MAC 주소를 사용하려면 *if_name* 옵션을 지정합니다.
string *text*	자동 업데이트 서버에 디바이스를 고유하게 식별하기 위한 텍스트 문자열을 지정합니다.

기본값

기본 ID는 호스트 이름입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 디바이스 ID를 일련 번호로 설정합니다.

```
ciscoasa(config)# auto-update device-id hardware-serial
```

관련 명령

auto-update poll-period	ASA에서 자동 업데이트 서버의 업데이트를 확인하는 빈도를 설정합니다.
auto-update server	자동 업데이트 서버를 식별합니다.
auto-update timeout	자동 업데이트 서버가 이 기간 내에 연결되지 않을 경우 트래픽이 ASA를 지날 수 없게 합니다.
clear configure auto-update	자동 업데이트 서버 컨피그레이션을 지웁니다.
show running-config auto-update	자동 업데이트 서버 컨피그레이션을 표시합니다.

auto-update poll-at

ASA에서 자동 업데이트 서버를 폴링하는 시점을 예약하려면 글로벌 컨피그레이션 모드에서 **auto-update poll-at** 명령을 사용합니다. ASA에서 자동 업데이트 서버를 폴링하도록 예약된 시간을 모두 제거하려면 이 명령의 **no** 형식을 사용합니다.

auto-update poll-at *days-of-the-week time* **[randomize** *minutes***] [***retry_count* **[***retry_period***]]**

no auto-update poll-at *days-of-the-week time* **[randomize** *minutes***] [***retry_count* **[***retry_period***]]**

구문 설명

days-of-the-week	하나의 요일 또는 여러 요일의 조합: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. 그 밖에도 daily (Monday through Sunday), weekdays (Monday through Friday), weekend (Saturday and Sunday)를 값으로 선택할 수 있습니다.
randomize *minutes*	지정된 시작 시간 이후에 폴링 시간을 무작위화하는 기간을 지정합니다. 범위는 1분~1439분입니다.
retry_count	첫 번째 시도가 실패한 경우 자동 업데이트 서버와의 재연결을 시도할 횟수를 지정합니다. 기본값은 0입니다.
retry_period	연결을 재시도하기 전에 기다리는 시간을 지정합니다. 기본값은 5분입니다. 범위는 1분~35791분입니다.
time	폴링을 시작할 시간을 HH:MM 형식으로 지정합니다. 예를 들어, 8:00는 오전 08:00, 20:00는 오후 08:00입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

auto-update poll-at 명령은 업데이트 폴링을 수행할 시점을 지정합니다. **randomize** 옵션을 활성화할 경우 첫 번째 *time* 옵션 이후 지정된 시간(분)의 범위에서 무작위 시간에 폴링이 수행됩니다. **auto-update poll-at** 명령과 **auto-update poll-period** 명령은 동시에 사용할 수 없습니다. 둘 중 하나만 구성할 수 있습니다.

예

다음 예에서는 ASA가 매주 금요일 및 토요일 저녁, 오후 10:00시~오후 11:00시의 무작위 시간에 자동 업데이트 서버를 폴링합니다. ASA에서 서버에 연결하지 못하면 10분 간격으로 2번 더 시도합니다.

```
ciscoasa(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
ciscoasa(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

관련 명령

auto-update device-id	자동 업데이트 서버에 사용할 ASA 디바이스 ID를 설정합니다.
auto-update poll-period	ASA에서 자동 업데이트 서버의 업데이트를 확인하는 빈도를 설정합니다.
auto-update timeout	자동 업데이트 서버가 이 기간 내에 연결되지 않을 경우 트래픽이 ASA를 지날 수 없게 합니다.
clear configure auto-update	자동 업데이트 서버 컨피그레이션을 지웁니다.
management-access	ASA에서 내부 관리 인터페이스에 대한 액세스를 활성화합니다.
show running-config auto-update	자동 업데이트 서버 컨피그레이션을 표시합니다.

auto-update poll-period

ASA에서 자동 업데이트 서버에 업데이트를 확인하는 빈도를 구성하려면 글로벌 컨피그레이션 모드에서 **auto-update poll-period** 명령을 사용합니다. 매개변수를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

auto-update poll-period *poll_period* **[***retry_count* **[***retry_period***]]**

no auto-update poll-period *poll_period* **[***retry_count* **[***retry_period***]]**

구문 설명

poll_period	자동 업데이트 서버를 폴링할 빈도를 1분~35791분의 범위에서 지정합니다. 기본값은 720분(12시간)입니다.
retry_count	첫 번째 시도가 실패한 경우 자동 업데이트 서버와의 재연결을 시도할 횟수를 지정합니다. 기본값은 0입니다.
retry_period	연결 시도의 간격을 1분~35791분의 범위에서 지정합니다. 기본값은 5분입니다.

기본값

기본 폴링 기간은 720분(12시간)입니다.

최초 시도가 실패할 경우 자동 업데이트 서버와의 재연결을 시도하는 횟수의 기본값은 0입니다.

연결 시도 간격의 기본값은 5분입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

auto-update poll-at 명령과 **auto-update poll-period** 명령은 동시에 사용할 수 없습니다. 둘 중 하나만 구성할 수 있습니다.

예

다음 예에서는 폴링 기간을 360분, 재시도를 1, 재시도 기간을 3분으로 설정합니다.

```
ciscoasa(config)# auto-update poll-period 360 1 3
```

관련 명령

auto-update device-id	자동 업데이트 서버에 사용할 ASA 디바이스 ID를 설정합니다.
auto-update server	자동 업데이트 서버를 식별합니다.
auto-update timeout	자동 업데이트 서버가 이 기간 내에 연결되지 않을 경우 트래픽이 ASA를 지날 수 없게 합니다.
clear configure auto-update	자동 업데이트 서버 컨피그레이션을 지웁니다.
show running-config auto-update	자동 업데이트 서버 컨피그레이션을 표시합니다.

auto-update server

자동 업데이트 서버를 식별하려면 글로벌 컨피그레이션 모드에서 **auto-update server** 명령을 사용합니다. 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

auto-update server *url* **[source** *interface***] {verify-certificate | no-verification}**

no auto-update server *url* **[source** *interface***] {verify-certificate | no-verification}**

구문 설명

no-verification	자동 업데이트 서버 인증서를 검증하지 않습니다.
source *interface*	자동 업데이트 서버에 요청을 보낼 때 사용하는 인터페이스를 지정합니다. **management-access** 명령에서 지정한 것과 동일한 인터페이스를 지정할 경우 자동 업데이트 서버 요청은 관리 액세스에 사용되는 것과 동일한 IPsec VPN 터널을 통해 전달됩니다.
url	다음 구문을 사용하여 자동 업데이트 서버의 위치를 지정합니다. **http**[**s**]**:**[[*user*:*password*@]*location* [:*port*]] **/** *pathname*
verify-certificate	HTTPS에서는 자동 업데이트 서버가 반환하는 인증서를 검증합니다. 기본 설정입니다.

기본값

9.1 이하: 인증서 검증이 비활성화되어 있습니다.

9.2(1) 이상: **verify-certificate** 옵션이 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	다중 서버를 지원하도록 명령을 수정했습니다.
9.2(1)	자동 업데이트 서버 인증서 확인이 기본적으로 활성화됩니다. **no-verification** 키워드를 추가했습니다.

사용 지침

ASA는 정기적으로 자동 업데이트 서버에 연결하여 컨피그레이션, 운영 체제, ASDM 업데이트를 찾습니다.

여러 서버에서 자동 업데이트를 수행하도록 구성할 수 있습니다. 업데이트를 확인할 때 첫 번째 서버에 연결합니다. 이 시도가 실패하면 다음 서버에 연결합니다. 이 프로세스는 모든 서버를 시도할 때까지 계속됩니다. 모든 서버에 연결하지 못할 경우, 연결을 재시도하도록 자동 업데이트 폴링 기간이 구성되었다면 첫 번째 서버부터 연결을 재시도합니다.

자동 업데이트 기능이 제대로 작동하려면 **boot system configuration** 명령을 사용하고 여기서 유효한 부트 이미지를 지정해야 합니다. 또한 **asdm image** 명령을 auto-update와 함께 사용하여 ASDM 소프트웨어 이미지를 업데이트해야 합니다.

source *interface* 인수에 지정된 인터페이스가 **management-access** 명령에 지정된 것과 동일할 경우 자동 업데이트 서버에 대한 요청이 VPN 터널을 통해 전송됩니다.

9.2(1) 이상: 자동 업데이트 서버 인증서 검증이 기본적으로 활성화됩니다. 신규 컨피그레이션의 경우 명시적으로 인증서 검증을 비활성화해야 합니다. 이전 릴리스에서 업그레이드하는 경우, 인증서 검증을 활성화하지 않았다면 인증서 검증을 할 수 없고 다음 경고가 표시됩니다.

```
WARNING: The certificate provided by the auto-update servers will not be verified. In
order to verify this certificate please use the verify-certificate option.
```

컨피그레이션이 검증 없음(no verification)을 명시적으로 구성하도록 마이그레이션됩니다.

auto-update server no-verification

예

다음 예에서는 자동 업데이트 서버 URL을 설정하고 인터페이스를 outside로 지정합니다.

```
ciscoasa(config)# auto-update server http://10.1.1.1:1741/ source outside
verify-certificate
```

관련 명령

auto-update device-id	자동 업데이트 서버에 사용할 ASA 디바이스 ID를 설정합니다.
auto-update poll-period	ASA에서 자동 업데이트 서버의 업데이트를 확인하는 빈도를 설정합니다.
auto-update timeout	자동 업데이트 서버가 이 기간 내에 연결되지 않을 경우 트래픽이 ASA를 지날 수 없게 합니다.
clear configure auto-update	자동 업데이트 서버 컨피그레이션을 지웁니다.
management-access	ASA에서 내부 관리 인터페이스에 대한 액세스를 활성화합니다.
show running-config auto-update	자동 업데이트 서버 컨피그레이션을 표시합니다.

auto-update timeout

자동 업데이트 서버 연결의 시간 초과 기간을 설정하려면 글로벌 컨피그레이션 모드에서 **auto-update timeout** 명령을 사용합니다. 시간 초과를 제거하려면 이 명령의 **no** 형식을 사용합니다.

auto-update timeout [*period***]**

no auto-update timeout [*period***]**

구문 설명

period	시간 초과 기간을 1분~35791분 범위에서 지정합니다. 기본값은 0입니다. 즉 시간 초과가 없습니다. 시간 초과를 0으로 설정할 수 없습니다. 0으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

기본값

시간 초과의 기본값은 0입니다. 그러면 ASA에서 시간 초과가 일어나지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

시간 초과 조건은 syslog 메시지 201008을 통해 보고됩니다.

이 기간 내에 자동 업데이트 서버가 연결되지 않으면 ASA는 그 서버를 지나는 모든 트래픽을 중지합니다. ASA에서 최신 이미지와 컨피그레이션을 받을 수 있도록 시간 초과를 설정합니다.

예

다음 예에서는 시간 초과를 24시간으로 설정합니다.

```
ciscoasa(config)# auto-update timeout 1440
```

관련 명령

auto-update device-id	자동 업데이트 서버에 사용할 ASA 디바이스 ID를 설정합니다.
auto-update poll-period	ASA에서 자동 업데이트 서버의 업데이트를 확인하는 빈도를 설정합니다.
auto-update server	자동 업데이트 서버를 식별합니다.
clear configure auto-update	자동 업데이트 서버 컨피그레이션을 지웁니다.
show running-config auto-update	자동 업데이트 서버 컨피그레이션을 표시합니다.

4 장

backup ~ browse-networks 명령

backup

ASA 컨피그레이션, 인증서, 키, 이미지를 백업하려면 특별 권한 EXEC 모드에서 **backup** 명령을 사용합니다.

backup [/noconfirm] [context *name***] [cert-passphrase** *value***] [location** *path***]**

구문 설명

cert-passphrase *value*	VPN 인증서 및 사전 공유 키의 백업 과정에서 **cert-passphrase** 키워드로 식별되는 보안 키가 인증서 인코딩에 필요합니다. 인증서 인코딩 및 디코딩에 사용할 패스프레이즈를 PKCS12 형식으로 제공해야 합니다. 백업에는 인증서와 연결된 RSA 키 쌍만 포함되며 독립형 인증서는 제외됩니다.
context *ctx-name*	다중 컨텍스트 모드에서는 시스템 실행 영역에서 **context** 키워드를 입력하여 지정된 컨텍스트 파일을 백업합니다.
location *path*	백업 **위치**는 로컬 디스크 또는 원격 URL일 수 있습니다. 위치를 지정하지 않으면 다음 기본 이름이 사용됩니다. • 단일 모드—disk0:*hostname*.backup.*timestamp*.tar.gz • 다중 모드—disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz
/noconfirm	**location** 및 **cert-passphrase** 매개변수를 묻지 않도록 지정합니다. 경고 및 오류 메시지를 건너뛰고 계속 백업을 진행할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(2)	이 명령을 도입했습니다.

사용 지침

다음 지침을 참조하십시오.

- 백업을 시작하기에 앞서 백업 위치에 300MB 이상의 사용 가능한 디스크 공간이 있어야 합니다.
- 백업 중에 또는 백업 후에 컨피그레이션을 변경할 경우, 이 변경 사항은 백업에 포함되지 않습니다. 백업한 후 컨피그레이션을 변경한 다음 복원을 수행할 경우, 이 컨피그레이션 변경 사항은 덮어쓰기됩니다. 따라서 ASA가 다르게 작동할 수 있습니다.
- 한 번에 하나의 백업만 시작할 수 있습니다.

- 최초의 백업을 수행했을 때와 동일한 ASA 버전에만 컨피그레이션을 복원할 수 있습니다. 복원 툴을 사용하여 어떤 ASA 버전의 컨피그레이션을 다른 버전으로 마이그레이션할 수 없습니다. 컨피그레이션 마이그레이션이 필요할 경우, ASA에서는 새 ASA OS를 로드할 때 상주하는 시작 컨피그레이션을 자동으로 업그레이드합니다.
- 클러스터링을 사용할 경우 시작 컨피그레이션, 실행 중인 컨피그레이션, ID 인증서만 백업할 수 있습니다. 각 유닛에서 개별적으로 백업을 생성하고 복원해야 합니다.
- 장애 조치를 사용할 경우, 활성 유닛과 대기 유닛의 백업을 따로 생성하고 복원해야 합니다.
- ASA에 대해 마스터 패스프레이즈를 설정한 경우, 이 절차로 생성한 백업 컨피그레이션을 복원하는 데 마스터 패스프레이즈가 필요합니다. ASA의 마스터 패스프레이즈를 모를 경우, 백업을 진행하기 전에 CLI 컨피그레이션 가이드에서 마스터 패스프레이즈를 재설정하는 방법을 확인하십시오.
- PKCS12 데이터를 가져왔고(**crypto ca trustpoint** 명령 사용) 신뢰 지점에서 RSA 키를 사용할 경우, 가져온 키 쌍에는 신뢰 지점과 동일한 이름이 지정됩니다. 이러한 제한 때문에 ASDM 컨피그레이션을 복원한 다음 신뢰 지점과 그 키 쌍의 이름을 다르게 지정할 경우, 시작 컨피그레이션은 원래의 컨피그레이션과 동일하지만 실행 중인 컨피그레이션은 다른 키 쌍 이름을 가지게 됩니다. 따라서 키 쌍과 신뢰 지점에 서로 다른 이름을 사용하는 경우 원래의 컨피그레이션을 복원할 수 없습니다. 이 문제를 해결하려면 신뢰 지점과 그 키 쌍에 동일한 이름을 사용해야 합니다.
- CLI로 백업했다가 ASDM으로 복원할 수 없습니다. 그 반대도 마찬가지입니다.
- 각 백업 파일에는 다음 내용이 들어 있습니다.
  - 실행 중인 컨피그레이션
  - 시작 컨피그레이션
  - 모든 보안 이미지

    Cisco Secure Desktop & Host Scan 이미지

    Cisco Secure Desktop & Host Scan 설정

    AnyConnect(SVC) 클라이언트 이미지 및 프로필

    AnyConnect(SVC) 사용자 지정 및 변환
  - ID 인증서(ID 인증서와 연결된 RSA 키 쌍 포함, 독립형 키는 제외)
  - VPN 사전 공유 키
  - SSL VPN 컨피그레이션
  - APCF(Application Profile Custom Framework)
  - 북마크
  - 사용자 지정 설정
  - DAP(동적 액세스 정책)
  - 플러그인
  - 미리 채워진 연결 프로필 스크립트
  - 프록시 자동 구성
  - 변환 테이블
  - 웹 콘텐츠
  - 버전 정보

예

다음 예에서는 백업을 만드는 방법을 보여줍니다.

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco. You will be
required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file is used to
restore to a device with a different master passphrase, you will need to provide the
current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

관련 명령

명령	설명
restore	백업 파일에서 ASA 컨피그레이션, 키, 인증서, 이미지를 복원합니다.

backup interface

ASA 5505와 같이 스위치가 내장된 모델의 경우 인터페이스 컨피그레이션 모드에서 **backup interface** 명령을 사용하여 ISP 등에 VLAN 인터페이스를 백업 인터페이스로 지정합니다. 일반 운영 모드를 복원하려면 이 명령의 **no** 형식을 사용합니다.

backup interface vlan *number*

no backup interface vlan *number*

구문 설명

vlan *number*	백업 인터페이스의 VLAN ID를 지정합니다.

기본값

기본적으로 **backup interface** 명령은 비활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
7.2(2)	Security Plus 라이센스에서는 VLAN 인터페이스 수를 일반 트래픽용 3개, 백업 인터페이스용 1개, 장애 조치용 1개로 제한하지 않습니다. 다른 제한 없이 최대 20개의 인터페이스를 구성할 수 있습니다. 따라서 3개 이상의 인터페이스를 활성화하는 데 **backup interface** 명령을 사용할 필요 없습니다.

사용 지침

이 명령은 VLAN 인터페이스에 한해 인터페이스 컨피그레이션 모드에서 입력할 수 있습니다. 이 명령은 기본 인터페이스를 지나는 기본 경로가 다운되지 않는 한 해당 백업 인터페이스에서 모든 통과 트래픽을 차단합니다.

backup interface 명령으로 Easy VPN을 구성할 때 백업 인터페이스가 기본 인터페이스가 되면 ASA는 VPN 규칙을 이 기본 인터페이스로 이동합니다. 백업 인터페이스의 상태를 보려면 **show interface** 명령을 참조하십시오.

기본 인터페이스가 실패할 때 백업 인터페이스를 사용할 수 있도록 두 인터페이스 모두에서 기본 경로를 구성해야 합니다. 이를테면 2개의 기본 경로를 구성할 수 있습니다. 기본 인터페이스에는 관리 거리가 더 짧은 경로를, 백업 인터페이스에는 관리 거리가 더 긴 경로를 구성합니다. DHCP 서버에서 얻은 기본 경로에서 관리 거리를 재정의하려면 **dhcp client route distance** 명령을 참조하십시오. 이중 ISP 지원을 구성하려는 경우 자세한 내용은 **sla monitor** 및 **track rtr** 명령을 참조하십시오.

management-only 명령이 인터페이스에서 이미 구성된 상태라면 백업 인터페이스를 구성할 수 없습니다.

예

다음 예에서는 4개의 VLAN 인터페이스를 구성합니다. backup-isp 인터페이스는 기본 인터페이스가 다운되었을 때만 통과 트래픽을 허용합니다. **route** 명령은 기본 인터페이스와 백업 인터페이스의 기본 경로를 생성하는데, 백업 경로는 관리 거리가 더 적습니다.

```
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)# backup interface vlan 400
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)# 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)# route outside 0 0 10.1.1.2 1
ciscoasa(config)# route backup-isp 0 0 10.1.2.2 2
```

관련 명령

명령	설명
forward interface	어떤 인터페이스에서 다른 인터페이스로 가는 트래픽을 시작할 수 없게 합니다.
interface vlan	VLAN 인터페이스를 만들고 인터페이스 컨피그레이션 모드를 시작합니다.
dhcp client route distance	DHCP 서버에서 얻은 기본 경로의 관리 거리를 재정의합니다.
sla monitor	고정 경로 추적을 위해 SLA 모니터링 작업을 생성합니다.
track rtr	SLA 모니터링 작업의 상태를 추적합니다.

backup-servers

백업 서버를 구성하려면 그룹 정책 컨피그레이션 모드에서 **backup-servers** 명령을 사용합니다. 백업 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

backup-servers {*server1 server2. . . . server10* **| clear-client-config | keep-client-config}**

no backup-servers [*server1 server2. . . . server10* **| clear-client-config | keep-client-config]**

구문 설명

clear-client-config	클라이언트에서 백업 서버를 사용하지 않도록 지정합니다. ASA는 null 서버 목록을 푸시합니다.
keep-client-config	ASA에서 클라이언트에 어떤 백업 서버 정보도 보내지 않도록 지정합니다. 클라이언트는 자체 백업 서버 목록이 구성된 경우 이를 사용합니다.
server1 server 2.... server10	기본 ASA를 사용할 수 없을 때 VPN 클라이언트에서 사용할 서버의 목록을 제공합니다. 공백으로 구분되며 우선 순위에 따라 표시됩니다. IP 주소 또는 호스트 이름으로 서버를 식별합니다. 이 목록은 500자까지 가능하지만, 10개의 엔트리만 포함할 수 있습니다.

기본값

백업 서버가 존재하려면 클라이언트 또는 기본 ASA에서 구성해야 합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

실행 중인 컨피그레이션에서 백업 서버 특성을 제거하려면 이 명령의 **no** 형식을 인수 없이 사용합니다. 그러면 백업 서버에 대한 값을 다른 그룹 정책에서 상속할 수 있게 됩니다.

IPsec 백업 서버는 기본 ASA를 사용할 수 없을 때 VPN 클라이언트에서 중앙 사이트에 연결할 수 있게 합니다. 백업 서버를 구성하면 ASA는 IPsec 터널이 설정될 때 클라이언트에 서버 목록을 푸시합니다.

클라이언트에서 또는 기본 ASA에서 백업 서버를 구성합니다. ASA에서 백업 서버를 구성할 경우 그룹의 클라이언트에 백업 서버 정책을 푸시합니다. 이는 클라이언트의 백업 서버 목록(구성된 경우)을 대체합니다.

참고 호스트 이름을 사용하는 경우 백업 DNS 및 WINS 서버를 기본 DNS 및 WINS 서버와 다른 네트워크에 두는 것이 좋습니다. 그렇지 않으면 만약 하드웨어 클라이언트 사용자가 DHCP를 통해 하드웨어 클라이언트에서 DNS 및 WINS 정보를 얻는데 기본 서버와의 연결이 끊기고 백업 서버에 다른 DNS 및 WINS 정보가 있을 경우, 클라이언트는 DHCP 임대가 만료될 때까지 업데이트되지 않습니다. 게다가 호스트 이름을 사용하는 경우 DNS 서버가 사용할 수 없게 되면 상당한 지연이 발생할 수 있습니다.

예 다음 예에서는 "FirstGroup"이라는 그룹 정책에 대해 IP 주소가 10.10.10.1 및 192.168.10.14인 백업 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

ASDM, 세션, 로그인 또는 message-of-the-day 배너를 구성하려면 글로벌 컨피그레이션 모드에서 **banner** 명령을 사용합니다. 지정된 배너 키워드에서 모든 라인을 제거하려면(**exec**, **login**, **motd**) 이 명령의 **no** 형식을 사용합니다.

banner {**asdm** | **exec** | **login** | **motd** *text*}

[no] banner {**asdm** | **exec** | **login** | **motd** [*text*]}

구문 설명

asdm	ASDM에 성공적으로 로그인한 다음 배너를 표시하도록 시스템을 구성합니다. 사용자에게 로그인을 계속할지 아니면 연결을 끊을지 묻습니다. 이 옵션을 통해 사용자가 연결하기 전에 문서화된 정책 약관에 동의하게 할 수 있습니다.
exec	enable 프롬프트를 표시하기 전에 배너를 표시하도록 시스템을 구성합니다.
login	텔넷 또는 직렬 콘솔을 사용하여 ASA에 액세스할 때 비밀번호 로그인 프롬프트에 앞서 배너를 표시하도록 시스템을 구성합니다.
motd	처음 연결할 때 message-of-the-day 배너를 표시하도록 시스템을 구성합니다.
text	표시할 메시지 텍스트 행.

기본값

기본적으로 배너를 표시하지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(4)/8.0(3)	**asdm** 키워드를 추가했습니다.
9.0(1)	**banner login** 명령은 직렬 콘솔 연결을 지원합니다.

사용 지침

banner 명령은 지정된 키워드에 대해 표시할 배너를 구성합니다. *text* 문자열은 첫 번째 공백 다음부터 행 끝(캐리지 리턴 또는 라인 피드(LF))까지의 모든 문자입니다. 텍스트의 공백은 유지됩니다. 그러나 CLI를 통해 탭을 입력할 수는 없습니다.

먼저 배너를 지우지 않는 한 후속 *text* 엔트리는 기존 배너의 끝에 추가됩니다.

참고 토큰 $(domain) 및 $(hostname)은 ASA의 호스트 이름 및 도메인 이름으로 대체됩니다. 컨텍스트 컨피그레이션에서 $(system) 토큰을 입력하면 이 컨텍스트는 시스템 컨피그레이션에 구성된 배너를 사용합니다.

여러 행으로 된 배너는 추가하려는 행마다 새 배너 명령을 입력하는 방법으로 처리됩니다. 그러면 각 행이 기존 배너의 끝에 추가됩니다.

참고 배너의 권한 부여 프롬프트는 최대 235자 또는 31단어(두 한도 중 먼저 해당하는 것 적용)입니다.

텔넷 또는 SSH를 통해 ASA에 액세스할 때 배너 메시지를 처리하기에 충분한 시스템 메모리가 없거나 TCP 쓰기 오류가 발생하면 세션이 종료됩니다. **exec** 및 **motd** 배너만 SSH를 통한 ASA 액세스가 가능합니다. 로그인 배너는 최초 연결의 일부로 사용자 이름을 전달하지 않는 SSHv1 클라이언트 또는 SSH 클라이언트를 지원하지 않습니다.

배너를 대체하려면 새 행을 입력하기 전에 **no banner** 명령을 사용합니다.

지정된 배너 키워드의 모든 행을 제거하려면 **no banner** {**exec** | **login** | **motd**} 명령을 사용합니다.

no banner 명령은 텍스트 문자열을 선택적으로 삭제하지 않습니다. 즉 **no banner** 명령의 끝에 입력하는 어떤 *텍스트*도 무시됩니다.

예

다음 예에서는 **asdm**, **exec**, **login**, **motd** 배너를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# banner asdm You successfully logged in to ASDM
ciscoasa(config)# banner motd Think on These Things
ciscoasa(config)# banner exec Enter your password carefully
ciscoasa(config)# banner login Enter your password to log in
ciscoasa(config)# show running-config banner
asdm:
You successfully logged in to ASDM

exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

다음 예에서는 **motd** 배너에 2번째 행을 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# banner motd and Enjoy Today
ciscoasa(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

관련 명령

명령	설명
clear configure banner	모든 배너를 제거합니다.
show running-config banner	모든 배너를 표시합니다.

banner(group-policy)

원격 클라이언트가 연결할 때 배너 또는 시작 화면 텍스트를 표시하려면 그룹 정책 컨피그레이션 모드에서 **banner** 명령을 사용합니다. 배너를 삭제하려면 이 명령의 **no** 형식을 사용합니다.

banner {value *banner_string* **| none}**

no banner

참고 하나의 VPN 그룹 정책에서 여러 배너를 구성한 경우 그 배너 중 하나를 삭제하면 모든 배너가 삭제됩니다.

구문 설명

none	null 값의 배너를 설정합니다. 즉 배너를 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 배너를 상속할 수 없게 합니다.
value *banner_string*	배너 텍스트를 구성합니다. 문자열은 최대 500자입니다. 캐리지 리턴을 삽입하려면 "\n" 시퀀스를 사용합니다.

기본값

기본 배너가 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

배너를 상속할 수 없게 하려면 **banner none** 명령을 사용합니다.

IPsec VPN 클라이언트는 배너에 대해 전체 HTML을 지원합니다. 그러나 클라이언트리스 포털 및 AnyConnect 클라이언트는 부분 HTML을 지원합니다. 배너가 원격 사용자에게 올바르게 표시되게 하려면 다음 지침을 따르십시오.

- IPsec 클라이언트 사용자를 위해서는 /n 태그를 사용합니다.
- AnyConnect 클라이언트 사용자를 위해서는
 태그를 사용합니다.
- 클라이언트리스 사용자를 위해서는
 태그를 사용합니다.

예

다음 예에서는 "FirstGroup"이라는 그룹 정책을 위해 배너를 만드는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

bgp aggregate-timer

BGP 경로를 종합하는 간격을 설정하거나 타이머 기준 경로 종합을 비활성화하려면 주소군 컨피그레이션 모드에서 **bgp aggregate-timer** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

bgp aggregate-timer *seconds*

no bgp aggregate-timer

구문 설명

seconds	시스템에서 BGP 경로를 종합하는 간격(초). 유효한 값은 6초~60초 또는 0(제로)입니다. 기본값은 30입니다. 값이 0(제로)이면 타이머 기준 종합이 비활성화되고 즉시 종합을 시작합니다.

기본값

BGP 종합 타이머의 기본값은 30초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션, 주소군 IPv6 하위 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.
9.3(2)	주소군 IPv6 하위 모듈에서 이 명령을 지원하기 위해 수정했습니다.

사용 지침

BGP 경로가 종합되는 기본 간격을 변경하려면 이 명령을 사용합니다.

매우 규모가 큰 컨피그레이션에서는 **aggregate-address summary-only** 명령이 구성되었더라도 더 특정한 경로가 광고되었다가 나중에 취소되곤 합니다. 이러한 동작을 방지하려면 **bgp aggregate-timer**를 0(제로)으로 구성합니다. 그러면 즉시 종합 경로를 확인하며 구체적인 경로를 억제합니다.

예

다음 예에서는 20초 간격으로 BGP 경로 종합을 구성합니다.

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

다음 예에서는 즉시 BGP 경로 종합을 시작합니다.

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

관련 명령

명령	설명
address-family ipv4	표준 IP 버전 4(IPv4) 주소 접두사를 사용하여 라우팅 세션을 구성하기 위해 주소군 컨피그레이션 모드를 시작합니다.
aggregate-address	BGP(Border Gateway Protocol) 데이터베이스에서 종합 엔트리를 생성합니다.

bgp always-compare-med

서로 다른 자율 시스템의 네이버 경로에 대해 MED(Multi Exit Discriminator)를 비교할 수 있게 하려면 라우터 컨피그레이션 모드에서 **bgp always-compare-med** 명령을 사용합니다. 비교를 허용하지 않으려면 이 명령의 **no** 형식을 사용합니다.

bgp always-compare-med

no bgp always-compare-med

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령이 활성화되지 않았거나 이 명령의 **no** 형식이 입력되면 ASA 라우팅 소프트웨어는 서로 다른 자율 시스템의 네이버 경로에 대해 MED를 비교하지 않습니다.

비교 대상 경로의 자율 시스템 경로가 동일한 경우에만 MED를 비교합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

RFC 1771에 명시된 것처럼 MED는 선택적 비 전이적(non-transitive) 특성으로서 4옥텟으로 이루어진 음수가 아닌 정수입니다. 이 특성의 값은 BGP 최적 경로 선택 프로세스에서 인접 자율 시스템에 대한 여러 출구 지점을 구별하는 데 사용될 수 있습니다.

MED는 여러 대체 경로 중에서 최적 경로를 선택할 때 고려하는 매개변수 중 하나입니다. MED가 낮은 경로가 MED가 높은 경로보다 우선합니다. 최적 경로 선택 프로세스에서 MED 비교는 동일한 자율 시스템의 경로에 대해서만 수행합니다. 이 동작을 변경하려면 **bgp always-compare-med** 명령을 사용하는데, 이는 경로를 제공한 자율 시스템과 상관없이 모든 경로 간에 MED 비교를 수행합니다.

동일한 자율 시스템에서 받은 모든 경로를 대상으로 MED 값에 대한 결정론적 비교를 수행하도록 **bgp deterministic-med** 명령을 구성할 수 있습니다.

예

다음 예에서는 경로를 제공한 자율 시스템과 상관없이 대체 경로의 MED를 비교하도록 로컬 BGP 라우팅 프로세스를 구성합니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp always-compare-med
```

관련 명령

명령	설명
bgp deterministic-med	동일한 자율 시스템에서 받은 모든 경로를 대상으로 MED 값에 대한 결정론적 비교를 수행합니다.

bgp asnotation dot

BGP 4바이트 자율 시스템 번호의 기본 표시 및 정규식 매칭 형식을 asplain(십진수)에서 dot notation으로 변경하려면 라우터 컨피그레이션 모드에서 **bgp asnotation dot** 명령을 사용합니다. 기본 4바이트 자율 시스템 번호의 표시 및 정규식 매칭 형식을 asplain으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

bgp asnotation dot

no bgp asnotation dot

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

BGP 자율 시스템 번호는 화면 출력에서 asplain(십진수)을 사용하여 표시되며, 정규식에서 4바이트 자율 시스템 번호를 매칭하는 데 쓰이는 기본 형식도 asplain입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

2009년 1월 이전에는 회사에 할당되는 BGP 자율 시스템 번호가 1~65535 범위의 2옥텟 숫자였습니다(RFC 4271, *A Border Gateway Protocol 4 (BGP-4)* 참조).

자율 시스템 번호의 수요가 증가함에 따라 65536~4294967295의 범위에서 4옥텟의 자율 시스템 번호를 할당하기 위한 IANA(Internet Assigned Number Authority)가 2009년 1월에 출범합니다. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*에서는 자율 시스템 번호를 나타내는 3가지 방법을 제시합니다. Cisco는 다음 2가지 방법을 구현했습니다.

- Asplain—십진수 값 표기법으로서 2바이트 및 4바이트 자율 시스템 번호 모두 그 십진수 값으로 나타냅니다. 예를 들어, 65526은 2바이트 자율 시스템 번호이고, 234567은 4바이트 자율 시스템 번호입니다.
- Asdot—자율 시스템 점 표기법으로서 2바이트 자율 시스템 번호는 그 십진수 값으로, 4바이트 자율 시스템 번호는 점 표기법(dot notation)으로 나타냅니다. 예를 들어, 65526은 2바이트 자율 시스템 번호이고 1.169031(십진수 234567의 점 표기법)은 4바이트 자율 시스템 번호입니다.

Cisco가 구현한 4바이트 자율 시스템 번호에서는 asplain을 자율 시스템 번호의 기본 표시 형식으로 사용합니다. 그러나 asplain 및 asdot 형식 모두로 4바이트 자율 시스템 번호를 구성할 수 있습니다. 또한 정규식에서 4바이트 자율 시스템 번호를 매칭할 때 기본 형식도 asplain입니다. 따라서 4바이트 자율 시스템 번호를 매칭해야 하는 모든 정규식은 asplain 형식으로 작성해야 합니다. 기본 **show** 명령 출력을 변경하여 4바이트 자율 시스템 번호를 asdot 형식으로 표시하게 하려면 라우터 컨피그레이션 모드에서 **bgp asnotation dot** 명령을 사용합니다. asdot 형식이 기본 설정으로 활성화되면 4바이트 자율 시스템 번호와 일치하는 모든 정규식은 asdot 형식으로 작성해야 합니다. 그렇지 않으면 정규식 매칭에서 실패합니다. 아래의 표는 4바이트 자율 시스템 번호를 asplain 또는 asdot 형식으로 구성할 수 있더라도 **show** 명령의 출력을 표시하고 정규식을 위해 4바이트 자율 시스템 번호 매칭을 제어하는 데 하나의 형식만 사용되며 기본 형식은 asplain임을 보여줍니다.

show 명령 출력에서 4바이트 자율 시스템 번호를 표시하고 정규식의 매칭을 제어하는 데 asdot 형식을 사용하려면 **bgp asnotation dot** 명령을 구성해야 합니다. **bgp asnotation dot** 명령을 활성화한 다음에는 **clearbgp *** 명령을 입력하여 모든 BGP 세션에 대해 하드 초기화를 시작해야 합니다.

표 4-1 기본 Asplain 4 바이트 자율 시스템 번호 형식

형식	컨피그레이션 형식	Show 명령 출력 및 정규식 매칭 형식
asplain	2-byte: 1 to 6553 4-byte: 65536 to 4294967295	2-byte: 1 to 6553 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 6553 4-byte: 1.0 to 65535.65535	2-byte: 1 to 6553 4-byte: 65536 to 4294967295

표 4-2 Asdot 4 바이트 자율 시스템 번호 형식

형식	컨피그레이션 형식	Show 명령 출력 및 정규식 매칭 형식
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

예

다음 **show bgp summary** 명령의 출력에서는 4바이트 자율 시스템 번호를 기본 asplain 형식으로 보여줍니다. asplain 형식의 4바이트 자율 시스템 번호 65536과 65550입니다.

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04       0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15       0
```

기본 출력 형식을 asdot 표기법 형식으로 바꾸기 위해 다음 컨피그레이션을 수행합니다.

```
ciscoasa# configure terminal
ciscoasa(config)# router bgp 65538
ciscoasa(config-router)# bgp asnotation dot
```

컨피그레이션을 수행하면 다음 **show bgp summary** 명령의 출력처럼 asdot 표기법 형식으로 변환됩니다. asdot 형식의 4바이트 자율 시스템 번호 1.0과 1.14입니다. 이는 자율 시스템 번호 65536과 65550을 asdot으로 변환한 것입니다.

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13     0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24     0
```

bgp asnotation dot 명령이 구성되면 4바이트 자율 시스템 경로의 정규식 매칭 형식이 asdot 표기법 형식으로 바뀝니다. 정규식에서 asplain 형식 또는 asdot 형식 중 하나로 4바이트 자율 시스템 번호를 구성할 수 있으나, 현재 기본 형식으로 구성된 4바이트 자율 시스템 번호만 매칭됩니다. 첫 번째 예에서는 **show bgp regexp** 명령이 asplain 형식의 4바이트 자율 시스템 번호로 구성됩니다. 현재 기본 형식이 asdot 형식이므로 이 매칭은 실패하고 아무 것도 출력되지 않습니다. asdot 형식을 사용하는 두 번째 예에서는 매칭이 전달되고 4바이트 자율 시스템 경로에 대한 정보가 asdot 표기법을 사용하여 표시됩니다.

```
ciscoasa(config-router)# show bgp regexp ^65536$
ciscoasa(config-router)# show bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

참고 asdot 표기법에서는 마침표를 사용하는데, 이는 Cisco 정규식에서 특수 문자입니다. 이 특수한 의미를 없애려면 마침표 앞에 백슬래시를 넣습니다.

관련 명령

명령	설명
show bgp summary	모든 BGP 연결의 상태를 표시합니다.
show bgp regexp	자율 시스템 경로 정규식과 매칭하는 경로를 표시합니다.

bgp bestpath compare-routerid

최적 경로 선택 프로세스에서 서로 다른 외부 피어로부터 받은 동일한 경로를 비교하고 라우터 ID가 가장 낮은 경로를 최적 경로로 선택하도록 BGP 라우팅 프로세스를 구성하려면 라우터 컨피그레이션 모드에서 **bgp bestpath compare-routerid** 명령을 사용합니다.

BGP 라우팅 프로세스를 기본 작동으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령의 동작은 기본적으로 비활성화됩니다. BGP는 동일한 특성의 두 경로를 받으면 먼저 받은 것을 선택합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

bgp bestpath compare-routerid 명령은 서로 다른 두 피어로부터 동일한 두 경로(라우터 ID를 제외하고 모든 특성이 동일)를 받았고 그중 최적 경로를 선택할 때 라우터 ID를 기준으로 삼게끔 BGP 라우팅 프로세스를 구성하는 데 사용합니다. 이 명령이 활성화된 경우, 다른 모든 특성이 동일하다면 라우터 ID가 가장 낮은 것이 최적 경로로 선택됩니다.

예

다음 예에서는 서로 다른 피어에서 동일한 경로를 받았고 그중에서 최적 경로를 선택할 때 라우터 ID를 결정 기준으로 삼아 비교하도록 BGP 라우팅 프로세스를 구성합니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath compare-routerid
```

bgp bestpath med missing-as-worst

MED 특성이 없는 경로에 무한대 값을 부여하도록, 즉 MED 값이 없는 경로를 가장 나쁜 경로로 만들도록 BGP 라우팅 프로세스를 구성하려면 라우터 컨피그레이션 모드에서 **bgp bestpath med missing-as-worst** 명령을 사용합니다. 라우터를 기본 동작으로 되돌리려면(누락된 MED에 값 0 지정) 이 명령의 **no** 형식을 사용합니다.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

ASA 소프트웨어는 MED 특성이 없는 경로에 값 0을 지정합니다. 즉 MED 특성이 없는 경로가 최적 경로로 간주됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 MED 특성이 없는 경로에 무한대(4294967294)의 값을 부여하여 가장 나쁜 경로로 간주하도록 BGP 라우터 프로세스를 구성합니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath med missing-as-worst
```

bgp default local-preference

기본 로컬 선호 값을 변경하려면 라우터 컨피그레이션 모드에서 **bgp default local-preference** 명령을 사용합니다. 로컬 선호 값을 기본 설정으로 되돌리려면 **no** 형식을 사용합니다.

bgp default local-preference *number*

no bgp default local-preference *number*

구문 설명

number	로컬 선호 값(0~4294967295)

기본값

이 명령이 활성화되지 않거나 이 명령의 **no** 형식이 입력되면 ASA 소프트웨어를 로컬 선호 값으로 100을 적용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

로컬 선호 특성은 BGP 최적 경로 선택 프로세스에서 경로에 선호도를 적용하는 데 쓰이는 임의의 특성입니다. 이 특성은 iBGP 피어끼리만 교환하며 로컬 정책을 결정하는 데 사용됩니다. 로컬 선호가 가장 높은 경로가 우선시됩니다.

예

다음 예에서는 로컬 선호의 값이 200으로 설정됩니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp default local-preference 200
```

bgp deterministic-med

동일한 자율 시스템 내에서 받은 모든 경로를 대상으로 MED 값에 대한 결정론적 비교를 수행하게 하려면 라우터 컨피그레이션 모드에서 **bgp deterministic-med** 명령을 사용합니다. 필수 MED 비교를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

bgp deterministic-med

no bgp deterministic-med

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

ASA 소프트웨어는 동일한 자율 시스템에서 받은 모든 경로를 대상으로 MED 변수에 대한 결정론적 비교를 수행하지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

bgp always-compare-med 명령은 서로 다른 자율 시스템의 네이버 경로에 대한 MED 비교를 활성화하는 데 사용합니다. **bgp always-compare-med** 명령이 구성되면, 서로 다른 네이버(동일한 자율 시스템에 있음)에서 받은, 동일한 접두사의 경로는 모두 함께 그룹화하고 MED 값의 오름차순으로 정렬합니다. 수신 전용 경로는 무시되어 그룹화 또는 정렬되지 않습니다.

그런 다음 최적 경로 선택 알고리즘은 기존 규칙을 사용하여 최적 경로를 선택합니다. 네이버 자율 시스템별로, 그 다음에는 전역에서 비교를 수행합니다. 이 명령이 입력되면 즉시 경로의 그룹화 및 정렬이 수행됩니다. 정확한 결과를 얻으려면 로컬 자율 시스템의 모든 경로에서 이 명령이 활성화되거나 비활성화되어야 합니다.

예

다음 예에서는 하나의 연합 내에서 동일한 하위 자율 시스템에 의해 광고된 경로를 대상으로 한 경로 선택 과정에서 MED를 비교하도록 BGP를 구성합니다.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp deterministic-med
```

다음 예는 **show bgp** 명령의 출력으로서 **bgp deterministic-med** 명령의 컨피그레이션이 경로 선택에 어떤 영향을 주는지 보여줍니다. **bgp deterministic-med** 명령을 활성화하지 않으면 경로를 수신한 순서가 최적 경로 선택 방식에 영향을 미칩니다. 다음 **show bgp** 명령의 샘플 출력에서는 동일한 접두사(10.100.0.0)로 받은 3개의 경로를 보여주며, **bgp deterministic-med** 명령은 활성화되지 않았습니다.

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external, best
```

bgp deterministic-med 기능이 라우터에서 활성화되지 않으면 경로 선택은 경로가 수신된 순서의 영향을 받을 수 있습니다. 라우터가 동일한 접두사로 3개의 경로를 받는 다음 시나리오를 살펴보십시오.

clear bgp * 명령을 입력하여 로컬 라우팅 테이블의 모든 경로를 지웁니다.

```
ciscoasa(router)# clear bgp *
```

라우팅 테이블이 다시 채워지면 **show bgp** 명령을 한 번 더 실행합니다. BGP 세션을 지운 다음 경로의 순서가 변경되었습니다. 선택 알고리즘의 결과도 바뀌었습니다. 두 번째 세션에서는 경로를 수신한 순서가 달라졌기 때문입니다.

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal, best
```

bgp deterministic-med 명령이 활성화된 경우에는 선택 알고리즘의 결과가 항상 같습니다. 로컬 라우터에서 경로를 수신하는 순서와 상관없습니다. 이 시나리오에서 로컬 라우터에 **bgp deterministic-med** 명령을 입력하면 항상 다음과 같이 출력됩니다.

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 15
Paths: (3 available, best #1, advertised over EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal, best 3
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
```

관련 명령

명령	설명
bgp always compare-med	서로 다른 자율 시스템의 네이버 경로에 대해 MED를 비교하게 합니다.
clear bgp	하드 또는 소프트 리컨피그레이션을 사용하여 BGP 연결을 재설정합니다.
show bgp	BGP 라우팅 테이블의 엔트리를 표시합니다.

bgp enforce-first-as

수신한 업데이트에서 AS_PATH의 시작에 자율 시스템 번호를 표시하지 않는 eBGP(외부 BGP) 피어로부터의 업데이트를 거부하도록 ASA를 구성하려면 라우터 컨피그레이션 모드에서 **bgp enforce-first-as** 명령을 사용합니다. 이 동작을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

bgp enforce-first-as

no bgp enforce-first-as

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령의 동작은 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

bgp enforce-first-as 명령은 AS_PATH 특성의 첫 세그먼트에 자율 시스템 번호를 표시하지 않는 eBGP 피어로부터 받은 업데이트를 거부하는 데 사용합니다. 이 명령을 활성화하면 잘못 구성되었거나 허가받지 않은 피어가 다른 자율 시스템에서 보낸 경로처럼 광고함으로써 트래픽을 잘못된 방향으로 전달하는, 즉 로컬 라우터를 스푸핑하는 것을 막을 수 있습니다.

예

다음 예에서는 eBGP 피어에서 보낸 모든 업데이트를 검사하여 AS_PATH의 첫 자율 시스템 번호가 전송하는 피어의 로컬 AS 번호임을 확인합니다. 다음 예에서는 10.100.0.1 피어의 첫 AS 번호가 65001이 아니면 여기서 보낸 업데이트가 폐기됩니다.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp enforce-first-as
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.100.0.1 remote-as 65001
```

관련 명령

명령	설명
address-family ipv4	주소군 컨피그레이션 모드를 시작합니다.
neighbor remote-as	BGP 또는 다중 프로토콜 BGP 라우팅 테이블에 엔트리를 추가합니다.

bgp fast-external-fallover

피어에 연결하는 데 사용된 링크가 다운되면 즉시 외부 BGP 피어링 세션을 재설정하도록 BGP 라우팅 프로세스를 구성하려면 라우터 컨피그레이션 모드에서 **bgp fast-external-fallover** 명령을 사용합니다. BGP 빠른 외부 장애 조치를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

bgp fast-external-fallover

no bgp fast-external-fallover

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

BGP 빠른 외부 장애 조치는 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

bgp fast-external-fallover 명령은 직접 연결된 외부 피어와의 BGP 피어링 세션에 대해 빠른 외부 장애 조치를 비활성화하거나 활성화하는 데 사용합니다. 링크가 다운되면 즉시 세션이 재설정됩니다. 직접 연결된 피어링 세션만 지원됩니다. BGP 빠른 외부 페일오버가 비활성화될 경우, BGP 라우팅 프로세스는 기본 대기 타이머(keepalive 3개)가 만료될 때까지 기다렸다가 피어링 세션을 재설정합니다. BGP 빠른 외부 페일오버는 인터페이스별로 구성할 수도 있습니다. 인터페이스 컨피그레이션 명령인 **ip bgp fast-external-fallover**를 사용하면 됩니다.

예

다음 예에서는 BGP 빠른 외부 장애 조치 기능이 비활성화됩니다. 이 세션이 지나는 링크가 플랩하면 연결은 재설정되지 않습니다.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# no bgp fast-external-fallover
```

관련 명령

명령	설명
ip bgp fast-external-fallover	인터페이스별로 빠른 외부 장애 조치를 구성합니다.

bgp inject-map

BGP 라우팅 테이블에 더 특정한 경로를 추가하기 위해 조건부 경로 삽입을 구성하려면 주소군 컨피그레이션 모드에서 **bgp inject-map** 명령을 사용합니다. 조건부 경로 삽입 컨피그레이션을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

no bgp inject-map *inject-map* **exist-map** *exist-map*

구문 설명

inject-map	로컬 BGP 라우팅 테이블에 삽입할 접두사를 지정하는 경로 맵의 이름.
exist-map *exist-map*	BGP 스피커가 추적하는 접두사를 포함하는 경로 지도의 이름.
copy-attributes	(선택 사항) 삽입된 경로가 종합 경로의 특성을 상속받도록 구성합니다.

기본값

어떤 특정 경로도 BGP 라우팅 테이블에 삽입되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션, 주소군 IPv6 하위 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.
9.3(2)	주소군 IPv6 하위 모듈에서 이 명령을 지원하기 위해 수정했습니다.

사용 지침

bgp inject-map 명령은 조건부 경로 삽입을 구성하는 데 사용합니다. 조건부 경로 삽입을 통해 더 특정한 접두사를 매칭 없이 BGP 라우팅 테이블에 넣을 수 있습니다. 2가지 경로 맵(*exist-map*, *inject-map*)이 글로벌 컨피그레이션 모드에서 구성된 다음 주소군 컨피그레이션 모드에서 **bgp inject-map** 명령을 통해 지정됩니다.

exist-map 인수에서는 BGP 스피커가 추적할 접두사를 정의하는 경로 맵을 지정합니다. 이 경로 맵은 종합 접두사를 지정하는 **match ip address prefix-list** 명령문과 경로 소스를 지정하는 **match ip route-source prefix-list** 명령문을 포함해야 합니다.

inject-map 인수에서 정의하는 접두사는 생성되어 라우팅 테이블에 설치됩니다. 삽입된 접두사는 로컬 BGP RIB에 설치됩니다. 유효한 상위 경로가 있어야 합니다. 종합 경로(기존 접두사)와 같거나 더 특정한 접두사만 삽입할 수 있습니다.

선태 사항인 **copy-attributes** 키워드는 삽입된 접두사가 종합 경로와 동일한 특성을 상속하도록 선택적으로 구성하는 데 사용합니다. 이 키워드를 입력하지 않으면 삽입된 접두사는 로컬에서 시작한 경로의 기본 특성을 사용합니다.

예

다음 예에서는 조건부 경로 삽입이 구성됩니다. 삽입된 접두사는 종합(상위) 경로의 특성을 상속합니다.

```
ciscoasa(config)# ip prefix-list ROUTE permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
ciscoasa(config)# route-map LEARNED_PATH permit 10
ciscoasa(config-route-map)# match ip address prefix-list ROUTE
ciscoasa(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
ciscoasa(config-route-map)# exit
ciscoasa(config)# route-map ORIGINATE permit 10
ciscoasa(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
ciscoasa(config-route-map)# set community 14616:555 additive
ciscoasa(config-route-map)# exit
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH
copy-attributes
```

관련 명령

명령	설명
ip prefix-list	접두사 목록을 생성하거나 접두사 목록 엔트리를 추가합니다.
set community	BGP 커뮤니티 특성을 설정합니다.
address-family ipv4	주소군 컨피그레이션 모드를 시작합니다.

bgp log-neighbor-changes

BGP 네이버 재설정의 로깅을 활성화하려면 라우터 컨피그레이션 모드에서 **bgp log-neighbor-changes** 명령을 사용합니다. BGP 네이버 인접성의 변경 사항 로깅을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

bgp log-neighbor-changes

no bgp log-neighbor-changes

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

BGP 네이버 로깅이 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

bgp log-neighbor-changes 명령은 BGP 네이버 상태(up 또는 down) 변경의 로깅을 활성화하고 네트워크 연결 문제 해결 및 네트워크 안정성 측정을 위해 재설정합니다. 예기치 않게 네이버가 재설정되면 네트워크의 오류율이 높거나 패킷 손실이 크다는 징후일 수 있으므로 조사해야 합니다.

bgp log-neighbor-changes 명령을 사용하여 상태 변경 메시지 로깅을 활성화하더라도 성능에 큰 영향을 주지 않습니다. 이를테면 BGP별 업데이트 디버깅을 활성화하는 것과는 다릅니다.

bgp log-neighbor-changes 명령이 활성화되지 않으면 네이버 상태 변경 메시지는 추적되지 않습니다. 단, 재설정의 경우 항상 **show bgp neighbors** 명령의 출력에 나타납니다.

eigrp log-neighbor-changes 명령은 EIGRP(Enhanced Interior Gateway Routing Protocol) 네이버 인접성의 로깅을 활성화하지만, BGP 네이버에 대한 메시지는 **bgp log-neighbor-changes** 명령으로 활성화된 경우에만 로깅됩니다.

BGP 네이버 변경 사항의 로그를 표시하려면 **show logging** 명령을 사용합니다.

예

다음 예에서는 라우터 컨피그레이션 모드에서 BGP 네이버 변경 사항을 로깅합니다.

```
ciscoasa(config)# bgp router 40000
ciscoasa(config-router)# bgp log-neighbor-changes
```

관련 명령

명령	설명
show BGP neighbors	네이버와의 BGP 연결에 대한 정보를 표시합니다.

bgp maxas-limit

AS-path의 자율 시스템 번호가 지정된 값을 초과하는 경로는 폐기하도록 BGP를 구성하려면 라우터 컨피그레이션 모드에서 **bgp maxas-limit** 명령을 사용합니다. 라우터를 기본 작동으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

bgp max-as limit *number*

no bgp max-as limit

구문 설명

number	BGP 업데이트 메시지의 AS-path 특성에 있는 자율 시스템 번호의 최대 개수. 범위는 1~254입니다. 이 명령은 AS-path 세그먼트에 있는 자율 시스템 번호의 개수를 제한할 뿐 아니라 AS-path 세그먼트의 수도 10개로 제한합니다. 10개의 AS-path 세그먼트를 허용하는 동작이 **bgp maxas-limit** 명령에 구현되어 있습니다.

기본값

삭제되는 경로는 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

bgp maxas-limit 명령은 인바운드 경로에서 허용되는, AS-path 특성에 있는 자율 시스템 번호의 개수를 제한하는 데 사용합니다. AS-path 세그먼트가 구성된 한도를 초과하는 경로가 수신되면 BGP 라우팅 프로세스는 그 경로를 폐기합니다.

예

다음 예에서는 AS-path 특성에 있는 자율 시스템 번호의 최대 개수를 30으로 설정합니다.

```
ciscoasa(config)# router bgp 4000
ciscoasa(config)# bgp maxas-limit 30
```

bgp nexthop

BGP next-hop 주소 추적을 구성하려면 주소군 또는 라우터 컨피그레이션 모드에서 **bgp nexthop** 명령을 사용합니다. BGP next-hop 주소 추적을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

no bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

구문 설명

trigger	BGP next-hop 주소 추적 사용을 지정합니다. 이 키워드를 **delay** 키워드와 함께 사용하여 next-hop 추적 지연을 변경합니다. 이 키워드를 **enable** 키워드와 함께 사용하여 next-hop 주소 추적을 활성화합니다.
delay	라우팅 테이블에 설치된 next-hop 경로의 업데이트를 확인할 때 그 대기 간격을 변경합니다.
seconds	그 대기 시간(초)을 지정합니다. 유효한 값은 0~100입니다. 기본값은 5입니다.
enable	BGP next-hop 주소 추적을 활성화합니다.
route-map	라우팅 테이블에서 BGP 접두사의 next-hop 경로에 적용되는 경로 맵을 사용하게 합니다.
map-name	경로 맵의 이름.

기본값

BGP next-hop 주소 추적은 IPv4에서 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션 주소군 IPv6 하위 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.
9.3(2)	주소군 IPv6 하위 모듈에서 이 명령을 지원하기 위해 수정했습니다.

사용 지침

BGP next-hop 주소 추적은 이벤트 기반입니다. 피어링 세션이 설정되면 BGP 접두사가 자동으로 추적됩니다. Next-hop 변경 사항은 RIB(routing information base)에서 업데이트되는 대로 신속하게 BGP에 보고됩니다. 이러한 최적화를 통해 RIB에 설치된 경로의 next-hop 변경에 대한 응답 시간을 단축함으로써 전반적인 BGP 컨버전스가 향상됩니다. BGP 검사 주기의 사이에 최적 경로 계산이 실행될 경우 변경 사항만 처리되고 추적됩니다.

참고

- BGP next-hop 주소 추적으로 BGP 응답 시간이 크게 향상됩니다. 그러나 불안정한 IGP(Interior Gateway Protocol) 피어로 인해 BGP가 불안정해질 수 있습니다. BGP에 미칠 영향을 줄이기 위해 불안정한 IGP 피어링 세션을 강력하게 억제하는 것이 좋습니다.
- BGP next-hop 주소 추적은 IPv6 주소군에서 지원되지 않습니다.

BGP next-hop 주소 추적에서 라우팅 테이블 검사의 대기 간격을 변경하려면 **trigger** 키워드를 **delay** 키워드 및 *seconds* 인수와 함께 사용합니다. 전체 라우팅 테이블 검사의 대기 간격을 IGP 튜닝 매개변수와 같게 함으로써 BGP next-hop 주소 추적의 성능을 높일 수 있습니다. 기본 대기 간격은 5초이며, 이는 고속 튜닝된 IGP에 적합한 값입니다. 컨버전스 속도가 더 느린 IGP의 경우, 그 컨버전스 시간에 따라 대기 간격을 20초 이상으로 바꿀 수 있습니다.

BGP next-hop 주소 추적을 활성화하려면 **trigger** 키워드를 **enable** 키워드와 함께 사용합니다. BGP next-hop 주소 추적은 기본적으로 활성화됩니다.

경로 맵을 사용할 수 있게 하려면 **route-map** 키워드를 *map-name* 인수와 함께 사용합니다. 경로 맵은 BGP 최적 경로 계산 과정에서 사용되며, BGP 접두사의 Next_Hop 특성에 해당하는 라우팅 테이블의 경로에 적용됩니다. next-hop 경로가 경로 맵 평가에서 실패할 경우 이 next-hop 경로는 연결 불가로 표시됩니다. 이 명령은 주소군별로 실행합니다. 따라서 서로 다른 주소군의 next-hop 경로에 각기 다른 경로 맵을 적용할 수 있습니다.

참고 **match ip address** 명령만 경로 맵에서 지원됩니다. **set** 명령이나 기타 **match** 명령은 지원되지 않습니다.

예

다음 예에서는 라우팅 테이블 검사의 대기 간격을 변경하여 IPv4 주소군 세션에서 BGP next-hop 주소 추적이 20초마다 실시되게 하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop trigger delay 20
```

다음 예에서는 IPv4 주소군에서 next-hop 주소 추적을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# no bgp nexthop trigger enable
```

다음 예에서는 주소 마스크 길이가 25를 초과할 때만 next-hop 경로로 간주하게 하는 경로 맵을 구성하는 방법을 보여줍니다. 이 컨피그레이션으로 접두사의 집합이 next-hop 경로로 간주되는 것을 방지합니다.

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP
ciscoasa(config-router-af)# exit-address-family
ciscoasa(config-router)# exit
ciscoasa(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
ciscoasa(config)# route-map CHECK-NEXTHOP permit 10
ciscoasa(config)# match ip address prefix-list FILTER25
```

bgp redistribute-internal

EIGRP, OSPF와 같은 IGP(interior gateway protocol)에 iBGP 재배포를 구성하려면 주소군 컨피그레이션 모드에서 **bgp redistribute-internal** 명령을 사용합니다. 라우터를 기본 동작으로 되돌리거나 IGP에 대한 iBGP 재배포를 중지하려면 이 명령의 **no** 형식을 사용합니다.

bgp redistribute-internal

no bgp redistribute-internal

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

IBGP 경로가 IGP에 재배포됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션 주소군 IPv6 하위 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.
9.3(2)	주소군 IPv6 하위 모듈에서 이 명령을 지원하기 위해 수정했습니다.

사용 지침

bgp redistribute-internal 명령은 IGP에 대한 iBGP 재배포를 구성하는 데 사용합니다. 이 명령을 구성한 다음 BGP 연결을 재설정하기 위해 **clear bgp** 명령을 입력해야 합니다.

임의의 IGP에 BGP를 재배포할 때 IP 접두사 목록 및 경로 맵 구문을 사용하여 재배포되는 접두사의 수를 제한해야 합니다.

주의 IGP에 iBGP를 재배포할 때 각별히 주의해야 합니다. 재배포되는 접두사의 수를 제한하기 위해 IP 접두사 목록 및 경로 맵 구문을 사용합니다. 필터링되지 않은 BGP 라우팅 테이블을 IGP에 재배포하면 정상적인 IGP 네트워크 작업에 지장을 줄 수 있습니다.

예

다음 예에서는 OSPF 경로에 대한 BGP 재배포가 활성화됩니다.

```
ciscoasa(config)# router ospf 300
ciscoasa(config-router)# redistribute bgp 200
ciscoasa(config-router)# exit
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp redistribute-internal
```

bgp router-id

로컬 BGP 라우팅 프로세스를 위해 고정 라우터 ID를 구성하려면 주소군 라우터 컨피그레이션 모드에서 **bgp router-id** 명령을 사용합니다. 실행 중인 컨피그레이션 파일에서 고정 라우터 ID를 제거하고 기본 라우터 ID 선택을 복원하려면 이 명령의 **no** 형식을 사용합니다.

bgp router-id *ip-address*

no bgp router-id

구문 설명

ip-address	IP 주소 형식의 라우터 식별자

기본값

이 명령이 활성화되지 않으면 라우터 ID는 물리적 인터페이스의 최상위 IP 주소로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.
9.3(2)	이 명령을 수정했습니다.

사용 지침

bgp router-id 명령은 로컬 BGP 라우팅 프로세스를 위해 고정 라우터 ID를 구성하는 데 사용합니다. 이 라우터 ID는 IP 주소의 형식으로 입력합니다. 라우터에서 로컬 구성되지 않은 것을 비롯하여 어떤 유효한 IP 주소도 사용할 수 있습니다. 라우터 ID가 바뀌면 피어링 세션은 자동으로 재설정됩니다. 각 컨텍스트에 별도의 라우터 ID를 사용할 수도 있습니다.

예

다음 예에서는 고정 BGP 라우터 ID 192.168.254.254로 로컬 라우터를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

bgp scan-time

next-hop 검증을 위해 BGP 라우터의 검사 간격을 구성하려면 주소군 컨피그레이션 모드에서 **bgp scan-time** 명령을 사용합니다. 라우터의 검사 간격을 기본 간격인 60초로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

bgp scan-time *scanner-interval*

no bgp scan-time *scanner-interval*

구문 설명

scanner-interval	BGP 라우팅 정보의 검사 간격. 유효한 값의 범위는 15초~60초입니다. 기본값은 60초입니다.

기본값

기본 검사 간격은 60초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령의 **no** 형식을 입력하더라도 검사가 비활성화되지 않습니다. 다만 **show running-config** 명령의 출력에서 제거됩니다.

주소군에 대해 **bgp nexthop** 주소 추적(NHT)이 활성화된 경우 **bgp scan-time** 명령은 해당 주소군에서 허용되지 않으며 기본값인 60초로 유지됩니다. 라우터 모드 또는 주소군 모드에서 **bgp scan-time** 명령을 실행하려면 먼저 NHT를 비활성화해야 합니다.

예

다음 라우터 컨피그레이션의 예에서는 BGP 라우팅 테이블을 위한 IPv4 유니캐스트 경로의 next-hop 검증 검사 간격이 20초로 설정됩니다.

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp scan-time 20
```

관련 명령

명령	설명
show running-config	현재 ASA에 나타난 컨피그레이션을 표시합니다.
bgp nexthop	BGP next-hop 주소 추적을 구성합니다.

bgp suppress-inactive

RIB에 설치되지 않은 경로의 광고를 억제하려면 주소군 또는 라우터 컨피그레이션 모드에서 **bgp suppress-inactive** 명령을 사용합니다.

bgp suppress-inactive

no bgp suppress-inactive

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

어떤 경로도 억제되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션, 주소군 IPv6 하위 모드	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.
9.3(2)	주소군 IPv6 하위 모듈에서 이 명령을 지원하기 위해 수정했습니다.

사용 지침

bgp suppress-inactive 명령은 RIB에 설치되지 않은 경로(비활성 경로)가 피어에 광고되는 것을 막는 데 사용합니다. 이 기능이 활성화되지 않거나 이 명령의 **no** 형식이 사용될 경우 BGP는 비활성 경로를 광고합니다.

참고 BGP는 RIB에 설치되지 않은 경로에 RIB-failure 플래그를 표시합니다. 이 플래그는 **show bgp** 명령의 출력에도 나타납니다. 이를테면 Rib-Failure (17)이라고 표시됩니다. 이 플래그는 해당 경로나 RIB에 오류나 문제가 있음을 의미하지 않습니다. 그리고 이 명령의 컨피그레이션에 따라 경로는 계속 광고될 수 있습니다. 비활성 경로에 대한 추가 정보를 보려면 **show bgp rib-failure** 명령을 입력합니다.

예

다음 예에서는 RIB에 설치되지 않은 경로는 광고하지 않도록 BGP 라우팅 프로세스를 구성합니다.

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp suppress-inactive
```

관련 명령

명령	설명
show bgp	BGP 라우팅 테이블의 엔트리를 표시합니다.
show bgp rib-failure	RIB(Routing Information Base) 테이블에서 설치에 실패한 BGP 경로를 표시합니다.

bgp transport

전역에서 모든 BGP 세션을 위해 TCP 전송 세션 매개변수를 활성화하려면 라우터 컨피그레이션 모드에서 **bgp transport** 명령을 사용합니다. 전역에서 모든 BGP 세션을 위해 TCP 전송 세션 매개변수를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

bgp transport path-mtu-discovery

no bgp transport path-mtu-discovery

구문 설명

path-mtu-discovery	전송 경로 MTU(maximum transmission unit) 검색을 활성화합니다.

기본값

TCP 경로 MTU 검색은 모든 BGP 세션에서 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 기본적으로 활성화됩니다. 그러면 BGP 세션에서 더 큰 MTU 링크를 활용할 수 있기 때문이며, 이는 iBGP(internal BGP) 세션에서 매우 중요할 수 있습니다. TCP 경로 MTU 검색이 반드시 활성화되게 하려면 **show bgp neighbors** 명령을 사용합니다.

예

다음 예에서는 모든 BGP 세션에 대해 TCP 경로 MTP 검색을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# router bgp 4500
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

다음 예에서는 모든 BGP 세션에 대해 TCP 경로 MTP 검색을 활성화하는 방법을 보여줍니다.

```
iscoasa(config)# router bgp 4500
ciscoasa(config-router)# bgp transport path-mtu-discovery
```

관련 명령

명령	설명
show bgp neighbors	네이버와의 BGP 연결에 대한 정보를 표시합니다.

bgp-community new format

AA:NN(자율 시스템:커뮤니티 번호/4바이트 번호)의 형식으로 커뮤니티를 표시하도록 BGP를 구성하려면 글로벌 컨피그레이션 모드에서 **bgp-community new-format** 명령을 사용합니다. 커뮤니티를 32비트 숫자로 표시하도록 BGP를 구성하려면 이 명령의 **no** 형식을 사용합니다.

bgp-community new-format

no bgp-community new-format

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

BGP 커뮤니티는(AA:NN 형식으로 입력될 때도) 이 명령이 활성화되지 않거나 **no** 형식이 활성화되면 32비트 숫자로 표시됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

bgp-community new-format 명령은 RFC-1997의 AA:NN 형식으로 BGP 커뮤니티를 표시하도록 로컬 라우터를 구성하는 데 사용합니다.

이 명령은 BGP 커뮤니티가 표시되는 형식에만 적용됩니다. 커뮤니티 또는 커뮤니티 교환에는 영향을 주지 않습니다. 그러나 로컬 구성된 정규식과 매칭하는 확장된 IP 커뮤니티 목록은 32비트 숫자가 아닌 AA:NN 형식에서 매칭하도록 업데이트해야 합니다.

RFC 1997, *BGP 커뮤니티 특성*에 따르면, BGP 커뮤니티는 최대 2개 파트로 구성되며 각 파트의 길이는 2바이트입니다. 첫 파트는 자율 시스템 번호, 두 번째 파트는 네트워크 운영자가 정의한 2바이트 번호입니다.

예

다음 예에서는 32비트 숫자의 커뮤니티 형식을 사용하는 라우터가 AA:NN 형식을 사용하도록 업그레이드됩니다.

```
ciscoasa(config)# bgp-community new-format
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

다음 샘플 출력은 **bgp-community new-format** 명령이 활성화되었을 때 BGP 커뮤니티 번호가 어떻게 표시되는지 보여줍니다.

```
ciscoasa(router)# show bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
Advertised to non peer-group peers:
10.0.33.35
35
10.0.33.35 from 10.0.33.35 (192.168.3.3)
Origin incomplete, metric 10, localpref 100, valid, external
Community: 1:1
Local
0.0.0.0 from 0.0.0.0 (10.0.33.34)
Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

blocks

(**show blocks** 명령으로 표시되는) 블록 진단에 추가 메모리를 할당하려면 특별 권한 EXEC 모드에서 **blocks** 명령을 사용합니다. 이 값을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

blocks queue history enable [*memory_size***]**

no blocks queue history enable [*memory_size***]**

구문 설명

*memory_size*s	(선택 사항) 블록 진단용 메모리 크기에 동적 값을 적용하지 않고 바이트 단위로 설정합니다. 이 값이 사용 가능 메모리보다 클 경우 오류 메시지가 나타나며 값이 적용되지 않습니다. 이 값이 사용 가능 메모리의 50% 보다 클 경우 경고 메시지가 나타나지만 값은 적용됩니다.

기본값

블록 진단 추적에 할당되는 기본 메모리는 2136바이트입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

현재 할당된 메모리를 보려면 **show blocks queue history** 명령을 입력합니다.

ASA를 다시 로드할 경우 메모리 할당이 기본 설정으로 돌아갑니다.

할당되는 메모리의 양은 최대 150KB이지만, 사용 가능 메모리의 50%를 초과할 수 없습니다. 선택적으로 메모리 크기를 직접 지정할 수 있습니다.

예

다음 예에서는 블록 진단의 메모리 크기를 늘립니다.

```
ciscoasa# blocks queue history enable
```

다음 예에서는 메모리 크기를 3000바이트로 늘립니다.

```
ciscoasa# blocks queue history enable 3000
```

다음 예에서는 메모리 크기를 3000바이트로 늘리려 하지만 이 값이 사용 가능 메모리보다 큽니다.

```
ciscoasa# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

다음 예에서는 메모리 크기를 3000바이트로 늘리지만, 이 값이 사용 가능 메모리의 50%보다 큽니다.

```
ciscoasa# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

관련 명령

명령	설명
clear blocks	시스템 버퍼 통계를 지웁니다.
show blocks	시스템 버퍼 사용량을 표시합니다.

boot

다음 번에 시스템이 다시 로드할 때 어떤 이미지를 사용할지 그리고 시스템 시작 시 어떤 컨피그레이션 파일을 사용할지 지정하려면 글로벌 컨피그레이션 모드에서 **boot** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

boot {config | system} *url*

no boot {config | system} *url*

구문 설명

config	시스템이 로드할 때 사용할 컨피그레이션 파일을 지정합니다.
system	시스템이 로드할 때 사용할 이미지 파일을 지정합니다.
url	이미지 또는 컨피그레이션의 위치를 설정합니다. 다중 컨텍스트 모드에서는 관리 컨텍스트에서 모든 원격 URL에 액세스할 수 있어야 합니다. 다음 URL 구문을 참조하십시오. • **disk0:/**[*path*/]*filename* ASA에서는 이 URL이 내부 플래시 메모리를 가리킵니다. **flash**를 **disk0** 대신 사용할 수 있습니다. 서로 별칭입니다. • **disk1:/**[*path*/]*filename* ASA에서는 이 URL이 외부 플래시 메모리 카드를 가리킵니다. 이 옵션은 ASA Services Module에서 사용할 수 없습니다. • **flash:/**[*path*/]*filename* 이 URL이 내부 플래시 메모리를 가리킵니다. • **tftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] 서버 address 경로를 재정의하려면 인터페이스 이름을 지정합니다. 이 옵션은 ASA 5500 시리즈에 한해 **boot system** 명령에 사용할 수 있습니다. **boot config** 명령을 사용하려면 시작 컨피그레이션이 플래시 메모리에 있어야 합니다. 하나의 **boot system tftp:** 명령만 구성할 수 있으며, 이는 구성된 첫 번째 항목이어야 합니다.

기본값

boot config 명령이 지정되지 않을 경우 시작 컨피그레이션 파일이 숨겨진 위치에 저장되며 이를 사용하는 명령(예: **show startup-config** 명령, **copy startup-config** 명령)에서만 사용됩니다.

boot system 명령은 기본 설정이 없습니다. 위치를 지정하지 않을 경우 ASA는 내부 플래시 메모리만 검색하여 부팅 가능한 첫 번째 이미지를 찾습니다. 부팅 가능한 이미지가 없을 경우 시스템 이미지가 로드되지 않으며 ROMMON 또는 모니터 모드에 들어갈 때까지 ASA의 부팅이 반복됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

write memory 명령을 사용하여 시작 컨피그레이션에 이 명령을 저장할 경우, BOOT 및 CONFIG_FILE 환경 변수에도 그 설정을 저장합니다. 이는 ASA에서 재시작할 때 부팅할 소프트웨어 이미지 및 시작 컨피그레이션을 결정하는 데 사용됩니다.

최대 4개의 **boot system** 명령 엔트리를 입력하여 각기 다른 이미지를 지정할 수 있습니다. 지정한 순서대로 부팅됩니다. ASA는 가장 먼저 발견한 부팅 가능한 이미지로 부팅합니다.

현재 실행 중인 컨피그레이션과 다른 새로운 위치에서 시작 컨피그레이션 파일을 사용하려는 경우, 실행 중인 컨피그레이션을 저장한 다음 이 컨피그레이션 파일을 새 위치에 복사하십시오. 그렇지 않으면 실행 중인 컨피그레이션을 저장할 때 새 시작 컨피그레이션을 덮어씁니다.

팁 ASDM 이미지 파일은 **asdm image** 명령으로 지정합니다.

예

다음 예에서는 ASA가 시작할 때 configuration.txt라는 컨피그레이션 파일을 로드하도록 지정합니다.

```
ciscoasa(config)# boot config disk0:/configuration.txt
```

관련 명령

명령	설명
asdm image	ASDM 소프트웨어 이미지를 지정합니다.
show bootvar	부트 파일 및 컨피그레이션 환경 변수를 표시합니다.

border style

인증된 WebVPN 사용자에게 표시되는 WebVPN Home 페이지의 테두리를 사용자 지정하려면 사용자 지정 컨피그레이션 모드에서 **border style** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

border style *value*

no border style *value*

구문 설명

value	사용할 CSS(Cascading Style Sheet) 매개변수를 지정합니다. 최대 256자입니다.

기본값

테두리의 기본 스타일은 background-color:#669999;color:white입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

style 옵션은 유효한 CSS 매개변수로 나타냅니다. 이 매개변수에 대한 설명은 본 설명서의 범위에 속하지 않습니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹 사이트(www.w3.org)의 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F는 편리한 CSS 매개변수 목록을 포함하고 있으며 www.w3.org/TR/CSS21/propidx.html에서 이용할 수 있습니다.

WebVPN 페이지 - 페이지 색상의 가장 대표적인 변경 방법에 대한 몇 가지 팁을 소개합니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 (HTML에서 인식된다면) 색상의 이름을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며, 각 색상(빨강, 녹색, 파랑)을 나타내는 0~255 범위의 10진수입니다. 쉼표로 구분하여 입력한 값은 해당 강도의 각 색상이 나머지 색상과 조합되는 것을 의미합니다.
- HTML 형식은 #000000이며, 6자리의 16진수입니다. 1번째와 2번째 자리는 빨강을, 3번째와 4번째 자리는 녹색을, 5번째와 6번째는 파랑을 나타냅니다.

참고 손쉽게 WebVPN 페이지를 사용자 지정하려면 ASDM을 사용하는 것이 좋습니다. 색 견본, 미리 보기 등 스타일 요소를 편리하게 구성할 수 있는 기능을 제공합니다.

예

다음 예에서는 테두리의 배경색을 RGB color #66FFFF, 연한 녹색으로 사용자 지정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# border style background-color:66FFFF
```

관련 명령

명령	설명
application-access	WebVPN Home 페이지의 Application Access 상자를 사용자 지정합니다.
browse-networks	WebVPN Home 페이지의 Browse Networks 상자를 사용자 지정합니다.
web-bookmarks	WebVPN Home 페이지의 Web Bookmarks 제목 또는 링크를 사용자 지정합니다.
file-bookmarks	WebVPN Home 페이지의 File Bookmarks 제목 또는 링크를 사용자 지정합니다.

bridge-group

투명 방화벽 모드에서 브리지 그룹에 인터페이스를 지정하려면 인터페이스 컨피그레이션 모드에서 **bridge-group** 명령을 사용합니다. 인터페이스 할당을 취소하려면 이 명령의 **no** 형식을 사용합니다. 투명 방화벽은 동일한 네트워크를 인터페이스에서 연결합니다. 최대 4개의 인터페이스가 하나의 브리지 그룹에 속할 수 있습니다.

bridge-group *number*

no bridge-group *number*

구문 설명

number	1~100의 정수를 지정합니다. 9.3(1) 이상에서는 1~250로 범위가 확대되었습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.3(1)	250개 BVI를 지원하기 위해 범위를 1~250으로 확대했습니다.

사용 지침

9.2 이하에서는 단일 모드에서 또는 다중 모드의 각 컨텍스트에서 최대 8개의 브리지 그룹을 구성할 수 있습니다. 9.3(1) 이상에서는 최대 250개의 브리지 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.

interface bvi 명령과 **ip address** 명령을 차례로 사용하면서 브리지 그룹에 관리 IP 주소를 지정합니다.

각 브리지 그룹은 별도의 네트워크에 연결됩니다. 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.

보안 컨텍스트의 오버헤드를 원치 않거나 보안 컨텍스트를 최대한 활용하려는 경우 둘 이상의 브리지 그룹을 사용할 수 있습니다. 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.

예

다음 예에서는 bridge-group 1에 GigabitEthernet 1/1을 지정합니다.

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# bridge-group 1
```

관련 명령

명령	설명
interface	인터페이스를 구성합니다.
interface bvi	관리 IP 주소를 설정할 수 있도록 브리지 그룹에 대한 인터페이스 컨피그레이션 모드를 시작합니다.
ip address	브리지 그룹의 관리 IP 주소를 설정합니다.
nameif	인터페이스 이름을 설정합니다.
security-level	인터페이스 보안 레벨을 설정합니다.

browse-networks

인증된 WebVPN 사용자에게 표시되는 WebVPN Home 페이지에서 Browse Networks 상자를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **browse-networks** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

browse-networks {**title** | **message** | **dropdown**} {**text** | **style**} *value*

no browse-networks [{**title** | **message** | **dropdown**} {**text** | **style**} *value*]

구문 설명

dropdown	드롭다운 목록에 대한 변경 사항을 지정합니다.
message	제목 아래 표시되는 메시지의 변경 사항을 지정합니다.
style	스타일의 변경 사항을 지정합니다.
text	텍스트의 변경 사항을 지정합니다.
title	제목의 변경 사항을 지정합니다.
value	표시할 실제 텍스트를 나타냅니다. 최대 256자입니다. 이 값은 CSS 매개변수에도 적용됩니다.

기본값

기본 제목 텍스트는 "Browse Networks"입니다.

기본 제목 스타일은

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase입니다.

기본 메시지 텍스트는 "Enter Network Path"입니다.

기본 메시지 스타일은

background-color:#99CCCC;color:maroon;font-size:smaller입니다.

기본 드롭다운 텍스트는 "File Folder Bookmarks"입니다.

기본 드롭다운 스타일은

border:1px solid black;font-weight:bold;color:black;font-size:80%입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

style 옵션은 유효한 CSS 매개변수로 나타냅니다. 이 매개변수에 대한 설명은 본 설명서의 범위에 속하지 않습니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹 사이트(www.w3.org)의 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F는 편리한 CSS 매개변수 목록을 포함하고 있으며 www.w3.org/TR/CSS21/propidx.html에서 이용할 수 있습니다.

WebVPN 페이지 - 페이지 색상의 가장 대표적인 변경 방법에 대한 몇 가지 팁을 소개합니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 (HTML에서 인식된다면) 색상의 이름을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며, 각 색상(빨강, 녹색, 파랑)을 나타내는 0~255 범위의 10진수입니다. 쉼표로 구분하여 입력한 값은 해당 강도의 각 색상이 나머지 색상과 조합되는 것을 의미합니다.
- HTML 형식은 #000000이며, 6자리의 16진수입니다. 1번째와 2번째 자리는 빨강을, 3번째와 4번째 자리는 녹색을, 5번째와 6번째는 파랑을 나타냅니다.

참고 손쉽게 WebVPN 페이지를 사용자 지정하려면 ASDM을 사용하는 것이 좋습니다. 색 견본, 미리 보기 등 스타일 요소를 편리하게 구성할 수 있는 기능을 제공합니다.

예

다음 예에서는 제목을 "Browse Corporate Networks"로 바꾸고 스타일의 텍스트를 blue로 바꿉니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
ciscoasa(config-webvpn-custom)# browse-networks title style color:blue
```

관련 명령

명령	설명
application-access	WebVPN Home 페이지의 Application Access 상자를 사용자 지정합니다.
file-bookmarks	WebVPN Home 페이지의 File Bookmarks 제목 또는 링크를 사용자 지정합니다.
web-applications	WebVPN Home 페이지의 Web Application 상자를 사용자 지정합니다.
web-bookmarks	WebVPN Home 페이지의 Web Bookmarks 제목 또는 링크를 사용자 지정합니다.

파 트 2

C 명령

5 장

cache ~ clear compression 명령

cache

캐시 모드를 시작하고 캐싱 특성의 값을 설정하려면 webvpn 컨피그레이션 모드에서 **cache** 명령을 입력합니다. 컨피그레이션에서 모든 캐시 관련 명령을 제거하고 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

cache

no cache

기본값

각 캐시 특성의 기본 설정과 함께 활성화됩니다.

명령 모드

다음 표는 명령을 입력하는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

캐싱은 자주 재사용되는 객체를 시스템 캐시에 저장합니다. 그러면 콘텐츠 다시 쓰기 및 압축을 반복할 필요성이 줄어듭니다. WebVPN과 원격 서버 및 최종 사용자 브라우저 간의 트래픽을 줄이므로 많은 애플리케이션이 훨씬 더 효율적으로 실행될 수 있습니다.

예

다음 예에서는 캐시 모드를 시작하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

관련 명령

명령	설명
cache-static-content	재작성 대상이 아닌 콘텐츠를 캐싱합니다.
disable	캐싱을 비활성화합니다.
expiry-time	캐싱 객체의 유효성을 재검사하지 않고 그 만료 시간을 구성합니다.
lmfactor	last-modified 타임스탬프만 있는 캐싱 객체에 대해 유효성 재검사 정책을 설정합니다.
max-object-size	캐싱할 객체의 최대 크기를 정의합니다.
min-object-size	캐싱할 객체의 최소 크기를 정의합니다.

cache-time

CRL이 오래된 것으로 간주될 때까지 캐시에 머물 수 있는 기간(분)을 지정하려면 ca-crl 컨피그레이션 모드에서 **cache-time** 명령을 사용합니다. 이 모드는 crypto ca trustpoint 컨피그레이션 모드에서 액세스할 수 있습니다. 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

cache-time *refresh-time*

no cache-time

구문 설명

refresh-time	CRL이 캐시에 머무를 수 있는 시간(분)을 지정합니다. 범위는 1분~1440분입니다. CRL에 NextUpdate 필드가 없을 경우 CRL은 캐싱되지 않습니다.

기본값

기본 설정은 60분입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ca-crl 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 ca-crl 컨피그레이션 모드를 시작하고 trustpoint central에 대해 캐시 시간 새로 고침의 값을 10분으로 지정합니다.

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# cache-time 10
ciscoasa(ca-crl)#
```

관련 명령

명령	설명
crl configure	crl 컨피그레이션 모드를 시작합니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.
enforcenextupdate	인증서의 NextUpdate CRL 필드를 처리할 방법을 지정합니다.

call-agent

통화 에이전트 그룹을 지정하려면 mgcp 맵 컨피그레이션 모드에서 **call-agent** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

구문 설명

group_id	통화 에이전트 그룹의 ID이며, 범위는 0~2147483647입니다.
ip_address	게이트웨이의 IP 주소.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Mgcp 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

하나 이상의 게이트웨이를 관리할 수 있는 통화 에이전트의 그룹을 지정하는 데 **call-agent** 명령을 사용합니다. 통화 에이전트 그룹 정보는 그룹(게이트웨이가 명령을 전송하는 그룹 제외)의 통화 에이전트에 대한 연결을 여는 데 사용됩니다. 그러면 모든 통화 에이전트에서 응답을 보낼 수 있습니다. 동일한 *group_id*의 통화 에이전트는 동일한 그룹에 속합니다. 통화 에이전트 하나가 여러 그룹에 속할 수 있습니다.

예

다음 예에서는 통화 에이전트 10.10.11.5 및 10.10.11.6에서 게이트웨이 10.10.10.115를 제어하고 통화 에이전트 10.10.11.7 및 10.10.11.8에서 두 게이트웨이 10.10.10.116 및 10.10.10.117을 모두 제어할 수 있게 합니다.

```
ciscoasa(config)# mgcp-map mgcp_inbound
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

관련 명령

명령	설명
debug mgcp	MGCP를 위한 디버깅 정보의 표시를 활성화합니다.
mgcp-map	MGCP 맵을 정의하고 MGCP 맵 컨피그레이션 모드를 활성화합니다.
show mgcp	MGCP 컨피그레이션 및 세션 정보를 표시합니다.

call-duration-limit

H.323 통화의 통화 기간을 구성하려면 매개변수 컨피그레이션 모드에서 **call-duration-limit** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

구문 설명

hh:mm:ss	기간을 시간, 분, 초 단위로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 H.323 통화에 대해 통화 기간을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-duration-limit 0:1:0
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3 또는 4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

call-party-numbers

H.323 통화 설정 과정에서 통화자 번호 전송을 적용하려면 매개변수 컨피그레이션 모드에서 **call-party-numbers** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

call-party-numbers

no call-party-numbers

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 H.323 통화의 설정 과정에서 통화자 번호를 적용하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-party-numbers
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3 또는 4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

call-home

콜 홈 컨피그레이션 모드를 시작하려면 글로벌 컨피그레이션 모드에서 **call-home** 명령을 사용합니다.

call-home

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

call-home 명령을 입력하면 프롬프트가 hostname (cfg-call-home)#으로 바뀌며 다음 콜 홈 컨피그레이션 명령에 액세스할 수 있게 됩니다.

- [**no**] **alert-group** {**group name** | **all**}—Smart Call Home 그룹을 활성화하거나 비활성화합니다. 기본적으로 모든 경고 그룹에 대해 활성화됩니다.
  group name: Syslog, diagnostic, environment, inventory, configuration, snapshot, threat, telemetry, test.
- [**no**] **contact-e-mail-addr e-mail-address**—고객 연락처 이메일 주소를 지정합니다. 이 필드는 필수 항목입니다.
  e-mail-address: 최대 127자의 고객 이메일 주소.
- [**no**] **contact-name contact name**—고객 이름을 지정합니다.
  e-mail-address: 최대 127자의 고객 이름.
- **copy profile src-profile-name dest-profile-name**—기존 프로필(**src-profile-name**)의 내용을 새 프로필(**dest-profile-name**)에 복사합니다.
  src-profile-name: 최대 23자의 기존 프로필 이름.
  dest-profile-name: 최대 23자의 새 프로필 이름.
- **rename profile src-profile-name dest-profile-name**—기존 프로필의 이름을 변경합니다.
  src-profile-name: 최대 23자의 기존 프로필 이름.
  dest-profile-name: 최대 23자의 새 프로필 이름.
- **no configuration all**—Smart Call-home 컨피그레이션을 지웁니다.
  [**no**] **customer-id customer-id-string**—고객 ID를 지정합니다.
  customer-id-string: 최대 64자의 고객 ID. 이 필드는 XML 형식 메시지에서 필수 항목입니다.

- [**no**] **event-queue-size queue_size**—이벤트 대기열 크기를 지정합니다.
  queue-size: 이벤트의 수. 범위는 5~60입니다. 기본값은 10입니다.
- [**no**] **mail-server ip-address | name priority 1-100 all**—SMTP 메일 서버를 지정합니다. 고객은 최대 5개의 메일 서버를 지정할 수 있습니다. Smart Call Home 메시지에 이메일 전송을 사용하려면 하나 이상의 메일 서버가 필요합니다.
  ip-address: 메일 서버의 IPv4 또는 IPv6 주소.
  name: 메일 서버의 호스트 이름.
  1-100: 메일 서버의 우선 순위. 번호가 낮을수록 우선 순위가 높습니다.
- [**no**] **phone-number phone-number-string**—고객 전화 번호를 지정합니다. 이 필드는 선택 사항입니다.
  phone-number-string: 전화 번호.
- [**no**] **rate-limit msg-count**—Smart Call Home에서 보낼 수 있는 분당 메시지 수를 지정합니다.
  msg-count: 분당 메시지 수. 기본값은 10입니다.
- [**no**] **sender** {**from e-mail-address | reply-to e-mail-address**} —이메일 메시지의 발신/회신 이메일 주소를 지정합니다. 이 필드는 선택 사항입니다.
  e-mail-address: 발신/회신 이메일 주소.
- [**no**] **site-id site-id-string**—고객 사이트 ID를 지정합니다. 이 필드는 선택 사항입니다.
  site-id-string: 고객의 위치를 식별하는 사이트 ID.
- [**no**] **street-address street-address**—고객 주소를 지정합니다. 이 필드는 선택 사항입니다.
  street-address: 최대 255자의 자유 형식 문자열.
- [**no**] **alert-group-config environment**—환경 그룹 컨피그레이션 모드를 시작합니다.
  [**no**] **threshold** {**cpu | memory**} **low-high**—환경 리소스 임계값을 지정합니다.
  low, high: 유효한 값의 범위는 0~100입니다. 기본값은 85~90입니다.
- [**no**] **alert-group-config snapshot**—스냅샷 그룹 컨피그레이션 모드를 시작합니다.
  system, user: 시스템 또는 사용자 컨텍스트에서 CLI를 실행합니다(멀티 모드에서만 사용 가능).
- [**no**] **add-command "cli command"** [{**system | user**}] —스냅샷 그룹에서 캡처할 CLI 메시지를 지정합니다.
  cli command: 입력할 CLI 명령.
  system, user: 시스템 또는 사용자 컨텍스트에서 CLI를 실행합니다(멀티 모드에서만 사용 가능). 시스템 및 사용자 모두 지정되지 않을 경우 CLI는 시스템 및 사용자 컨텍스트 모두에서 실행됩니다. 기본값은 사용자 컨텍스트입니다.
- [**no**] **profile profile-name | no profile all**—프로필을 생성, 삭제하거나 편집합니다. 프로필 컨피그레이션 모드를 시작하고 프롬프트를 hostname (cfg-call-home-profile)#으로 변경합니다.
  profile-name: 최대 20자의 프로필 이름.
- [**no**] **active**—프로필을 활성화하거나 비활성화합니다. 기본값은 enabled입니다.
  no destination address {**e-mail | http**} **all | [no] destination** {**address** {**e-mail | http**} **e-mail-address | http-url** [**msg-format short-text | long-text | xml**] **| message-size-limit max-size | preferred-msg-format short-text | long-text | xml | transport-method e-mail | http**}—Smart Call Home 메시지 수신자에 대해 목적지, 메시지 크기, 메시지 형식, 전송 방법을 구성합니다. 기본 메시지 형식은 XML이며 기본적으로 활성화된 라우팅 방법은 이메일입니다.
  e-mail-address: Smart Call Home 수신자의 이메일 주소이며 최대 100자입니다.
  http-url: HTTP 또는 HTTPS URL.
  max-size: 최대 메시지 크기(바이트). 0은 제한 없음을 의미합니다. 기본값은 5MB입니다.
- [**no**] **subscribe-to-alert-group alert-group-name** [**severity** {**catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging**}]—지정된 심각도의 그룹 이벤트에 등록합니다.
  alert-group-name: syslog, diagnostic, environment 또는 threat가 유효한 값입니다.

- [**no**] **subscribe-to-alert-group syslog** [{**severity** {**catastrophic** | **disaster** | **emergencies** | **alert** | **critical** | **errors** | **warning** | **notifications** | **informational** | **debugging**} | **message start** [**-end**]}]—어떤 심각도 또는 메시지 ID의 syslog에 등록합니다.
  start-[**end**]: 단일 syslog 메시지 ID 또는 syslog 메시지 ID의 범위.
- [**no**] **subscribe-to-alert-group inventory** [**periodic** {**daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]]—인벤토리 이벤트에 등록합니다.
  day_of_month: 일(1~31).
  day_of_week: 요일(Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: 하루 중 시간과 분(24시간 형식).
- [**no**] **subscribe-to-alert-group configuration** [**export full** | **minimum**] [**periodic** {**daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]]—컨피그레이션 이벤트에 등록합니다.
  full: 실행 중인 컨피그레이션, 시작 컨피그레이션, 기능 목록, 액세스 목록의 요소 수, 멀티 모드에서의 컨텍스트 이름을 내보내기 위한 컨피그레이션.
  minimum: 기능 목록, 액세스 목록의 요소 수, 멀티 모드에서의 컨텍스트 이름만 내보내기 위한 컨피그레이션.
  day_of_month: 일(1~31).
  day_of_week: 요일(Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: 하루 중 시간과 분(24시간 형식).
- [**no**] **subscribe-to-alert-group telemetry periodic** {**hourly** | **daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]—원격 분석 정기 이벤트에 등록합니다.
  day_of_month: 일(1~31).
  day_of_week: 요일(Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: 하루 중 시간과 분(24시간 형식).
- [**no**] **subscribe-to-alert-group snapshot periodic** {**interval minutes** | **hourly** [**mm**] | **daily** | **monthly day_of_month** |**weekly day_of_week** [**hh:mm**]}—스냅샷 정기 이벤트에 등록합니다.
  minutes: 간격(분).
  day_of_month: 일(1~31).
  day_of_week: 요일(Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: 하루 중 시간과 분(24시간 형식).

참고 콜 홈 HTTPS 메시지는 오로지 VRF의 지정된 소스 인터페이스를 통해 **ip http client source-interface** 명령을 사용하여 보낼 수 있으며, 여기서 설명한 **vrf** 명령과는 상관없습니다.

예 다음 예에서는 연락처 정보를 구성하는 방법을 보여줍니다.

```
hostname(config)# call-home
hostname(cfg-call-home)# contact-e-mail-addr username@example.com
hostname(cfg-call-home)# customer-id Customer1234
hostname(cfg-call-home)# phone-number +1-800-555-0199
hostname(cfg-call-home)# site-id Site1
hostname(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

다음 예에서는 콜 홈 메시지 속도 제한 임계값을 구성하는 방법을 보여줍니다.

```
hostname(config)# call-home
hostname(cfg-call-home)# rate-limit 50
```

다음 예에서는 콜 홈 메시지 속도 제한 임계값을 기본 설정으로 바꾸는 방법을 보여줍니다.

```
hostname(config)# call-home
hostname(cfg-call-home)# default rate-limit
```

다음 예에서는 기존 프로필과 동일한 컨피그레이션 설정으로 새 목적지 프로필을 만드는 방법을 보여줍니다.

```
hostname(config)# call-home
hostname(cfg-call-home)# copy profile profile1 profile1a
```

다음 예에서는 기본 및 보조 이메일 서버를 비롯하여 일반적인 이메일 매개변수를 구성하는 방법을 보여줍니다.

```
hostname(config)# call-home
hostname(cfg-call-home)# mail-server smtp.example.com priority 1
hostname(cfg-call-home)# mail-server 192.168.0.1 priority 2
hostname(cfg-call-home)# sender from username@example.com
hostname(cfg-call-home)# sender reply-to username@example.com
```

관련 명령

명령	설명
alert-group	경고 그룹을 활성화합니다.
profile	콜 홈 프로필 컨피그레이션 모드를 시작합니다.
show call-home	콜 홈 컨피그레이션 정보를 표시합니다.

call-home send

CLI 명령을 실행하고 명령 출력을 지정된 이메일 주소로 보내려면 특별 권한 EXEC 모드에서 **call-home send** 명령을 사용합니다.

call-home send cli command [email *email***] [service-number** *service number***]**

구문 설명

cli-command	실행할 CLI 명령을 지정합니다. 명령 출력이 이메일을 통해 전송됩니다.
email *email*	CLI 명령 출력을 보낼 이메일 주소를 지정합니다. 이메일 주소가 지정되지 않을 경우 명령 출력은 Cisco TAC(attach@cisco.com)로 전송됩니다.
service-number *service number*	명령 출력과 관련된 활성 TAC 케이스 번호를 지정합니다. 이 번호는 이메일 주소(또는 TAC 이메일 주소)가 지정되지 않은 경우에만 필요하며, 이메일 제목 줄에 나타납니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

이 명령을 사용하면 지정된 CLI 명령을 시스템에서 실행할 수 있습니다. 지정된 CLI 명령은 따옴표("")로 묶어야 하며 모든 모듈을 위한 명령을 비롯하여 어떤 **run** 또는 **show** 명령도 가능합니다.

그러면 명령 출력이 지정된 이메일 주소로 전송됩니다. 이메일 주소가 지정되지 않을 경우 명령 출력은 Cisco TAC(attach@cisco.com)로 전송됩니다. 이메일은 제목 줄에 서비스 번호(지정된 경우)를 포함하여 긴 텍스트 형식으로 전송됩니다.

예

다음 예에서는 CLI 명령을 보내고 명령 출력을 이메일로 전송하는 방법을 보여줍니다.

```
hostname# call-home send "show diagnostic result module all" email support@example.com
```

관련 명령

call-home	콜 홈 컨피그레이션 모드를 시작합니다.
call-home test	정의한 콜 홈 테스트 메시지를 보냅니다.
service call-home	콜 홈을 활성화하거나 비활성화합니다.
show call-home	콜 홈 컨피그레이션 정보를 표시합니다.

call-home send alert-group

특정 경고 그룹 메시지를 보내려면 특별 권한 EXEC 모드에서 **call-home send alert-group** 명령을 사용합니다.

call-home send alert-group {configuration | telemetry | inventory | group snapshot} [profile *profile-name*]

구문 설명

컨피그레이션	목적지 프로필에 컨피그레이션 경고 그룹 메시지를 보냅니다.
group snapshot	스냅샷 그룹을 보냅니다.
inventory	인벤토리 콜 홈 메시지를 보냅니다.
profile *profile-name*	(선택 사항) destination 프로필의 이름을 지정합니다.
telemetry	특정 모듈, 슬롯/하위 슬롯, 슬롯/베이 번호에 대해 목적지 프로필에 진단 경고 그룹 메시지를 보냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

profile *profile-name*을 지정하지 않을 경우 메시지는 모든 등록된 목적지 프로필에 보내집니다.

컨피그레이션, 진단, 인벤토리 경고 그룹만 직접 보낼 수 있습니다. 목적지 프로필은 경고 그룹에 등록할 필요 없습니다.

예

다음 예에서는 목적지 프로필에 컨피그레이션 경고 그룹 메시지를 보내는 방법을 보여줍니다.

```
hostname# call-home send alert-group configuration
```

다음 예에서는 특정 모듈, 슬롯/하위 슬롯, 슬롯/베이 번호에 대해 목적지 프로필에 진단 경고 그룹 메시지를 보내는 방법을 보여줍니다.

```
hostname# call-home send alert-group diagnostic module 3 5/2
```

다음 예에서는 특정 모듈, 슬롯/하위 슬롯, 슬롯/베이 번호에 대해 모든 목적지 프로필에 진단 경고 그룹 메시지를 보내는 방법을 보여줍니다.

```
hostname# call-home send alert-group diagnostic module 3 5/2 profile Ciscotac1
```

이 예에서는 인벤토리 콜 홈 메시지를 보내는 방법을 보여줍니다.

```
hostname# call-home send alert-group inventory
```

관련 명령

call-home	콜 홈 컨피그레이션 모드를 시작합니다.
call-home test	정의한 콜 홈 테스트 메시지를 보냅니다.
service call-home	콜 홈을 활성화하거나 비활성화합니다.
show call-home	콜 홈 컨피그레이션 정보를 표시합니다.

call-home test

프로필의 컨피그레이션을 사용하여 콜 홈 테스트 메시지를 수동으로 보내려면 특별 권한 EXEC 모드에서 **call-home test** 명령을 사용합니다.

call-home test ["*test-message*"**] profile** *profile-name***e**

구문 설명

profile *profile-name*	destination 프로필의 이름을 지정합니다.
"*test-message*"	(선택 사항) 테스트 메시지 텍스트.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 지정된 목적지 프로필에 테스트 메시지를 보냅니다. 테스트 메시지 텍스트를 입력할 경우 공백이 포함되었다면 따옴표("")로 텍스트를 묶어야 합니다. 메시지를 입력하지 않을 경우 기본 메시지가 보내집니다.

예

다음 예에서는 콜 홈 테스트 메시지를 수동으로 보내는 방법을 보여줍니다.

```
hostname# call-home test "test of the day" profile Ciscotac1
```

관련 명령

call-home	콜 홈 컨피그레이션 모드를 시작합니다.
call-home send alert-group	특정 경고 그룹 메시지를 보냅니다.
service call-home	콜 홈을 활성화하거나 비활성화합니다.
show call-home	콜 홈 컨피그레이션 정보를 표시합니다.

capability lls

LLS 기능이 기본적으로 활성화됩니다. 발생한 OSPF 패킷의 LLS(Link-Local Signalling) 데이터 블록의 사용을 명시적으로 활성화하거나 OSPF NSF 인식을 재활성화하려면 라우터 컨피그레이션 모드에서 **lls command** 기능을 사용합니다. LLS 및 OSPF NSF 인식을 비활성화하려면 이 명령의 no 형식을 사용합니다.

capability lls

no capability lls

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

LLS 기능이 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 도입했습니다.

사용 지침

발생한 OSPF 패킷에서 LLS 데이터 블록의 사용을 비활성화함으로써 NSF 인식을 비활성화하려는 경우가 있습니다. 라우터에서 LLS를 사용하는 애플리케이션이 없어 NSF 인식을 비활성화하려는 경우가 있습니다.

NSF가 구성된 경우 LLS를 비활성화하려고 하면 "OSPF Non-Stop Forwarding (NSF) must be disabled first."라는 오류 메시지가 나타납니다.

LLS가 비활성화된 상태에서 NSF를 구성하려고 하면 "OSPF Link-Local Signaling (LLS) capability must be enabled first."라는 오류 메시지가 나타납니다.

예

다음 예에서는 LLS 지원 및 OSPF 인식을 활성화합니다.

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability lls
```

관련 명령

capability opaque	MPLS TE 정보가 불투명 LSA를 통해 네트워크에 플러딩할 수 있게 합니다.

capability opaque

MPLS TE(Multiprotocol Label Switching traffic engineering) 토폴로지 정보가 불투명 LSA를 통해 네트워크에 플러딩할 수 있게 하려면 라우터 컨피그레이션 모드에서 **capability opaque** 명령을 사용합니다. MPLS TE 토폴로지 정보가 불투명 LSA를 통해 네트워크에 플러딩할 수 없게 하려면 이 명령의 no 형식을 사용합니다.

capability opaque

no capability opaque

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

불투명 LSA는 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 도입했습니다.

사용 지침

capability opaque 명령은 모든 범위의 불투명 LSA(Types 9, 10, 11)를 통해 MPLS TE 정보(Type 1, 4)를 플러딩합니다.

MPLS TE를 지원하려면 OSPF에 대해 불투명 LSA 지원 제어 기능이 활성화되어야 합니다.

기본적으로 MPLS TE 토폴로지 정보가 불투명 LSA를 통해 영역에 플러딩됩니다.

예

다음 예에서는 opaque 기능을 활성화합니다.

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability opaque
```

관련 명령

capability lls	OSPF 발생 패킷에서 LLS 데이터 블록의 사용을 활성화하고 OSPF NSF 인식을 활성화합니다.

capture

패킷 스니핑 및 네트워크 오류 격리를 위해 패킷 캡처 기능을 활성화하려면 특별 권한 EXEC 모드에서 **capture** 명령을 사용합니다. 패킷 캡처 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

[cluster exec] capture *capture_name* **[type {asp-drop all** [*drop-code*] **| tls-proxy | raw-data | lacp | isakmp [ikev1 | ikev2] | inline-tag [***tag***] | webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] [**interface asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

[cluster exec] no capture *capture_name* [**type {asp-drop all** [*drop-code*] **| tls-proxy | raw-data | lacp | isakmp** [**ikev1 | ikev2**] **| inline-tag [***tag***] | webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] [**asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

구문 설명

access-list *access_list_name*	(선택 사항) 액세스 목록과 매칭하는 트래픽을 캡처합니다. 다중 컨텍스트 모드에서는 하나의 컨텍스트 내에서만 사용 가능합니다.
any	단일 IP 주소 및 마스크가 아니라 임의의 IP 주소를 지정합니다.
all	ASA에서 삭제하는 모든 패킷을 캡처합니다.
asa_dataplane	ASA를 지나는 ASA 백플레인 및 이 백플레인을 사용하는 모듈(예: ASA CX 또는 ASA FirePOWER 모듈)의 패킷을 캡처합니다.
asp-drop *drop-code*	(선택 사항) 가속 보안 경로에서 삭제하는 패킷을 캡처합니다. *drop-code*는 가속 보안 경로에서 삭제하는 트래픽의 유형을 지정합니다. drop code의 목록은 **show asp drop frame** 명령을 참조하십시오. *drop-code* 인수를 입력하지 않을 경우 삭제된 패킷이 모두 캡처됩니다. **packet-length**, **circular-buffer**, **buffer** 키워드와 함께 이 키워드를 입력할 수 있습니다. **interface** 또는 **ethernet-type** 키워드는 함께 사용하지 않습니다. 클러스터에서는 유닛 간의 폐기 전달 데이터 패킷도 캡처합니다. 다중 컨텍스트 모드에서는 이 옵션을 시스템 컨텍스트에서 실행하면 모든 폐기된 데이터 패킷이 캡처됩니다. 이 옵션을 사용자 컨텍스트에서 실행하면 그 사용자 컨텍스트에 속한 인터페이스에서 들어온 폐기 데이터 패킷만 캡처됩니다.
buffer *buf_size*	(선택 사항) 패킷을 저장할 버퍼 크기(바이트)를 정의합니다. 바이트 버퍼가 차면 패킷 캡처를 중지합니다. 클러스터에서 사용될 때는 모든 유닛의 합계가 아니라 유닛별 크기입니다.
capture_name	패킷 캡처의 이름을 지정합니다.. 여러 트래픽 유형을 캡처하려면 여러 **capture** 문에 동일한 이름을 사용합니다. **show capture** 명령을 사용하여 캡처 컨피그레이션을 볼 경우 모든 옵션이 한 행으로 조합됩니다.
circular-buffer	(선택 사항) 버퍼가 차면 처음부터 버퍼를 덮어씁니다.
cluster exec	(선택 사항) 클러스터링 구축에서 래퍼 CLI 접두사로만 사용하며, **capture** 및 **show capture** 명령과 함께 사용할 수 있습니다. 한 유닛에서 **capture** 명령을 보내고 동시에 나머지 모든 유닛에서 이 명령을 실행할 수 있게 합니다.
ethernet-type *type*	(선택 사항) 캡처할 이더넷 유형을 선택합니다. 지원되는 이더넷 유형은 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, VLAN 등입니다. 802.1Q 또는 VLAN 유형에는 예외 사항이 있습니다. 802.1Q 태그는 자동으로 건너뛰며, 내부 이더넷 유형은 매칭에 사용됩니다.

host *ip*	패킷이 보내지는 호스트의 단일 IP 주소를 지정합니다.
inline-tag *tag*	특정 SGT 값의 태그를 지정하거나 미지정 상태로 두어 임의의 SGT 값을 갖는 태그 있는 패킷을 캡처합니다.
interface *interface_name*	패킷 캡처를 사용할 인터페이스의 이름을 설정합니다. 캡처할 모든 패킷에 대해 인터페이스를 구성해야 합니다. 여러 **capture** 명령을 동일한 이름으로 사용하여 여러 인터페이스를 구성할 수 있습니다. ASA의 데이터 플레인에서 패킷을 캡처하려면 **interface** 키워드를 "asa_dataplane"이라는 인터페이스 이름과 함께 사용할 수 있습니다. 클러스터 제어 링크 인터페이스의 트래픽을 캡처하기 위해 "cluster"를 인터페이스 이름으로 지정할 수 있습니다. "cluster" 및 "asa-dataplane"은 고정된 인터페이스 이름이므로 구성할 수 없습니다. type **lacp** 캡처가 구성된 경우 인터페이스 이름은 물리적 이름입니다.
ikev1/ikev2	IKEv1 또는 IKEv2 프로토콜 정보를 캡처합니다.
isakmp	(선택 사항) VPN 연결에 대해 ISAKMP 트래픽을 캡처합니다. ISAKMP 하위 시스템은 상위 레이어 프로토콜에 대한 액세스 권한이 없습니다. 이 캡처는 의사 캡처로서 PCAP 파서를 충족하기 위해 물리적, IP, UDP 레이어를 결합합니다. 피어 주소는 SA 교환에서 얻으며 IP 레이어에 저장됩니다.
lacp	(선택 사항) LACP 트래픽을 캡처합니다. 구성된 경우 인터페이스 이름은 물리적 인터페이스 이름입니다. **trace**, **match**, **access-list** 키워드는 **lacp** 키워드와 함께 사용할 수 없습니다.
mask	IP 주소에 대한 서브넷 마스크. 네트워크 마스크를 지정할 때의 방식은 Cisco IOS 소프트웨어 **access-list** 명령과 다릅니다. ASA에서는 네트워크 마스크(예: 클래스 C 마스크는 255.255.255.0)를 사용합니다. Cisco IOS 마스크는 와일드카드 비트(예: 0.0.0.255)를 사용합니다.
match *prot*	캡처할 패킷의 필터링을 허용하기 위해 5-튜플과 매칭하는 패킷을 지정합니다. 한 행에서 이 키워드를 최대 3번 사용할 수 있습니다.
operator	(선택 사항) 소스 또는 목적지에서 사용하는 포트 번호와 매칭합니다. 허용되는 연산자는 다음과 같습니다. • **lt**—보다 작음 • **gt**—보다 큼 • **eq**—같음 • **neq**—같지 않음 • **range**—범위
packet-length *bytes*	(선택 사항) 캡처 버퍼에 저장할 각 패킷의 최대 바이트 수를 설정합니다.
port	(선택 사항) 프로토콜을 **tcp** 또는 **udp**로 설정할 경우 TCP 또는 UDP 포트의 정수 또는 이름을 지정합니다.
raw-data	(선택 사항) 하나 이상의 인터페이스에서 인바운드 및 아웃바운드 패킷을 캡처합니다.
real-time	캡처된 패킷을 실시간으로 연속 표시합니다. 실시간 패킷 캡처를 종료하려면 **Ctrl + c** 를 입력합니다.캡처를 영구적으로 삭제하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션은 **raw-data** 및 **asp-drop** 캡처에만 적용됩니다. **cluster exec capture** 명령을 사용할 때는 이 옵션이 지원되지 않습니다.
reinject-hide	(선택 사항) 재삽입된 패킷은 캡처하지 않도록 지정합니다. 클러스터링 환경에서만 적용합니다.
tls-proxy	(선택 사항) 하나 이상의 인터페이스에서 TLS 프록시로부터 해독된 인바운드 및 아웃바운드 데이터를 캡처합니다.

trace *trace_count*	(선택 사항) 패킷 추적 정보 및 캡처할 패킷 수를 캡처합니다. 이 옵션을 액세스 목록과 함께 사용하여 데이터 경로에 추적 패킷을 삽입함으로써 패킷이 예상대로 처리되었는지 여부를 확인할 수 있습니다.
type	(선택 사항) 캡처한 데이터의 유형을 지정합니다.
user *webvpn-user*	(선택 사항)WebVPN 캡처를 위한 사용자 이름을 지정합니다.
webvpn	(선택 사항) 특정 WebVPN 연결을 위한 WebVPN 데이터를 캡처합니다.

기본값

기본 설정은 다음과 같습니다.

- 기본 **type**은 **raw-data**입니다.
- 기본 **buffer** *size*는 512 KB입니다.
- 기본 Ethernet type은 IP 패킷입니다.
- 기본 **packet-length**는 1518바이트입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
6.2(1)	이 명령을 도입했습니다.
7.0(1)	**type asp-drop**, **type isakmp**, **type raw-data**, **type webvpn** 키워드를 포함하도록 이 명령을 수정했습니다.
7.0(8)	**all** 옵션을 추가했습니다. ASA에서 삭제하는 모든 패킷을 캡처할 수 있습니다.
7.2(1)	**trace** *trace_count*, **match** *prot*, **real-time**, **host** *ip*, **any**, *mask*, *operator* 옵션을 포함하도록 명령을 수정했습니다.
8.0(2)	콘텐츠를 캡처하기 위해 경로를 업데이트하도록 명령을 수정했습니다.
8.4(1)	새로운 **type** 키워드인 **ikev1** 및 **ikev2**를 추가했습니다.
8.4(2)	IDS 출력에 세부 사항을 추가했습니다.
8.4(4.1)	ASA CX 모듈에서 백플레인을 지나는 트래픽을 지원하기 위해 **asa_dataplane** 옵션을 추가했습니다.
9.0(1)	**cluster**, **cluster exec**, **reinject-hide** 키워드를 추가했습니다. 새로운 **type** 옵션 **lacp**를 추가했습니다. ISAKMP를 위해 다중 컨텍스트 모드 지원을 추가했습니다.
9.1(3)	**asa_dataplane** 옵션으로 ASA CX 백플레인에서 캡처한 패킷의 필터링을 지원합니다.
9.2(1)	**asa_dataplane** 옵션을 확장하여 ASA FirePOWER 모듈을 지원합니다.
9.3(1)	SGT plus Ethernet Tagging 기능을 지원하기 위해 **inline-tag** *tag* 키워드-인수 쌍을 추가했습니다.

사용 지침

패킷 캡처는 연결 문제를 해결하거나 의심스러운 활동을 모니터링할 때 유용합니다. 다중 캡처를 생성할 수 있습니다. 패킷 캡처를 보려면 **show capture** *name* 명령을 사용합니다. 파일에 캡처를 저장하려면 **copy capture** 명령을 사용합니다. 웹 브라우저에서 패킷 캡처 정보를 보려면 **https://***ASA-ip-address***/admin/capture/***capture_name*[**/pcap**] 명령을 사용합니다. **pcap** 선택적 키워드를 지정할 경우 libpcap 형식의 파일이 웹 브라우저에 다운로드되며 웹 브라우저에서 이를 저장할 수 있습니다. libcap 파일은 TCPDUMP 또는 Ethereal로 볼 수 있습니다.

버퍼 내용을 ASCII 형식으로 TFTP 서버에 복사할 경우 헤더만 볼 수 있습니다. 패킷의 세부 사항 및 16진수 덤프는 볼 수 없습니다. 세부 사항 및 16진수 덤프를 보려면 버퍼를 PCAP 형식으로 전송하고 TCPDUMP 또는 Ethereal로 읽어야 합니다.

참고 WebVPN 캡처를 활성화하면 ASA의 성능에 영향을 줍니다. 문제 해결에 필요한 캡처 파일을 만든 후 반드시 캡처를 비활성화하십시오.

선택적 키워드 없이 **no capture**를 입력하면 캡처가 삭제됩니다. **access-list** 선택적 키워드를 지정할 경우 액세스 목록이 캡처에서 제거되고 캡처는 보존됩니다. **interface** 키워드를 지정할 경우 캡처가 지정된 인터페이스에서 분리되고 캡처는 보존됩니다. 캡처 자체를 지우지 않으려면 **no capture** 명령을 **ccess-list** 또는 **interface** 선택적 키워드와 함께 사용합니다.

실시간 표시가 진행 중일 때는 캡처에 대해 어떤 작업도 수행할 수 없습니다. 느린 콘솔 연결에서 **real-time** 키워드를 사용하면 성능 문제 때문에 매우 많은 수의 패킷이 표시되지 않을 수 있습니다. 버퍼의 고정 한도는 패킷 1000개입니다. 버퍼가 찰 경우 캡처된 패킷에 대해 카운터가 관리됩니다. 다른 세션을 열 경우 **no capture real-time** 명령을 입력하여 실시간 표시를 비활성화할 수 있습니다.

참고 **capture** 명령은 실행 중인 컨피그레이션에 저장되지 않으며, 장애 조치 과정에서 스탠바이 유닛에 복사되지 않습니다.

ASA는 자신을 지나는 모든 IP 트래픽을 추적하고 자신을 목적지로 하는 모든 IP 트래픽을 캡처할 수 있습니다. 여기에는 모든 관리 트래픽(예: SSH 및 텔넷 트래픽)도 포함됩니다.

ASA 아키텍처는 패킷 처리를 위한 서로 다른 3가지 프로세서 집합으로 구성됩니다. 이 아키텍처는 캡처 기능에 일정한 제한을 가합니다. 일반적으로 ASA의 패킷 전달 기능 대부분은 2개의 프론트엔드 네트워크 프로세서에 의해 처리되며, 이 프로세서에서 애플리케이션 검사를 필요로 하는 경우에만 컨트롤 플레인 범용 프로세서에 패킷을 보냅니다. 가속 경로 프로세서에 세션 누락이 있을 경우에만 세션 관리 경로 네트워크 프로세서에 패킷을 보냅니다.

ASA에서 전달하거나 삭제하는 모든 패킷이 2개의 프론트엔드 네트워크 프로세서를 거치므로 패킷 캡처 기능은 이 네트워크 프로세서에 구현됩니다. 따라서 ASA를 지나는 모든 패킷은 이 프론트엔드 프로세서에서 캡처합니다. 단, 이 트래픽 인터페이스에 대해 알맞은 캡처가 구성되어야 합니다. 인그레스에서는 패킷이 ASA 인터페이스에 도착할 때 패킷이 캡처됩니다. 이그레스에서는 패킷이 외부로 전송되기 직전에 패킷이 캡처됩니다.

클러스터 전체 캡처를 수행한 다음 클러스터에 있는 모든 유닛의 동일한 캡처 파일을 TFTP 서버에 동시에 복사하려면 마스터 유닛에서 다음 명령을 입력합니다.

```
ciscoasa# cluster exec copy /pcap capture: cap_name tftp://location/path/filename.pcap
```

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일 이름에는 유닛 이름이 자동으로 추가됩니다(예: filename_A.pcap, filename_B.pcap 등). 이 예에서는 A와 B가 클러스터 유닛 이름입니다.

참고 파일 이름의 끝에 유닛 이름을 추가하면 다른 목적지 이름이 생성됩니다.

다음은 캡처 기능의 몇 가지 제한 사항입니다. 이러한 제한 대부분은 ASA 아키텍처의 분산 특성 및 ASA에서 사용하는 하드웨어 가속기에서 비롯된 것입니다.

- IP 트래픽만 캡처할 수 있습니다. ARP와 같은 비 IP 패킷은 캡처할 수 없습니다.
- 다중 컨텍스트 모드의 클러스터 제어 링크 캡처에서는 클러스터 제어 링크에서 전송된, 해당 컨텍스트와 관련된 패킷만 캡처됩니다.
- 다중 컨텍스트 모드에서 **copy capture** 명령은 시스템 영역에서만 사용할 수 있습니다. 구문은 다음과 같습니다.

  copy /pcap capture:*Context-name*/*in-cap* **tftp**:

  여기서 *in-cap*은 컨텍스트 *context-name*에 구성된 캡처입니다.
- **cluster exec capture realtime** 명령은 지원되지 않습니다. 다음과 같은 오류 메시지가 표시됩니다.

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```

- 공유 VLAN은 다음 지침이 적용됩니다.
  - VLAN에서는 하나의 캡처만 구성할 수 있습니다. 공유 VLAN에서 다중 컨텍스트 캡처를 구성할 경우, 구성된 마지막 캡처만 사용됩니다.
  - 마지막으로 구성된 (활성) 캡처를 삭제하면, 어떤 캡처도 활성화되지 않습니다. 앞서 다른 컨텍스트에서 캡처를 구성했더라도 그렇습니다. 캡처를 제거했다가 다시 추가해야 활성화됩니다.
  - 캡처가 연결된 인터페이스에 들어온 (그리고 캡처 액세스 목록과 매칭하는) 모든 트래픽이 캡처됩니다. 공유 VLAN의 다른 컨텍스트로 가는 트래픽도 포함됩니다.
  - 따라서 컨텍스트 B에서도 사용하는 VLAN에서 컨텍스트 A의 캡처를 활성화한 경우 컨텍스트 A와 컨텍스트 B의 인그레스 트래픽이 모두 캡처됩니다.
- 이그레스 트래픽의 경우 활성 캡처의 컨텍스트 트래픽만 캡처됩니다. 유일한 예외는 ICMP 검사를 활성화하지 않은 경우입니다. 그러면 ICMP 트래픽은 가속 경로에 세션이 없습니다. 그러한 경우 공유 VLAN의 모든 컨텍스트에 대한 인그레스 및 이그레스 ICMP 트래픽이 캡처됩니다.
- 일반적으로 캡처 구성은 캡처할 트래픽에 매칭하는 액세스 목록을 구성하는 것입니다. 트래픽 패턴에 매칭하는 액세스 목록이 구성된 다음에는 캡처를 정의하고 이 액세스 목록을 캡처에 연결하며 캡처가 구성될 인터페이스와도 연결해야 합니다. IPv4 트래픽을 캡처할 때는 액세스 목록과 인터페이스가 캡처와 연결된 경우에만 캡처가 작동합니다. IPv6 트래픽에는 액세스 목록이 필요하지 않습니다.
- ASA CX 모듈 트래픽의 경우 캡처된 패킷은 PCAP 뷰어에서 읽을 수 없는 추가 AFBP 헤더를 포함합니다. 이 패킷을 보려면 알맞은 플러그인을 사용해야 합니다.
- 인라인 SGT 태그 처리된 패킷의 경우, 캡처된 패킷은 PCAP 뷰어에서 이해하지 못할 추가 CMD 헤더를 포함합니다.
- 인그레스 인터페이스가 없고 전역 인터페이스가 없을 경우 백플레인에서 전송된 패킷은 시스템 컨텍스트에서 제어 패킷으로 간주됩니다. 이 패킷은 액세스 목록 검사를 건너뛰므로 항상 캡처됩니다. 이 동작은 단일 모드 및 다중 컨텍스트 모드 모두에 적용됩니다.

예

패킷을 캡처하려면 다음 명령을 입력합니다.

```
ciscoasa# capture captest interface inside
ciscoasa# capture captest interface outside
```

웹 브라우저에서 다음 위치로 이동하면 실행된 **capture** 명령인 "captest"의 내용을 볼 수 있습니다.

```
https://171.69.38.95/admin/capture/captest
```

(웹 브라우저에서 사용하는) libpcap 파일을 로컬 시스템에 다운로드하려면 다음 명령을 입력합니다.

```
https://171.69.38.95/capture/http/pcap
```

다음 예에서는 171.71.69.234의 외부 호스트에서 내부 HTTP 서버에 트래픽을 캡처하는 것을 보여줍니다.

```
ciscoasa# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
ciscoasa# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
ciscoasa# capture http access-list http packet-length 74 interface inside
```

다음 예에서는 ARP 패킷을 캡처하는 방법을 보여줍니다.

```
ciscoasa# capture arp ethernet-type arp interface outside
```

다음 예에서는 데이터 스트림에 5개의 추적(tracer) 패킷을 삽입합니다. 여기서 *access-list 101*은 TCP 프로토콜 FTP와 매칭하는 트래픽을 정의합니다.

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

추적된 패킷 및 패킷 처리 정보를 읽기 쉽게 표시하려면 **show capture ftptrace** 명령을 사용합니다.

다음 예에서는 캡처된 패킷을 실시간으로 표시하는 방법을 보여줍니다.

```
ciscoasa# capture test interface outside real-time
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.

10 packets displayed
12 packets not displayed due to performance limitations
```

다음 예에서는 캡처해야 할 IPv4 트래픽을 매칭하는 확장 액세스 목록을 구성하는 방법을 보여줍니다.

```
ciscoasa (config)# access-list capture extended permit ip any any
```

다음 예에서는 캡처를 구성하는 방법을 보여줍니다.

```
ciscoasa (config)# capture name access-list acl_name interface interface_name
```

기본적으로 캡처를 구성하면 512KB 크기의 선형 캡처 버퍼가 생성됩니다. 선택적으로 순환형 버퍼를 구성할 수 있습니다. 기본적으로 패킷의 68바이트만 버퍼에 캡처됩니다. 선택적으로 이 값을 변경할 수 있습니다.

다음 예에서는 외부 인터페이스에 적용되는 이미 구성된 캡처 액세스 목록을 사용하여 "ip-capture"라는 캡처를 만듭니다.

```
ciscoasa (config)# capture ip-capture access-list capture interface outside
```

다음 예에서는 캡처를 보는 방법을 보여줍니다.

```
ciscoasa (config)# show capture name
```

다음 예에서는 캡처를 종료하되 버퍼를 보존하는 방법을 보여줍니다.

```
ciscoasa (config)# no capture name access-list acl_name interface interface_name
```

다음 예에서는 캡처를 종료하고 버퍼를 삭제하는 방법을 보여줍니다.

```
ciscoasa (config)# no capture name
```

다음 예에서는 단일 모드의 백플레인에서 캡처된 트래픽을 필터링하는 방법을 보여줍니다.

```
ciscoasa# capture x interface asa_dataplane access-list any4
ciscoasa# capture y interface asa_dataplane match ip any any
```

참고 액세스 목록을 지정했더라도 제어 패킷은 단일 모드에서 캡처됩니다.

다음 예에서는 다중 컨텍스트 모드의 백플레인에서 캡처되는 트래픽을 필터링하는 방법을 보여줍니다.

사용자 컨텍스트에서 사용:

```
ciscoasa (contextA)# capture x interface asa_dataplane access-list any4
ciscoasa (contextA)# capture y interface asa_dataplane match ip any any
```

시스템 컨텍스트에서 사용:

```
ciscoasa# capture z interface asa_dataplane
```

참고 다중 컨텍스트 모드에서는 **access-list** 및 **match** 옵션을 시스템 컨텍스트에서 사용할 수 없습니다.

클러스터링을 위한 캡처

클러스터의 모든 유닛에서 캡처를 활성화하기 위해 각 명령의 앞에 **cluster exec** 키워드를 추가할 수 있습니다.

다음 예에서는 클러스터링 환경에서 LACP 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet0/0
```

다음 예는 클러스터링 링크에서 제어 경로 패킷의 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# cap cp interface cluster match udp any eq 49495 any
ciscoasa (config)# cap cp interface cluster match udp any any eq 49495
```

다음 예는 클러스터링 링크에서 데이터 경로 패킷의 캡처를 생성하는 방법을 보여줍니다.

```
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
```

다음 예는 클러스터를 지나는 데이터 경로 트래픽을 캡처하는 방법을 보여줍니다.

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match dup host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

다음 예는 실제 소스를 실제 목적지에 매칭하는 흐름의 로직 업데이트 메시지를 캡처하는 방법 그리고 실제 소스를 실제 목적지에 매칭하는, CCL을 통해 전달되는 패킷을 캡처하는 방법을 보여줍니다.

```
ciscoasa (config)# access-list dp permit real src real dst
```

다음 예에서는 icmp echo request/response와 같이 한 ASA에서 다른 ASA로 전달되는 특정 유형의 데이터 플레인 메시지를 **match** 키워드 또는 그 메시지 유형의 액세스 목록을 사용하여 캡처하는 방법을 보여줍니다.

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

다음 예에서는 클러스터링 환경의 클러스터 제어 링크에서 액세스 목록 103을 사용하여 캡처를 만드는 방법을 보여줍니다.

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster
```

앞의 예에서 A와 B가 CCL 인터페이스의 IP 주소일 경우 이 두 유닛 간에 전송된 패킷만 캡처됩니다.

A와 B가 디바이스를 지나는 트래픽의 IP 주소라면 다음과 같이 됩니다.

- 전달된 패킷은 평소와 같이 캡처됩니다. 단, 소스 및 목적지 IP 주소가 액세스 목록과 매칭되어야 합니다.
- 데이터 경로 로직 업데이트 메시지는 A와 B 간의 흐름 또는 액세스 목록(예: access-list 103)을 위한 것일 때만 캡처됩니다. 캡처는 임베드된 흐름의 5-튜플에 매칭합니다.
- UDP 패킷의 소스 및 수신 주소가 CCL 주소이지만 이 패킷이 주소 A 및 B와 연결된 흐름을 업데이트하는 것이라면 이 역시 캡처됩니다. 즉 패킷에 임베드된 주소 A와 B가 매칭되는 한 역시 캡처됩니다.

관련 명령

명령	설명
clear capture	캡처 버퍼를 지웁니다.
copy capture	서버에 캡처 파일을 복사합니다.
show capture	어떤 옵션도 지정되지 않으면 캡처 컨피그레이션을 표시합니다.

cd

현재 작업 디렉토리를 지정된 디렉토리로 변경하려면 특별 권한 EXEC 모드에서 **cd** 명령을 사용합니다.

cd [disk0: | disk1: | flash:] [*path*]

구문 설명

disk0:	내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다.
disk1:	이동식 외부 플래시 메모리 카드를 지정하고 그 다음에 콜론을 표시합니다.
flash:	내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다. ASA 5500 시리즈에서는 **flash** 키워드의 별칭이 **disk0**입니다.
path	(선택 사항) 변경 후 디렉토리의 절대 경로.

기본값

디렉토리를 지정하지 않을 경우 루트 디렉토리로 변경됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 "config" 디렉토리를 변경하는 방법을 보여줍니다.

```
ciscoasa# cd flash:/config/
```

관련 명령

명령	설명
pwd	현재 작업 디렉토리를 표시합니다.

cdp-url

로컬 CA에서 발급하는 인증서에 포함할 CDP를 지정하려면 ca 서버 컨피그레이션 모드에서 **cdp-url** 명령을 사용합니다. 기본 CDP로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

[no] cdp-url *url*

구문 설명

url	유효성 검사 당사자가 로컬 CA에서 발급한 인증서의 폐기 상태를 확인하는 URL을 지정합니다. URL은 500자 이내의 영숫자여야 합니다.

기본값

기본 CDP URL은 로컬 CA를 포함하는 ASA의 URL입니다. 기본 URL은 http://hostname.domain/+CSCOCA+/asa_ca.crl 형식입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

CDP는 발급된 인증서에 포함할 수 있는 확장으로서 유효성 검사 당사자가 인증서의 폐기 상태를 확인할 수 있는 위치를 지정합니다. 한 번에 하나의 CDP만 구성할 수 있습니다.

참고 CDP URL이 지정될 경우 관리자는 그 위치에서 현재 CRL에 대한 액세스 권한을 관리할 책임이 있습니다.

예

다음 예에서는 로컬 CA 서버에서 발급한 인증서에 대해 10.10.10.12를 CDP로 구성합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# cdp-url http://10.10.10.12/ca/crl
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	ca server 컨피그레이션 모드 CLI 명령 집합에 대한 액세스를 제공합니다. 그러면 로컬 CA를 구성하고 관리할 수 있습니다.
crypto ca server crl issue	강제적으로 CRL을 발행합니다.
crypto ca server revoke	로컬 CA 서버가 발급한 인증서를 인증서 데이터베이스 및 CRL에서 폐기된 것으로 표시합니다.
crypto ca server unrevoke	로컬 CA 서버에서 발급했고 이미 폐기된 인증서를 폐기 해제합니다.
lifetime crl	인증서 폐기 목록의 수명을 지정합니다.

certificate

지정된 인증서를 추가하려면 crypto ca 인증서 체인 컨피그레이션 모드에서 **certificate** 명령을 사용합니다. 인증서를 삭제하려면 이 명령의 **no** 형식을 사용합니다.

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

구문 설명

ca	인증서가 CA 발급 인증서임을 나타냅니다.
certificate-serial-number	16진수 형식이고 "quit"로 끝나는 인증서의 일련 번호를 지정합니다.
ra-encrypt	인증서가 SCEP에서 사용하는 RA 키 암호화 인증서임을 나타냅니다.
ra-general	인증서가 SCEP 메시징에서 디지털 서명 및 키 암호화에 사용되는 RA 인증서임을 나타냅니다.
ra-sign	인증서가 SCEP 메시징에서 사용하는 RA 디지털 서명 인증서임을 나타냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Crypto ca 인증서 체인 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령이 실행되면 ASA는 함께 제공된 데이터를 16진수 형식의 인증서로 해석합니다. **quit** 문자열은 인증서의 끝을 나타냅니다.

CA는 네트워크에서 보안 자격 증명 및 메시지 암호화용 공개 키를 발급하고 관리하는 권한을 갖고 있습니다. 공개 키 인프라에서 CA는 디지털 인증서 요청자가 제공한 정보를 RA에게 확인합니다. RA가 요청자 정보를 확인하면 CA는 인증서를 발급할 수 있습니다.

예

다음 예에서는 일련 번호가 29573D5FF010FE25B45인 CA 인증서를 추가합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crypto ca certificate chain central
ciscoasa(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.
crypto ca certificate chain	crypto ca certificate chain 모드를 시작합니다.
crypto ca trustpoint	ca trustpoint 모드를 시작합니다.
show running-config crypto map	모든 암호 맵에 대한 모든 컨피그레이션을 표시합니다.

certificate-group-map

인증서 맵의 규칙 엔트리를 터널 그룹과 연결하려면 webvpn 컨피그레이션 모드에서 **certificate-group-map** 명령을 사용합니다. 현재 터널 그룹 맵 연결을 지우려면 이 명령의 **no** 형식을 사용합니다.

certificate-group-map *certificate_map_name index tunnel_group_name*

no certificate-group-map

구문 설명

certificate_map_name	인증서 맵의 이름.
index	인증서 맵에 있는 맵 엔트리의 숫자 식별자. 이 색인 값의 범위는 1~65535입니다.
tunnel_group_name	맵 엔트리가 인증서와 매칭할 경우 선택되는 터널 그룹의 이름. *tunnel-group name*이 이미 있어야 합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

certificate-group-map 명령이 실행된 상태에서 WebVPN 클라이언트에서 받은 인증서가 맵 엔트리와 일치할 경우, 그에 따라 생성되는 터널 그룹이 연결에 사용됩니다. 사용자가 선택한 터널 그룹은 무시됩니다.

certificate-group-map 명령의 다중 인스턴스로 다중 매핑이 가능합니다.

예

다음 예에서는 tgl이라는 터널 그룹에 대해 규칙 6를 연결하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

관련 명령

명령	설명
crypto ca certificate map	인증서 발급자 및 주체 DN(distinguished name)을 기반으로 규칙을 구성하기 위해 ca 인증서 맵 컨피그레이션 모드를 시작합니다.
tunnel-group-map	인증서 기반 IKE 세션을 터널 그룹에 매핑하기 위한 정책과 규칙을 구성합니다.

chain

인증서 체인 전송을 활성화하려면 tunnel-group ipsec-attributes 컨피그레이션 모드에서 **chain** 명령을 사용합니다. 이 명령을 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

chain

no chain

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

모든 IPsec 터널 그룹 유형에 이 특성을 적용할 수 있습니다.

이 명령을 입력하면 루트 인증서 모든 부속 CA 인증서가 함께 전송됩니다.

예

tunnel-group-ipsec attributes 컨피그레이션 모드에서 입력한 다음 예에서는 IP 주소가 209.165.200.225인 IPSec LAN-to-LAN 터널 그룹을 위한 체인 전송을 활성화합니다. 여기에는 루트 인증서 및 모든 부속 CA 인증서가 포함됩니다.

```
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)# chain
ciscoasa(config-tunnel-ipsec)#
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	현재 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group ipsec-attributes	이 그룹에 대한 tunnel-group ipsec-attributes를 구성합니다.

change-password

사용자가 자신의 계정 비밀번호를 변경할 수 있게 하려면 특별 권한 EXEC 모드에서 **change-password** 명령을 사용합니다.

change-password [/silent] [old-password *old-password* **[new-password** *new-password*]]

구문 설명

new-password *new-password*	새 비밀번호를 지정합니다.
old-password *old-password*	사용자를 다시 인증합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	—	—	• 예
글로벌 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
8.4(4.1)	이 명령을 도입했습니다.

사용 지침

사용자가 비밀번호를 생략할 경우 ASA는 입력 프롬프트를 표시합니다. 사용자가 **change-password** 명령을 입력할 때 실행 중인 컨피그레이션을 저장하라는 메시지가 표시됩니다. 사용자가 비밀번호를 변경한 다음에는 컨피그레이션 변경 사항을 저장하도록 다시 안내하는 메시지가 나타납니다.

예

다음 예에서는 사용자 계정 비밀번호를 변경합니다.

```
ciscoasa# change-password old-password myoldpassword000 new password mynewpassword123
```

관련 명령

명령	설명
show run password-policy	현재 컨텍스트에 대한 비밀번호 정책을 표시합니다.
clear configure password-policy	현재 컨텍스트에 대한 비밀번호 정책을 기본값으로 재설정합니다.
clear configure username	사용자 계정에서 사용자 이름을 제거합니다.

changeto

보안 컨텍스트와 시스템 사이에서 전환하려면 특별 권한 EXEC 모드에서 **changeto** 명령을 사용합니다.

changeto {system | context *name***}**

구문 설명

context *name*	지정된 이름의 컨텍스트로 변경합니다.
system	시스템 실행 영역으로 변경합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

시스템 실행 영역 또는 관리 컨텍스트에 로그인한 경우 여러 컨텍스트 사이에서 전환하면서 각 컨텍스트에서 컨피그레이션 및 모니터링 작업을 수행할 수 있습니다. 컨피그레이션 모드에서 수정하거나 **copy** 또는 **write** 명령에 사용되는 "실행 중" 컨피그레이션은 현재 어떤 실행 영역에 있느냐에 따라 달라집니다. 시스템 실행 영역에 있다면 실행 중 컨피그레이션은 시스템 컨피그레이션으로만 이루어집니다. 컨텍스트 실행 영역에 있을 경우 실행 중 컨피그레이션은 해당 컨텍스트로만 이루어집니다. 예를 들어, **show running-config** 명령을 입력할 때 모든 실행 중 컨피그레이션(시스템 및 모든 컨텍스트)을 볼 수는 없습니다. 현재 컨피그레이션만 표시됩니다.

예

다음 예에서는 특별 권한 EXEC 모드에서 여러 컨텍스트와 시스템 사이를 전환합니다.

```
ciscoasa/admin# changeto system
ciscoasa# changeto context customerA
ciscoasa/customerA#
```

다음 예에서는 인터페이스 컨피그레이션 모드에서 시스템과 관리 컨텍스트 사이를 전환합니다. 여러 실행 영역 사이에서 전환할 때 컨피그레이션 모드에 있다면 다음 실행 영역에서는 글로벌 컨피그레이션 모드로 바뀝니다.

```
ciscoasa(config-if)# changeto context admin
ciscoasa/admin(config)#
```

관련 명령

명령	설명
admin-context	어떤 컨텍스트를 관리 컨텍스트로 설정합니다.
context	시스템 컨피그레이션에서 보안 컨텍스트를 만들고 컨텍스트 컨피그레이션 모드를 시작합니다.
show context	컨텍스트의 목록(시스템 실행 영역) 또는 현재 컨텍스트에 대한 정보를 표시합니다.

channel-group

물리적 인터페이스를 EtherChannel에 할당하려면 인터페이스 컨피그레이션 모드에서 **channel-group** 명령을 사용합니다. 인터페이스 할당을 취소하려면 이 명령의 **no** 형식을 사용합니다.

channel-group *channel_id* **mode {active | passive | on} [vss-id {1 | 2}]**

no channel-group *channel_id*

구문 설명

channel_id	인터페이스를 할당할 EtherChannel을 1~48 범위에서 지정합니다.
vss-id {**1** | **2**}	(선택 사항) 클러스터링 환경에서 ASA를 VSS 또는 vPC에 있는 2개의 스위치에 연결하는 경우 **vss-id** 키워드를 구성하여 이 인터페이스가 연결될 스위치(1 또는 2)를 식별합니다. 또한 포트 채널 인터페이스에 **port-channel span-cluster vss-load-balance** 명령을 사용해야 합니다.
mode {**active** | **passive** | **on**}	EtherChannel의 각 물리적 인터페이스를 다음과 같이 구성할 수 있습니다. • Active—LACP(Link Aggregation Control Protocol) 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다. • 패시브 — LACP 업데이트를 받습니다. 액티브 EtherChannel에서는 액티브 EtherChannel과의 연결만 설정할 수 있습니다. • On — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 또 다른 "on" 상태의 EtherChannel과의 연결만 설정할 수 있습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	ASA 클러스터링 및 Spanned EtherChannel을 지원하기 위해 **vss-id** 키워드를 추가했습니다.

사용 지침

각 채널 그룹은 8개의 액티브 인터페이스를 가질 수 있습니다. 하나의 채널 그룹에 최대 16개의 인터페이스를 할당할 수 있습니다. 8개의 인터페이스만 액티브 상태이지만, 나머지 인터페이스는 인터페이스 오류가 발생하면 스탠바이 링크의 역할을 할 수 있습니다.

채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.

이러한 채널 ID의 채널 포트 인터페이스가 컨피그레이션에 아직 없을 경우, 다음이 추가됩니다.

interface port-channel *channel_id*

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 컨피그레이션원 인터페이스의 끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

ASA 클러스터링

Spanned EtherChannel에서는 각 ASA에 여러 인터페이스를 포함할 수 있습니다. ASA당 여러 인터페이스는 VSS 또는 vPC에서 두 스위치에 모두 연결하는 경우에 특히 유용합니다. ASA를 VSS 또는 vPC에 있는 두 개의 스위치에 연결할 경우, **vss-load-balance** 키워드를 사용하여 VSS 로드 밸런싱을 활성화해야 합니다. 이 기능은 VSS(또는 vPC) 쌍에 대한 ASA 간의 물리적 링크 연결이 균형을 이루도록 보장합니다. 로드 밸런싱을 활성화하기 전에 멤버 인터페이스별로 **channel-group** 명령에서 **vss-id** 키워드를 구성해야 합니다.

예

다음 예에서는 채널 그룹 1에 인터페이스를 할당합니다.

```
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-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# channel-group 1 mode passive
```

관련 명령

명령	설명
interface port-channel	EtherChannel을 구성합니다.
lacp max-bundle	채널 그룹에서 허용되는 액티브 인터페이스의 최대 개수를 지정합니다.
lacp port-priority	채널 그룹에서 물리적 인터페이스의 우선 순위를 설정합니다.
lacp system-priority	LACP 시스템 우선 순위를 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, 네이버 세부 정보 같은 LACP 정보가 표시됩니다.
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령어를 사용하면 포트 및 포트 채널 정보도 표시됩니다.
show port-channel load-balance	지정된 매개변수 범위에 대해 선택된 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

character-encoding

WebVPN 포털 페이지에서 전역 문자 인코딩을 지정하려면 webvpn 컨피그레이션 모드에서 **character-encoding** 명령을 사용합니다. 문자 인코딩 특성의 값을 제거하려면 이 명령의 **no** 형식을 사용합니다.

character-encoding *charset*

no character-encoding *charset*

구문 설명

charset	최대 40자의 문자열이며, http://www.iana.org/assignments/character-sets에 지정된 유효한 문자 집합 중 하나와 같습니다. 이 페이지에 있는 문자 집합의 이름 또는 별칭을 사용할 수 있습니다. 이를테면 iso-8859-1, shift_jis, ibm850입니다. 이 문자열은 대/소문자를 구분하지 않습니다. 명령 해석기가 ASA 컨피그레이션에서 대문자를 소문자로 변환합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

*문자 인코딩*은 "문자 코딩" 및 "문자 집합"이라고도 하며 데이터를 나타내기 위해 원시 데이터(예: 0과 1)와 문자를 짝지은 것입니다. 언어에 따라 사용할 문자 인코딩 방식이 결정됩니다. 일부 언어는 동일한 방식을 사용하며, 그렇지 않은 언어도 있습니다. 일반적으로 지리적 위치에 따라 브라우저의 기본 인코딩 방식이 결정되지만 사용자가 이를 변경할 수 있습니다. 또한 브라우저가 페이지에 지정된 인코딩을 감지하고 알맞게 문서를 렌더링할 수도 있습니다. 문자 인코딩 특성은 사용자가 WebVPN 포털 페이지의 문자 인코딩 방식을 지정함으로써 브라우저를 사용하는 지역 또는 브라우저의 변경 사항과 상관없이 브라우저에서 제대로 렌더링할 수 있게 합니다.

문자 인코딩 특성을 전역 설정이므로 기본적으로 모든 WebVPN 포털 페이지가 상속합니다. 그러나 사용자는 문자 인코딩 특성의 값과 다른 문자 인코딩을 사용하는 CIFS(Common Internet File System) 서버에 대해 파일 인코딩 특성을 재정의할 수 있습니다. 다른 문자 인코딩을 요구하는 CIFS 서버에 다른 파일 인코딩 값을 사용합니다.

CIFS 서버에서 WebVPN 사용자에게 다운로드된 WebVPN 포털 페이지는 서버를 식별하는 WebVPN 파일 인코딩 특성의 값을 인코딩합니다. 그렇지 않으면 문자 인코딩 특성의 값을 상속합니다. 원격 사용자의 브라우저는 이 값을 자체 문자 인코딩 집합의 엔트리에 매핑하여 사용하기에 적합한 문자 집합을 확인합니다. WebVPN 컨피그레이션에서 CIFS 서버를 위한 파일 인코딩 엔트리를 지정하지 않고 문자 인코딩 특성도 설정되지 않은 경우, WebVPN 포털 페이지는 값을 지정하지 않습니다. WebVPN 포털 페이지에서 문자 인코딩을 지정하지 않을 경우 또는 브라우저에서 지원하지 않는 문자 인코딩 값을 지정할 경우, 원격 브라우저는 자체 기본 인코딩을 사용합니다.

페이지뿐 아니라 파일 이름 또는 디렉토리 경로를 올바르게 렌더링하는 것과 관련하여 문제가 있을 경우, 전역으로는 WebVPN 문자 인코딩 특성을 사용하여, 개별적으로는 파일 인코딩 재정의를 통해 CIFS 서버를 알맞은 문자 인코딩에 매핑함으로써 CIFS 페이지를 정확하게 처리하고 표시할 수 있습니다.

참고 문자 인코딩 값과 파일 인코딩 값은 브라우저에서 사용하는 글꼴 패밀리를 제외하지 않습니다. 사용자는 다음 예와 같이 일본어 Shift_JIS 문자 인코딩을 사용하는 경우 이 값 중 하나의 설정을 webvpn 사용자 지정 명령 모드의 **page style** 명령으로 보완하여 글꼴 패밀리를 대체해야 합니다. 또는 webvpn 사용자 지정 명령 모드에서 **no page style** 명령을 입력하여 글꼴 패밀리를 제거해야 합니다.

이 특성의 값이 없을 때는 원격 브라우저에 설정된 인코딩 유형에 따라 WebVPN 포털 페이지의 문자 집합이 결정됩니다.

예

다음 예에서는 일본어 Shift_JIS 문자를 지원하도록 문자 인코딩 특성을 설정하고 글꼴 패밀리를 제거하며 기본 배경색을 유지합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# character-encoding shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

관련 명령

명령	설명
debug webvpn cifs	CIFS 서버에 대한 디버깅 메시지를 표시합니다.
file-encoding	CIFS 서버와 이 특성의 값을 재정의할 문자 인코딩을 지정합니다.
show running-config [all] webvpn	WebVPN을 위해 실행 중인 컨피그레이션을 표시합니다. 기본 컨피그레이션을 포함하려면 **all** 키워드를 사용합니다.

checkheaps

체크힙 확인 간격을 구성하려면 글로벌 컨피그레이션 모드에서 **checkheaps** 명령을 사용합니다. 이 값을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

구문 설명

check-interval	버퍼 확인 간격을 설정합니다. 버퍼 확인 프로세스에서는 힙의 온전성(할당된 메모리 버퍼 및 여유 메모리 버퍼)을 검사합니다. 이 프로세스를 실행할 때마다 ASA는 전체 힙을 확인하면서 각 메모리 버퍼의 유효성을 검사합니다. 하자가 있다면 ASA는 "할당 버퍼 오류" 또는 "여유 버퍼 오류"를 표시합니다. 오류가 있을 경우 ASA는 가능하다면 추적 정보를 덤프하고 다시 로드합니다.
seconds	간격을 1초~2147483초 범위에서 설정합니다.
validate-checksum	코드 영역 체크섬 유효성 검사 간격을 설정합니다. ASA에서 처음으로 부팅할 때 ASA는 전체 코드의 해시를 계산합니다. 그 이후의 정기 점검에서는 ASA가 새 해시를 생성하고 이를 최초의 해시와 비교합니다. 불일치하다면 ASA는 "텍스트 체크섬 체크힙 오류"를 표시합니다. 오류가 있을 경우 ASA는 가능하다면 추적 정보를 덤프하고 다시 로드합니다.

기본값

기본 간격은 각각 60초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

체크힙은 힙 메모리 버퍼의 온전성(동적 메모리는 시스템 힙 메모리 영역으로부터 할당됨) 및 코드 영역의 무결성을 확인하는 주기적인 프로세스입니다.

예

다음 예에서는 버퍼 할당 간격을 200초로, 코드 영역 체크섬 간격을 500초로 설정합니다.

```
ciscoasa(config)# checkheaps check-interval 200
ciscoasa(config)# checkheaps validate-checksum 500
```

관련 명령

명령	설명
show checkheaps	체크힙 정의를 표시합니다.

check-retransmission

TCP 재전송 유형의 공격을 방지하려면 tcp-map 컨피그레이션 모드에서 **check-retransmission** 명령을 사용합니다. 이 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

check-retransmission

no check-retransmission

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본값은 disabled입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용합니다. **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 모드를 시작하려면 **tcp-map** 명령을 사용합니다. 불일치한 재전송에 대한 최종 시스템의 해석에서 비롯되는 TCP 재전송 유형의 공격을 방지하려면 tcp-map 컨피그레이션 모드에서 **check-retransmission** 명령을 사용합니다.

ASA는 재전송된 데이터가 원본과 동일한지 확인하려고 시도합니다. 데이터가 일치하지 않으면 ASA는 연결을 끊습니다. 이 기능이 활성화되면 TCP 연결의 패킷은 오로지 순서대로 허용됩니다. 자세한 내용은 **queue-limit** 명령을 참조하십시오.

예

다음 예에서는 모든 TCP 플로우에서 TCP check-retransmission 기능을 활성화합니다.

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# check-retransmission
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.
help	**policy-map**, **class**, **description** 명령에 대한 구문 도움말을 표시합니다.
policy-map	정책을 구성합니다. 즉 트래픽 클래스와 하나 이상의 작업과 연결합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 컨피그레이션 모드에 대한 액세스를 허용합니다.

checksum-verification

TCP 체크섬 확인을 활성화하거나 비활성화하려면 tcp-map 컨피그레이션 모드에서 **checksum-verification** 명령을 사용합니다. 이 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

checksum-verification

no checksum-verification

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

체크섬 확인은 기본적으로 비활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용합니다. **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 모드를 시작하려면 **tcp-map** 명령을 사용합니다. TCP 체크섬 확인을 활성화하려면 tcp-mcp 컨피그레이션 모드에서 **checksum-verification** 명령을 사용합니다. 검사에서 통과하지 못하면 패킷은 삭제됩니다.

예

다음 예에서는 TCP 연결 10.0.0.0~20.0.0.0에서 TCP 체크섬 확인을 활성화합니다.

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# checksum-verification

ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1

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.
help	**policy-map**, **class**, **description** 명령에 대한 구문 도움말을 표시합니다.
policy-map	정책을 구성합니다. 즉 트래픽 클래스와 하나 이상의 작업과 연결합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 컨피그레이션 모드에 대한 액세스를 허용합니다.

cipc security-mode authenticated

CIPC(Cisco IP Communicator) 소프트폰이 음성/데이터 VLAN 시나리오에 구축되었을 때 CIPS 소프트폰이 반드시 인증 모드에서만 작동하게 하려면 phone-proxy 컨피그레이션 모드에서 **cipc security-mode authenticated** 명령을 사용합니다. CIPC 소프트폰이 암호화를 지원할 경우 이 명령을 해제하려면 이 명령의 **no** 형식을 사용합니다.

cipc security-mode authenticated

no cipc security-mode authenticated

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본적으로 이 명령은 no 형식을 통해 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
전화 프록시 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

VLAN을 사용하여 음성과 데이터 트래픽을 분리하면 데이터 VLAN에 침투하려는 보안 위협에 음성 스트림이 노출되지 않아 보안상 매우 바람직합니다. 그러나 CIPC 소프트폰 애플리케이션은 음성 VLAN에 상주하는 각자의 IP 전화기에 연결해야 합니다. 이러한 요구 사항이 음성 VLAN과 데이터 VLAN을 분리하는 데 걸림돌로 작용합니다. SIP 프로토콜과 SCCP 프로토콜이 광범위한 포트에서 RTP/RTCP 포트에 대한 동적 협상을 수행하기 때문입니다. 이러한 동적 협상이 이루어지려면 두 VLAN 간에 수많은 포트가 열려 있어야 합니다.

참고 인증 모드를 지원하지 않는 CIPC 초기 버전에서는 전화 프록시가 지원되지 않습니다.

수많은 포트에서 VLAN 간의 액세스가 발생하는 일 없이 데이터 VLAN의 CIPS 소프트폰을 음성 VLAN에 있는 각자의 IP 전화기에 연결하기 위해 **cipc security-mode authenticated** 명령을 사용하여 전화 프록시를 구성할 수 있습니다.

이 명령을 사용하면 전화 프록시가 CIPC 컨피그레이션 파일을 찾아내고 CIPC 소프트폰에 암호화 모드가 아닌 인증 모드를 적용할 수 있습니다. 최신 버전의 CIPC는 암호화 모드를 지원하지 않기 때문입니다.

이 명령이 활성화되면 전화 프록시는 전화 컨피그레이션 파일을 구문 분석하여 전화기가 CIPC 소프트폰인지 확인하고 보안 모드를 인증 모드로 전환합니다. 또한 전화 프록시가 기본적으로 모든 전화기에 암호화 모드를 적용하지만, CIPC 소프트폰은 인증 모드만 지원합니다.

예

다음 예에서는 CIPC 소프트폰이 음성/데이터 VLAN 시나리오에 구축되었을 때 CIPC 소프트폰을 반드시 인증 모드에서 작동하기 위해 **cipc security-mode authenticated** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)#cipc security-mode authenticated
```

관련 명령

명령	설명
phone-proxy	전화 프록시 인스턴스를 구성합니다.

clacp static-port-priority

액티브 EtherChannel 멤버가 9개 이상일 때 필요한, 클러스터링 Spanned EtherChannel의 LACP 동적 포트 우선 순위를 비활성화하려면 글로벌 컨피그레이션 모드에서 **clacp static-port-priority** 명령을 사용합니다. 동적 포트 우선 순위를 활성화하려면 이 명령의 **no** 형식을 사용합니다.

clacp static-port-priority

no clacp static-port-priority

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

이 명령은 기본적으로 비활성화됩니다. 즉 동적 포트 우선 순위가 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

일부 스위치에서는 동적 포트 우선 순위를 지원하지 않으므로, 이 명령을 사용하면 스위치 호환성이 개선됩니다. 또한 이 명령을 사용하면 8개 이상의 액티브 Spanned EtherChannel 멤버를 지원하는 것이 허용되므로 최대 32개의 멤버를 지원할 수 있습니다. 이 명령을 사용하지 않을 경우 8개의 액티브 멤버 및 8개의 스탠바이 멤버만 지원됩니다.

ASA EtherChannel에서 최대 16개의 액티브 링크를 지원합니다. *Spanned* EtherChannel에서는 이 기능이 더욱 확장되어 vPC에서 2개의 스위치와 함께 사용할 때 그리고 **clacp static-port-priority** 명령으로 동적 포트 우선 순위를 비활성화할 때 클러스터의 전 범위에서 최대 32개의 액티브 링크를 지원합니다. 스위치에서는 16개의 액티브 링크가 포함된 EtherChannel(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000)을 지원해야 합니다.

VSS 또는 vPC에서 8개의 액티브 링크를 지원하는 스위치를 사용하려는 경우, 이제 Spanned EtherChannel에서 16개의 액티브 링크를 구성하면 됩니다(각 스위치에 8개씩 연결됨).

참고 Spanned EtherChannel에서 액티브 링크를 9개 이상 사용하려는 경우 스탠바이 링크까지 보유할 수는 없습니다. 액티브 링크를 9~32개까지 지원하려면 스탠바이 링크를 사용할 수 있게 해주는 cLACP 동적 포트 우선 순위를 비활성화해야 합니다.

예

다음 예에서는 동적 포트 우선 순위를 비활성화합니다.

```
ciscoasa(config)# clacp static-port-priority
```

관련 명령

명령	설명
clacp system-mac	cLACP 시스템 ID를 설정합니다.

clacp system-mac

ASA 클러스터의 마스터 유닛에서 cLACP 시스템 ID를 수동으로 구성하려면 클러스터 그룹 컨피그레이션 모드에서 **clacp system-mac** 명령을 사용합니다. 기본 설정으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

no clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

구문 설명

mac_address	수동으로 *H.H.H* 형식의 시스템 ID를 설정합니다. 여기서 H는 16비트 16진수입니다. 예를 들어, MAC 주소 00-0A-00-00-AA-AA는 000A.0000.AAAA로 입력됩니다.
auto	시스템 ID를 자동으로 생성합니다.
system-priority *number*	시스템 우선 순위를 1~65535 범위에서 설정합니다. 우선순위는 번들링 결정을 담당할 유닛을 지정하는 데 사용됩니다. 기본적으로 ASA에서는 우선순위가 가장 높은 우선순위 1을 사용합니다. 우선순위는 스위치의 우선순위보다 높아야 합니다.

명령 기본값

기본적으로 system-mac는 자동으로 생성됩니다(**auto**).

기본적으로 시스템 우선 순위는 1입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

Spanned EtherChannel을 사용하면 ASA에서는 cLACP를 통해 네이버 스위치와 EtherChannel을 협상합니다.클러스터의 ASA는 cLACP 협상 과정에서 협업을 수행하므로 스위치에 단일(가상) 디바이스로 표시됩니다. cLACP 협상의 한 가지 매개변수는 MAC 주소 형식으로 된 시스템 ID입니다. 모든 ASA에서 동일한 시스템 ID를 사용합니다. 이는 (기본 설정에 따라) 마스터 유닛에서 자동으로 생성되어 모든 슬레이브에 복제됩니다. 또는 이 명령에서처럼 수동으로 지정됩니다. 문제 해결을 위해, 이를테면 식별하기 쉬운 MAC 주소를 사용하기 위해 MAC 주소를 수동으로 구성할 수도 있습니다. 일반적으로 자동 생성된 MAC 주소를 사용하게 됩니다.

이 명령은 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다. 그러나 클러스터링을 활성화한 후에는 이 값을 변경할 수 없습니다.

예

다음 예에서는 시스템 ID를 수동으로 구성합니다.

```
cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    health-check
    clacp system-mac 000a.0000.aaaa
    enable noconfirm
```

관련 명령

명령	설명
cluster group	클러스터 매개변수를 구성합니다.

class(global)

보안 컨텍스트를 지정할 리소스 클래스를 만들려면 글로벌 컨피그레이션 모드에서 **class** 명령을 사용합니다. 클래스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

class *name*

no class *name*

구문 설명

name	최대 20자의 문자열로 이름을 지정합니다. 기본 클래스에 대해 이 제한을 설정하려면 **default**를 이름으로 입력합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

기본적으로 모든 보안 컨텍스트는 ASA의 리소스에 무제한으로 액세스할 수 있습니다. 단, 컨텍스트별로 최대 한도가 적용되는 경우는 제외합니다. 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.

클래스를 만들 때 ASA는 그 클래스에 지정되는 컨텍스트별로 일정 부분의 리소스를 떼어 놓지 않습니다. 그 대신 ASA는 하나의 컨텍스트에 대해 최대 한도를 설정합니다. 리소스를 오버서브스크립션하거나 일부 리소스가 무제한이 되는 것을 허용할 경우, 몇몇 컨텍스트에서 이 리소스를 "소진"하여 다른 컨텍스트에 대한 서비스에 영향을 줄 수 있습니다. 클래스에 대한 리소스를 설정하려면 **limit-resource** 명령을 참조하십시오.

모든 컨텍스트는 별도의 클래스에 지정되지 않는 한 기본 클래스에 속해 있습니다. 직접 기본 클래스에 컨텍스트를 지정할 필요는 없습니다.

어떤 컨텍스트가 기본 클래스가 아닌 클래스에 속할 경우, 항상 이 클래스의 설정이 기본 클래스의 설정에 우선합니다. 그러나 그 클래스에서 어떤 설정이 정의되지 않았다면 멤버 컨텍스트는 기본 클래스의 해당 제한을 적용합니다. 예를 들어, 모든 동시 연결에 대한 2% 제한이 있지만 그 밖의 어

떤 제한도 없는 클래스를 만든다면 그 밖의 제한은 기본 클래스로부터 상속됩니다. 이와 달리 모든 리소스에 대해 제한이 있는 클래스를 만들 경우 이 클래스는 기본 클래스의 어떤 설정도 사용하지 않습니다.

기본적으로 기본 클래스는 모든 컨텍스트에서 리소스에 대해 무제한 액세스 권한을 제공합니다. 단, 다음 항목은 컨텍스트당 최대 허용 한도가 기본적으로 설정되어 있습니다.

- 텔넷 세션—5개 세션
- SSH 세션—5개 세션
- MAC 주소—65,535개 항목

예

다음 예에서는 conns에 대한 기본 클래스 한도를 무제한이 아닌 10%로 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 5000
```

관련 명령

명령	설명
clear configure class	클래스 컨피그레이션을 지웁니다.
context	보안 컨텍스트를 구성합니다.
limit-resource	클래스에 대한 리소스 제한을 설정합니다.
member	리소스 클래스에 컨텍스트를 지정합니다.
show class	클래스에 지정된 컨텍스트를 표시합니다.

class(policy-map)

정책 맵에 클래스 맵을 지정하려면(여기서 클래스 맵 트래픽에 작업을 지정할 수 있음) 정책 맵 컨피그레이션 모드에서 **class** 명령을 사용합니다. 정책 맵에서 클래스 맵을 제거하려면 이 명령의 **no** 형식을 사용합니다.

class *classmap_name*

no class *classmap_name*

구문 설명

classmap_name	클래스 맵의 이름을 지정합니다. 레이어 3/4 정책 맵의 경우(**policy-map** 명령) 레이어 3/4 클래스 맵 이름(**class-map** 또는 **class-map type management** 명령)을 지정해야 합니다. 검사 정책 맵의 경우(**policy-map type inspect** 명령) 검사 클래스 맵 이름(**class-map type inspect** 명령)을 지정해야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
정책 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

class 명령을 사용하려면 Modular Policy Framework를 사용합니다. 레이어 3/4 정책 맵에서 클래스를 사용하려면 다음 명령을 입력합니다.

1. **class-map**—작업을 수행할 트래픽을 나타냅니다.
2. **policy-map**—각 클래스 맵과 관련된 작업을 나타냅니다.
   a. **class**—작업을 수행할 클래스 맵을 나타냅니다.
   b. *commands for supported features*—지정된 클래스 맵에서 QoS, 애플리케이션 검사, CSC 또는 AIP SSM, TCP 및 UDP 연결 제한 및 시간 초과, TCP 정규화와 같은 다양한 기능에 대한 여러 작업을 구성할 수 있습니다. 각 기능에서 사용할 수 있는 명령에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.
3. **service-policy**—인터페이스에 또는 전역에 정책 맵을 지정합니다.

검사 정책 맵에서 클래스를 사용하려면 다음 명령을 입력합니다.

1. **class-map type inspect**—작업을 수행할 트래픽을 나타냅니다.
2. **policy-map type inspect**—각 클래스 맵과 연관된 작업을 나타냅니다.
   a. **class**—작업을 수행할 검사 클래스 맵을 나타냅니다.
   b. *commands for application types*—각 애플리케이션 유형에서 사용할 수 있는 명령은 CLI 컨피그레이션 가이드를 참조하십시오. 검사 정책 맵의 클래스 컨피그레이션 모드에서 다음과 같은 작업이 지원됩니다.
   - 패킷 삭제
   - 연결 중지
   - 연결 재설정
   - 로깅
   - 메시지 속도 제한
   - 콘텐츠 작성

   c. **parameters**—검사 엔진에 영향을 미치는 매개변수를 구성합니다. CLI가 매개변수 컨피그레이션 모드로 들어갑니다. 사용 가능한 명령에 대해서는 CLI 컨피그레이션 가이드를 참조하십시오.
3. **class-map**—작업을 수행할 트래픽을 나타냅니다.
4. **policy-map**—각 클래스 맵과 관련된 작업을 나타냅니다.
   a. **class**—작업을 수행할 레이어 3/4 클래스 맵을 나타냅니다.
   b. **inspect** *application inspect_policy_map*—애플리케이션 검사를 활성화하고 특별한 작업을 수행할 검사 정책 엔진을 호출합니다.
5. **service-policy**—인터페이스에 또는 전역에 정책 맵을 지정합니다.

이 컨피그레이션은 모든 트래픽과 매칭하는 **class-default**라는 클래스 맵을 항상 포함합니다. 이 컨피그레이션은 각 레이어 3/4 정책 맵의 끝에 아무런 작업도 정의되지 않은 **class-default** 클래스 맵을 넣습니다. 모든 트래픽과 매칭하려는 경우 그리고 다른 클래스 맵을 만드는 수고를 피하기 위해 이 클래스 맵을 사용할 수도 있습니다. 실제로 **class-default** 클래스 맵에서는 **shape** 명령과 같은 일부 기능만 구성 가능합니다.

class-default 클래스 맵까지 포함하여 최대 63개의 **class** 및 **match** 명령을 정책 맵에서 구성할 수 있습니다.

예

다음은 **class** 명령을 포함하는 연결 정책을 위한 **policy-map** 명령의 예입니다. 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.

관련 명령

명령	설명
class-map	레이어 3/4 클래스 맵을 만듭니다.
class-map type management	관리 트래픽을 위한 레이어 3/4 클래스 맵을 만듭니다.
clear configure policy-map	모든 정책 맵 컨피그레이션을 제거합니다. **service-policy** 명령에서 사용 중인 정책 맵은 제외합니다.
match	트래픽 매칭 매개변수를 정의합니다.
policy-map	정책을 구성합니다. 이는 각각 하나 이상의 작업이 있는 트래픽 클래스가 하나 이상 연결된 것입니다.

class-map

Modular Policy Framework를 사용할 때 글로벌 컨피그레이션 모드에서 **class-map** 명령을 **type** 키워드 없이 사용하여 작업을 적용할 레이어 3 또는 4 트래픽을 식별합니다. 클래스 맵을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

class-map *class_map_name*

no class-map *class_map_name*

구문 설명

class_map_name	최대 길이 40자로 클래스 맵 이름을 지정합니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 클래스 맵 유형은 레이어 3/4 통과 트래픽에만 사용할 수 있습니다. ASA를 목적지로 하는 관리 트래픽에 대해서는 **class-map type management** 명령을 참조하십시오.

Layer 3/4 클래스 맵은 작업을 적용할 Layer 3 및 4 트래픽을 식별합니다. 각 Layer 3/4 정책 맵에 대해 여러 Layer 3/4 클래스 맵을 만들 수 있습니다.

기본 클래스 맵

이 컨피그레이션은 ASA가 기본 전역 정책에서 사용하는 기본 레이어 3/4 클래스 맵을 포함합니다. 이를 **inspection_default**라고 하며 기본 검사 트래픽을 매칭합니다.

```
class-map inspection_default
 match default-inspection-traffic
```

기본 컨피그레이션에 존재하는 또 다른 클래스 맵은 모든 트래픽을 확인하는 class-default입니다.

```
class-map class-default
 match any
```

이 클래스 맵은 모든 Layer 3/4 정책 맵의 끝에 나타나며, 모든 기타 트래픽에 대해서는 어떤 작업도 수행하지 않도록 ASA에 특별히 지시합니다. 원한다면 직접 **match any** 클래스 맵을 만들지 않고 class-default 클래스 맵을 사용할 수 있습니다. 사실 class-default에서는 QoS 트래픽 쉐이핑과 같은 일부 기능만 사용 가능합니다.

최대 클래스 맵

모든 유형을 포괄하여 클래스 맵의 최대 개수는 단일 모드에서 또는 다중 모드의 컨텍스트당 255개입니다. 클래스 맵에는 다음 유형이 포함됩니다.

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** 명령: 정책 맵 유형 검사 컨피그레이션 모드

이 한도에는 모든 유형의 기본 클래스 맵도 포함됩니다.

컨피그레이션 개요

Modular Policy Framework의 컨피그레이션은 4가지 작업으로 구성됩니다.

1. **class-map** 또는 **class-map type management** 명령을 사용하여 작업을 적용하려는 레이어 3 및 레이어 4 트래픽을 식별합니다.
2. (애플리케이션 검사만) **policy-map type inspect** 명령을 사용하여 애플리케이션 검사 트래픽을 위한 특별한 작업을 정의합니다.
3. **policy-map** 명령을 사용하여 레이어 3 및 4 트래픽에 작업을 적용합니다.
4. **service-policy** 명령을 사용하여 인터페이스에서 작업을 활성화합니다.

class-map 컨피그레이션 모드를 시작하려면 **class-map** 명령을 사용합니다. class-map 컨피그레이션 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다. 레이어 3/4 클래스 맵은 클래스 맵에 포함되는 트래픽을 식별하는 **match** 명령을 최대 1개 포함합니다(**match tunnel-group** 및 **match default-inspection-traffic** 명령 제외).

예

다음 예에서는 4개의 레이어 3/4 클래스 맵을 만듭니다.

```
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 all_http
ciscoasa(config-cmap)# description "This class-map matches all HTTP traffic"
ciscoasa(config-cmap)# match port tcp eq http

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 type management	ASA로 향하는 트래픽을 위한 클래스 맵을 만듭니다.
policy-map	트래픽 클래스를 하나 이상의 작업과 연결하여 정책 맵을 생성합니다.
policy-map type inspect	애플리케이션 검사를 위한 특별한 작업을 정의합니다.
service-policy	정책 맵을 하나 이상의 인터페이스와 연결하여 보안 정책을 생성합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

class-map type inspect

Modular Policy Framework를 사용할 때 글로벌 컨피그레이션 모드에서 **class-map type inspect** 명령을 사용하여 검사 애플리케이션과 관련된 기준과 매칭합니다. 검사 클래스 맵을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

class-map type inspect *application* **[match-all | match-any]** *class_map_name*

no class-map [type inspect *application* **[match-all | match-any]]** *class_map_name*

구문 설명

application	매칭할 애플리케이션 트래픽의 유형을 지정합니다. 다음과 같은 유형을 사용할 수 있습니다. • **dns** • **ftp** • **h323** • **http** • **im** • **scansafe** • **sip**
class_map_name	최대 길이 40자로 클래스 맵 이름을 지정합니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.
match-all	(선택 사항) 트래픽이 모든 기준에 부합해야 클래스 맵과 매칭할 수 있다고 지정합니다. 어떤 옵션도 지정하지 않을 경우 **match-all**이 기본 설정입니다.
match-any	(선택 사항) 트래픽이 하나 이상의 기준에 부합하면 클래스 맵과 매칭할 수 있다고 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
8.0(2)	**match-any** 키워드를 추가했습니다.

사용 지침

Modular Policy Framework에서는 여러 애플리케이션 검사를 위해 특별한 작업을 구성할 수 있습니다. 레이어 3/4 정책 맵에서 검사 엔진을 활성화할 때 *검사 정책 맵*에 정의된 작업을 선택적으로 활성화할 수도 있습니다(**policy-map type inspect** 명령 참조).

검사 정책 맵에서는 검사 클래스 맵을 만들어 작업을 수행할 트래픽을 식별할 수 있습니다. 클래스 맵은 하나 이상의 **match** 명령으로 구성됩니다. 또는 하나의 기준과 작업을 짝짓고 싶다면 검사 정책 맵에서 직접 **match** 명령을 사용할 수도 있습니다. 어떤 애플리케이션과 관련된 기준을 매칭할 수 있습니다. 예를 들어 DNS 트래픽의 경우 DNS 쿼리에서 도메인 이름을 맞춰볼 수 있습니다.

하나의 클래스 맵에서 여러 트래픽 일치를 그룹화하거나(match-all 클래스 맵), 일치 리스트 중 하나를 확인할 수 있습니다(match-any 클래스 맵). 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 여러 일치 명령을 그룹화하고 클래스 맵을 재사용할 수 있다는 점입니다. 이 클래스 맵에서 식별하는 트래픽에 대해, 검사 정책 맵에서 연결의 삭제, 재설정 및/또는 기록 등의 작업을 지정할 수 있습니다.

모든 유형을 포괄하여 클래스 맵의 최대 개수는 단일 모드에서 또는 다중 모드의 컨텍스트당 255개입니다. 클래스 맵에는 다음 유형이 포함됩니다.

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** 명령: 정책 맵 유형 검사 컨피그레이션 모드

이 한도에는 모든 유형의 기본 클래스 맵도 포함됩니다. 자세한 내용은 **class-map** 명령을 참조하십시오.

예

다음 예는 모든 기준과 일치해야 하는 HTTP 클래스 맵을 만듭니다.

```
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
```

다음 예는 기준 중 하나와 일치하면 되는 HTTP 클래스 맵을 만듭니다.

```
ciscoasa(config-cmap)# class-map type inspect http match-any monitor-http
ciscoasa(config-cmap)# match request method get
ciscoasa(config-cmap)# match request method put
ciscoasa(config-cmap)# match request method post
```

관련 명령

명령	설명
class-map	통과 트래픽을 위한 레이어 3/4 클래스 맵을 만듭니다.
policy-map	트래픽 클래스를 하나 이상의 작업과 연결하여 정책 맵을 생성합니다.
policy-map type inspect	애플리케이션 검사를 위한 특별한 작업을 정의합니다.
service-policy	정책 맵을 하나 이상의 인터페이스와 연결하여 보안 정책을 생성합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

class-map type management

Modular Policy Framework를 사용할 때 글로벌 컨피그레이션 모드에서 **class-map type management** 명령을 사용하여 작업을 적용할, ASA로 향하는 레이어 3 또는 4 관리 트래픽을 식별합니다. 클래스 맵을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

class-map type management *class_map_name*

no class-map type management *class_map_name*

구문 설명

class_map_name	최대 길이 40자로 클래스 맵 이름을 지정합니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
8.0(2)	레이어 3/4 관리 클래스 맵에서 **et connection** 명령을 to-the-ASA 관리 트래픽을 위해 사용할 수 있습니다. **conn-max** 및 **embryonic-conn-max** 키워드만 사용 가능합니다.

사용 지침

이 클래스 맵 유형은 관리 트래픽 전용입니다. 통과 트래픽에 대해서는 **class-map** 명령(**type** 키워드 없음)을 참조하십시오.

ASA로 이동하는 관리 트래픽에 대해서는 이 종류의 트래픽에만 해당하는 작업을 수행할 수 있습니다. 정책 맵의 관리 클래스 맵에 사용할 수 있는 작업의 유형은 관리 트래픽에 맞게 특화되어 있습니다. 예를 들어, 이 유형의 클래스 맵에서는 RADIUS 어카운팅 트래픽을 검사하고 연결 한도를 설정할 수 있습니다.

Layer 3/4 클래스 맵은 작업을 적용할 Layer 3 및 4 트래픽을 식별합니다. 모든 유형을 포괄하여 클래스 맵의 최대 개수는 단일 모드에서 또는 다중 모드의 컨텍스트당 255개입니다.

각 Layer 3/4 정책 맵에 대해 여러 Layer 3/4 클래스 맵(관리 또는 통과 트래픽)을 만들 수 있습니다.

Modular Policy Framework의 컨피그레이션은 4가지 작업으로 구성됩니다.

1. **class-map** 및 **class-map type management** 명령을 사용하여 작업을 적용하려는 레이어 3 및 레이어 4 트래픽을 식별합니다.
2. (애플리케이션 검사만) **policy-map type inspect** 명령을 사용하여 애플리케이션 검사 트래픽을 위한 특별한 작업을 정의합니다.
3. **policy-map** 명령을 사용하여 레이어 3 및 4 트래픽에 작업을 적용합니다.
4. **service-policy** 명령을 사용하여 인터페이스에서 작업을 활성화합니다.

class-map 컨피그레이션 모드를 시작하려면 **class-map type management** 명령을 사용합니다. class-map 컨피그레이션 모드에서 **match** 명령을 사용하여 클래스에 포함할 트래픽을 정의할 수 있습니다. 액세스 목록, TCP 또는 UDP 포트와 매칭할 관리 클래스 맵을 지정할 수 있습니다. 레이어 3/4 클래스 맵은 클래스 맵에 포함되는 트래픽을 식별하는 **match** 명령을 최대 1개 포함합니다.

모든 유형을 포괄하여 클래스 맵의 최대 개수는 단일 모드에서 또는 다중 모드의 컨텍스트당 255개입니다. 클래스 맵에는 다음 유형이 포함됩니다.

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** 명령: 정책 맵 유형 검사 컨피그레이션 모드

이 한도에는 모든 유형의 기본 클래스 맵도 포함됩니다. 자세한 내용은 **class-map** 명령을 참조하십시오.

예

다음 예에서는 레이어 3/4 관리 클래스 맵을 만듭니다.

```
ciscoasa(config)# class-map type management radius_acct
ciscoasa(config-cmap)# match port tcp eq 10000
```

관련 명령

명령	설명
class-map	통과 트래픽을 위한 레이어 3/4 클래스 맵을 만듭니다.
policy-map	트래픽 클래스를 하나 이상의 작업과 연결하여 정책 맵을 생성합니다.
policy-map type inspect	애플리케이션 검사를 위한 특별한 작업을 정의합니다.
service-policy	정책 맵을 하나 이상의 인터페이스와 연결하여 보안 정책을 생성합니다.
show running-config class-map	클래스 맵 컨피그레이션에 대한 정보를 표시합니다.

class-map type regex

Modular Policy Framework를 사용할 때 글로벌 컨피그레이션 모드에서 **class-map type regex** 명령을 사용하여 매칭 텍스트와 함께 사용할 정규식을 그룹화합니다. 정규식을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

class-map type regex match-any *class_map_name*

no class-map [type regex match-any] *class_map_name*

구문 설명

class_map_name	최대 길이 40자로 클래스 맵 이름을 지정합니다. "class-default"라는 이름 그리고 "_internal" 또는 "_default"로 시작하는 모든 이름은 예약되어 있습니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.
match-any	트래픽이 정규식 중 단 하나에 부합할 경우 클래스 맵과 매칭한다고 지정합니다. **match-any**가 유일한 옵션입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

Modular Policy Framework에서는 여러 애플리케이션 검사를 위해 특별한 작업을 구성할 수 있습니다. 레이어 3/4 정책 맵에서 검사 엔진을 활성화할 때 *검사 정책 맵*에 정의된 작업을 선택적으로 활성화할 수도 있습니다(**policy-map type inspect** 명령 참조).

검사 정책 맵에서 하나 이상의 **match** 명령을 포함하는 검사 클래스 맵을 만들어 작업을 수행할 트래픽을 식별하거나 검사 정책 맵에서 직접 **match** 명령을 사용할 수 있습니다. 일부 **match** 명령은 정규식을 사용하여 패킷의 텍스트를 식별할 수 있게 합니다. 예를 들어, HTTP 패킷에 포함된 URL 문자열과 매칭할 수 있습니다. 정규식 클래스 맵에서 정규식을 그룹화할 수 있습니다.

정규식 클래스 맵을 만들기 전에 **regex** 명령을 사용하여 정규식을 만듭니다. 그런 다음 클래스 맵 컨피그레이션 모드에서 **match regex** 명령을 사용하여 명명된 정규식을 식별합니다.

모든 유형을 포괄하여 클래스 맵의 최대 개수는 단일 모드에서 또는 다중 모드의 컨텍스트당 255개입니다. 클래스 맵에는 다음 유형이 포함됩니다.

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** 명령: 정책 맵 유형 검사 컨피그레이션 모드

이 한도에는 모든 유형의 기본 클래스 맵도 포함됩니다. 자세한 내용은 **class-map** 명령을 참조하십시오.

예

다음 예에서는 정규식 2개를 만들어 정규식 클래스 맵에 추가합니다. "example.com" 또는 "example2.com" 문자열이 포함되어 있으면 트래픽이 클래스 맵과 일치합니다.

```
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
```

관련 명령

명령	설명
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	트래픽 클래스를 하나 이상의 작업과 연결하여 정책 맵을 생성합니다.
policy-map type inspect	애플리케이션 검사를 위한 특별한 작업을 정의합니다.
service-policy	정책 맵을 하나 이상의 인터페이스와 연결하여 보안 정책을 생성합니다.
regex	정규식을 만듭니다.

clear aaa kerberos

ASA에서 모든 Kerberos 티켓 정보를 지우려면 webvpn 컨피그레이션 모드에서 **clear aaa kerberos** 명령을 사용합니다.

[cluster exec] clear aaa kerberos [username *user* **| host** *ip* **|** *hostname***]**

구문 설명

cluster exec	(선택 사항) 클러스터링 환경에서는 한 유닛에서 **clear aaa kerberos** 명령을 보내고 다른 모든 유닛에서 동시에 이 명령을 실행할 수 있습니다.
host	Kerberos 티켓에서 지울 호스트를 지정합니다.
hostname	호스트 이름을 지정합니다.
ip	호스트의 IP 주소를 지정합니다.
username	Kerberos 티켓에서 지울 사용자를 지정합니다.

기본값

이 명령은 기본 설정이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	**cluster exec** 옵션을 추가했습니다.

사용 지침

webvpn 컨피그레이션 모드에서 **clear aaa kerberos** 명령을 사용하여 ASA에 캐싱된 모든 Kerberos 티켓을 지울 수 있습니다. 특정 사용자 또는 호스트의 Kerberos 티켓을 지우려면 **username** 및 **host** 키워드를 사용합니다.

예

다음 예에서는 **clear aaa kerberos** 명령의 사용을 보여줍니다.

```
ciscoasa(config)# clear aaa kerberos
```

관련 명령

명령	설명
show aaa kerberos	ASA에 캐싱된 모든 Kerberos 티켓을 표시합니다.

clear aaa local user fail-attempts

사용자 잠금 상태를 수정하지 않고 사용자 인증 시도 실패 횟수를 0으로 재설정하려면 특별 권한 EXEC 모드에서 **clear aaa local user fail-attempts** 명령을 사용합니다.

[cluster exec] clear aaa local user authentication fail-attempts {username *name* **| all}**

구문 설명

all	모든 사용자에게 실패한 시도 카운터를 0으로 재설정합니다.
cluster exec	(선택 사항) 클러스터링 환경에서는 한 유닛에서 **clear aaa local user authentication fail-attempts** 명령을 보내고 다른 모든 유닛에서 동시에 이 명령을 실행할 수 있습니다.
name	실패한 시도 카운터를 0으로 재설정할 사용자 이름을 지정합니다.
username	다음에 오는 매개변수가 실패한 시도 카운터를 0으로 재설정할 사용자 이름임을 나타냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	**cluster exec** 옵션을 추가했습니다.

사용 지침

사용자가 몇 차례 시도로 인증하지 못할 경우 이 명령을 사용합니다.

구성된 인증 시도 실패 횟수가 지나면 사용자는 시스템에서 잠기게 되며 시스템 관리자가 사용자 이름의 잠금을 해제하거나 시스템이 재부팅할 때까지 로그인할 수 없습니다. 사용자가 성공적으로 인증하거나 ASA가 재부팅되면 실패 횟수가 0으로, 잠금 상태가 No로 재설정됩니다. 또한 컨피그레이션이 최근 수정되었다면 카운터는 0으로 재설정됩니다.

사용자 이름을 잠그거나 잠금 해제하면 시스템 로그 메시지가 생성됩니다. 권한 레벨이 15인 시스템 관리자는 잠겨질 수 없습니다.

예

다음 예에서는 anyuser라는 사용자 이름에 대해 시도 실패 카운터를 0으로 재설정하기 위해 **clear aaa local user authentication fail-attempts** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# clear aaa local user authentication fail-attempts username anyuser
ciscoasa(config)#
```

다음 예에서는 모든 사용자에 대해 시도 실패 카운터를 0으로 재설정하기 위해 **clear aaa local user authentication fail-attempts** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# clear aaa local user authentication fail-attempts all
ciscoasa(config)#
```

관련 명령

명령	설명
aaa local authentication attempts max-fail	사용자 인증 시도 실패 횟수의 허용 한도를 구성합니다.
clear aaa local user lockout	사용자 잠금 상태를 수정하지 않고 사용자 인증 시도의 실패 횟수를 0으로 재설정합니다.
show aaa local user [locked]	현재 잠겨 있는 사용자 이름의 목록을 표시합니다.

clear aaa local user lockout

지정된 사용자의 잠금 상태를 해제하고 시도 실패 카운터를 0으로 설정하려면 특별 권한 EXEC 모드에서 **clear aaa local user lockout** 명령을 사용합니다.

[cluster exec] clear aaa local user lockout {username *name* **| all}**

구문 설명

all	모든 사용자에게 실패한 시도 카운터를 0으로 재설정합니다.
cluster exec	(선택 사항) 클러스터링 환경에서는 한 유닛에서 **clear aaa local user lockout** 명령을 보내고 다른 모든 유닛에서 동시에 이 명령을 실행할 수 있습니다.
name	실패한 시도 카운터를 0으로 재설정할 사용자 이름을 지정합니다.
username	다음에 오는 매개변수가 실패한 시도 카운터를 0으로 재설정할 사용자 이름임을 나타냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	**cluster exec** 옵션을 추가했습니다.

사용 지침

username 옵션으로 단일 사용자 또는 **all** 옵션으로 모든 사용자를 지정할 수 있습니다.

이 명령은 잠겨진 사용자의 상태에만 적용됩니다.

관리자는 디바이스에서 잠겨질 수 없습니다.

사용자 이름을 잠그거나 잠금 해제하면 syslog 메시지가 생성됩니다.

예

다음 예에서는 anyuser라는 사용자 이름에 대해 잠금 조건을 해제하고 시도 실패 카운터를 0으로 재설정하기 위해 **clear aaa local user lockout** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# clear aaa local user lockout username anyuser
ciscoasa(config)#
```

관련 명령

명령	설명
aaa local authentication attempts max-fail	사용자 인증 시도 실패 횟수의 허용 한도를 구성합니다.
clear aaa local user fail-attempts	사용자 잠금 상태를 수정하지 않고 사용자 인증 시도의 실패 횟수를 0으로 재설정합니다.
show aaa local user [locked]	현재 잠겨 있는 사용자 이름의 목록을 표시합니다.

clear aaa-server statistics

AAA 서버의 통계를 재설정하려면 특별 권한 EXEC 모드에서 **clear aaa-server statistics** 명령을 사용합니다.

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

구문 설명

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

기본값

모든 그룹에서 모든 AAA 서버 통계를 제거합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	CLI 지침을 준수하기 위해 명령을 수정했습니다. 프로토콜 값에서 **nt**가 기존의 **nt-domain**을, **sdi**가 기존의 **rsa-ace**를 대체했습니다.

예

다음 예에서는 그룹의 특정 서버에 대해 AAA 통계를 재설정하는 방법을 보여줍니다.

```
ciscoasa(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

다음 예에서는 어떤 서버 그룹의 전체에 대해 AAA 통계를 재설정하는 방법을 보여줍니다.

```
ciscoasa(config)# clear aaa-server statistics svrgrp1
```

다음 예에서는 모든 서버 그룹에 대해 AAA 통계를 재설정하는 방법을 보여줍니다.

```
ciscoasa(config)# clear aaa-server statistics
```

다음 예에서는 특정 프로토콜(여기서는 TACACS+)에 대해 AAA 통계를 재설정하는 방법을 보여줍니다.

```
ciscoasa(config)# clear aaa-server statistics protocol tacacs+
```

관련 명령

명령	설명
aaa-server protocol	AAA 서버 연결 데이터의 그룹을 지정하고 관리합니다.
clear configure aaa-server	기본이 아닌 AAA 서버 그룹을 모두 제거하거나 지정된 그룹을 지웁니다.
show aaa-server	AAA 서버 통계를 표시합니다.
show running-config aaa-server	현재 AAA 서버 컨피그레이션의 값을 표시합니다.

clear access-list

액세스 목록 카운터를 지우려면 글로벌 컨피그레이션 모드에서 **clear access-list** 명령을 사용합니다.

clear access-list *id* **counters**

구문 설명

counters	액세스 목록 카운터를 지웁니다.
id	액세스 목록의 이름 또는 번호.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear access-list 명령을 입력할 때 카운터를 지울 액세스 목록의 *id*를 지정해야 합니다.

예

다음 예에서는 특정 액세스 목록 카운터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear access-list inbound counters
```

관련 명령

명령	설명
access-list extended	컨피그레이션에 액세스 목록을 추가하고 방화벽을 지나는 IP 트래픽에 대한 정책을 구성합니다.
access-list standard	OSPF 경로의 목적지 IP 주소를 식별하기 위해 액세스 목록을 추가합니다. 이는 경로 맵에서 OSPF 재배포에 사용할 수 있습니다.
clear configure access-list	실행 중인 컨피그레이션에서 액세스 목록을 지웁니다.
show access-list	액세스 목록 엔트리를 번호별로 표시합니다.
show running-config access-list	ASA에서 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

clear arp

동적 ARP 엔트리 또는 ARP 통계를 지우려면 특별 권한 EXEC 모드에서 **clear arp** 명령을 사용합니다.

clear arp [statistics]

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 모든 ARP 통계를 지웁니다.

```
ciscoasa# clear arp statistics
```

관련 명령

명령	설명
arp	고정 ARP 항목을 추가합니다.
arp-inspection	투명 방화벽 모드에서 ARP 스푸핑을 방지하기 위해 ARP 패킷을 검사합니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config arp	ARP 시간 초과의 현재 컨피그레이션을 표시합니다.

clear asp drop

ASP(가속 보안 경로) 삭제 통계를 지우려면 특별 권한 EXEC 모드에서 **clear asp drop** 명령을 사용합니다.

clear asp drop [flow *type* **| frame** *type***]**

구문 설명

flow	(선택 사항) 삭제된 플로우 통계를 지웁니다.
frame	(선택 사항) 삭제된 패킷 통계를 지웁니다.
type	(선택 사항) 특정 프로세스에 대해 삭제된 플로우 또는 패킷 통계를 지웁니다.

기본값

기본적으로 이 명령은 모든 삭제 통계를 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

다음과 같은 프로세스 유형이 있습니다.

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
```

```
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

예

다음 예에서는 모든 삭제 통계를 지웁니다.

```
ciscoasa# clear asp drop
```

관련 명령

명령	설명
show asp drop	삭제된 패킷의 ASP 카운터를 표시합니다.

clear asp load-balance history

패킷별 ASP 로드 밸런싱 기록을 지우고 자동 켜기/끄기 횟수를 재설정하려면 특별 권한 EXEC 모드에서 **clear asp load-balance history** 명령을 사용합니다.

clear asp load-balance history

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 패킷별 ASP 로드 밸런싱 기록을 지우고 자동 켜기/끄기 횟수를 재설정합니다. ASA 5585-X 및 ASASM에서만 이 명령을 사용할 수 있습니다.

예

다음 예에서는 패킷별 ASP 로드 밸런싱 기록을 지우고 자동 켜기/끄기 횟수를 재설정합니다.

```
ciscoasa# clear asp load-balance history
```

관련 명령

명령	설명
asp load-balance per-packet	로드 밸런싱 동작을 변경합니다.
show asp load-balance	로드 밸런서 큐 크기를 히스토그램으로 표시합니다.
show asp load-balance per-packet	현재 상태, 상위/하위 워터마크, 전역 임계값을 표시합니다.
show asp load-balance per-packet history	현재 상태, 상위/하위 워터마크, 전역 임계값, 최근 재설정 후 패킷별 ASP 로드 밸런싱을 켜고 끈 횟수, 패킷별 ASP 로드 밸런싱 기록(타임스탬프 포함), 켜고 끈 사유를 표시합니다.

clear asp table

ASP ARP 테이블, ASP 분류 테이블 또는 둘 다의 계수기를 지우려면 특별 권한 EXEC 모드에서 **clear asp table** 명령을 사용합니다.

clear asp table [arp | classify]

구문 설명

arp	ASP ARP 테이블에서만 계수기를 지웁니다.
classify	ASP 분류 테이블에서만 계수기를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(4)	이 명령을 도입했습니다.

사용 지침

arp와 **classify**의 2가지 옵션만 **clear asp table** 명령에서 계수됩니다.

예

다음 예에서는 모든 ASP 테이블 통계를 지웁니다.

```
ciscoasa# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! ciscoasa#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands! ciscoasa#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! ciscoasa(config)# clear
asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! ciscoasa# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

관련 명령

명령	설명
show asp table arp	ASP의 내용을 표시합니다. 문제 해결에 도움이 될 수 있습니다.

clear asp table filter

ASP 필터 테이블 엔트리에 대한 계수기를 지우려면 특별 권한 EXEC 모드에서 **clear asp table filter** 명령을 사용합니다.

clear asp table filter [access-list *acl-name*]

구문 설명

acl-name	지정된 액세스 목록의 계수기만 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

access-list 옵션만 **clear asp table filter** 명령에서 계수됩니다.

예

다음 예에서는 모든 ASP 필터 테이블 통계를 지웁니다.

```
ciscoasa# clear asp table filter
```

관련 명령

명령	설명
show asp table arp	ASP의 내용을 표시합니다. 문제 해결에 도움이 될 수 있습니다.

clear bgp

하드 또는 소프트 리컨피그레이션을 토해 BGP(Border Gateway Protocol) 연결을 재설정하려면 특별 권한 EXEC 모드에서 clear bgp 명령을 사용합니다.

다중 모드- 시스템 컨텍스트

clear bgp *

다중 모드- 사용자 컨텍스트/단일 모드

clear bgp {* [ipv4 {unicast} [in | out | soft [in | out]] |*autonomous-system-number* | *neighbor-address* **} [in | out | soft [in | out]]**

구문 설명

*	모든 현재 BGP 세션이 재설정되도록 지정합니다.
autonomous-system-number	모든 BGP 피어 세션이 재설정될 자율 시스템 번호. 1~65535 범위의 숫자입니다. 4바이트 자율 시스템 번호의 지원 범위는 asplain 표기법에서 65536~4294967295, asdot 표기법에서는 1.0~65535.65535입니다. 자율 시스템 번호 형식에 대한 자세한 내용은 router bgp 명령을 참조하십시오.
neighbor-address	식별된 BGP 네이버만 재설정되도록 지정합니다. 이 인수의 값으로는 IPv4 또는 IPv6 주소가 가능합니다.
in	(선택 사항) 인바운드 리컨피그레이션을 시작합니다. in 및 out 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
out	(선택 사항) 인바운드 또는 아웃바운드 리컨피그레이션을 시작합니다. in 및 out 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
soft	(선택 사항) 저속 피어(slow-peer) 상태를 강제로 해제하고 원래의 업데이트 그룹으로 이동합니다.
ipv4	IPv4 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션을 통해 BGP 연결을 재설정합니다.
unicast	(선택 사항) 유니캐스트 주소군 세션을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

clear bgp 명령을 사용하여 하드 리셋 또는 소프트 리컨피그레이션을 시작할 수 있습니다. 하드 리셋은 지정된 피어링 세션을 해제하고 재구성하며 BGP 라우팅 테이블을 재구성합니다. 소프트 리컨피그레이션은 기존 피어링 세션을 해제하지 않고 저장된 접두사 정보를 사용하여 BGP 라우팅 테이블을 재구성하고 활성화합니다. 소프트 리컨피그레이션에서는 저장된 업데이트 정보를 사용하므로 메모리를 추가로 사용합니다. 이와 같이 업데이트를 저장함으로써 네트워크 중단 없이 새 BGP 정책을 적용할 수 있습니다. 소프트 리컨피그레이션은 인바운드 또는 아웃바운드 세션에 대해 구성할 수 있습니다.

1. 다중 모드- 시스템 컨텍스트

```
ciscoasa(config)# clear bgp *


This command will reset BGP in all contexts.
Are you sure you want to continue ? [no]:
```

2. 단일 모드/다중 모드- 사용자 컨텍스트

```
ciscoasa/c1(config)# clear bgp ?
```

exec 모드 명령/옵션

```
  *               Clear all peers
  <1-4294967295>  Clear peers with the AS number
  <1.0-XX.YY>     Clear peers with the AS number
  A.B.C.D         BGP neighbor address to clear
  external        Clear all external peers
  ipv4            Address family
  table-map       Update BGP table-map configuration
```

예

1. 다음 예에서는 시스템 컨텍스트에서 clear bgp 명령이 실행되어 모든 컨텍스트의 모든 bgp 세션이 재설정됩니다. 이 명령이 모든 bgp 세션을 재설정할 것임을 확인하는 경고 메시지가 나타납니다.

```
ciscoasa# clear bgp ?
  *  Clear all peers
ciscoasa# clear bgp *


This command will reset BGP in ALL contexts.
Are you sure you want to continue? [no]:
```

2. 다음 예에서는 단일 모드 또는 다중 모드 사용자 컨텍스트에서 모든 bgp 세션이 재설정됩니다. 단일 모드/사용자 컨텍스트에서는 이 작업을 확인하는 어떤 경고도 표시되지 않습니다.

```
ciscoasa# clear bgp * (Single mode)
ciscoasa/c1(config)# clear bgp * (Multiple mode user context)
```

3. 다음 예에서는 네이버 10.100.0.1과의 인바운드 세션에 대해 소프트 리컨피그레이션이 시작되며 아웃바운드 세션은 영향을 받지 않습니다.

```
ciscoasa(config)# clear bgp 10.100.0.1 soft in (Single mode)
ciscoasa/c1(config)# clear bgp 10.100.0.1 soft in (Multiple mode user context)
```

4. 다음 예에서는 BGP 네이버 라우터에서 경로 새로 고침 기능이 활성화되고 네이버 172.16.10.2와의 인바운드 세션에 대해 소프트 리컨피그레이션이 시작되며 아웃바운드 세션은 영향을 받지 않습니다.

```
ciscoasa(config)# clear bgp 172.16.10.2 in (Single mode)
ciscoasa/c1(config)# clear bgp 172.16.10.2 in (Multiple mode user context)
```

5. 다음 예에서는 자율 시스템 번호 35700을 갖는 모든 라우터와의 세션에 대해 하드 리셋이 시작됩니다.

```
ciscoasa(config)# clear bgp 35700 (Single mode)
ciscoasa/c1(config)# clear bgp 35700 (Multiple mode user context)
```

관련 명령

명령	설명
clear bgp external	하드 또는 소프트 리컨피그레이션을 통해 eBGP(external Border Gateway Protocol) 피어링 세션을 재설정합니다.
clear bgp ipv4	IPv4 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션으로 BGP 연결을 재설정합니다.
clear bgp table-map	BGP 라우팅 테이블에서 테이블-맵 컨피그레이션 정보를 새로 고칩니다.

clear bgp external

하드 또는 소프트 리컨피그레이션을 통해 eBGP 피어링 세션을 재설정하려면 특별 권한 EXEC 모드에서 clear bgp external 명령을 사용합니다.

clear bgp external [in |out | soft [in|out] | ipv4 {unicast} [in | out | soft [in | out]]

구문 설명

in	(선택 사항) 인바운드 리컨피그레이션을 시작합니다. in 및 out 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
out	(선택 사항) 인바운드 또는 아웃바운드 리컨피그레이션을 시작합니다. in 및 out 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
soft	(선택 사항) 저속 피어(slow-peer) 상태를 강제로 해제하고 원래의 업데이트 그룹으로 이동합니다.
ipv4	IPv4 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션을 통해 BGP 연결을 재설정합니다.
unicast	(선택 사항) 유니캐스트 주소군 세션을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

clear bgp external 명령은 eBGP 네이버 세션에 대한 하드 리셋 또는 소프트 리컨피그레이션을 시작하는 데 사용할 수 있습니다. 하드 리셋은 지정된 피어링 세션을 해제하고 재구성하며 BGP 라우팅 테이블을 재구성합니다. 소프트 리컨피그레이션은 기존 피어링 세션을 해제하지 않고 저장된 접두사 정보를 사용하여 BGP 라우팅 테이블을 재구성하고 활성화합니다. 소프트 리컨피그레이션에서는 저장된 업데이트 정보를 사용하므로 메모리를 추가로 사용합니다. 이와 같이 업데이트를 저장함으로써 네트워크 중단 없이 새 BGP 정책을 적용할 수 있습니다. 소프트 리컨피그레이션은 인바운드 또는 아웃바운드 세션에 대해 구성할 수 있습니다.

이 명령은 시스템 컨텍스트에서는 작동하지 않습니다.

예

다음 예에서는 모든 인바운드 eBGP 피어링 세션에 대해 소프트 리컨피그레이션이 구성됩니다.

```
ciscoasa(config)# clear bgp external soft in (Single mode)
ciscoasa/c1(config clear bgp external soft in (Multiple mode user context)
```

다음 예에서는 모든 아웃바운드 주소군 IPv4 멀티캐스트 eBGP 피어링 세션이 지워집니다.

```
ciscoasa(config)# clear bgp external ipv4 multicast out (Single mode)
ciscoasa/c1(config)# clear bgp external ipv4 multicast out (Multiple mode user context)
```

관련 명령

명령	설명
clear bgp	하드 또는 소프트 리컨피그레이션을 통해 BGP 피어링 세션을 재설정합니다.
clear bgp ipv4	IPv4 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션으로 BGP 연결을 재설정합니다.
clear bgp table-map	BGP 라우팅 테이블에서 테이블-맵 컨피그레이션 정보를 새로 고칩니다.

clear bgp ipv4

IPv4 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션을 통해 BGP 피어링 세션을 재설정하려면 특별 권한 EXEC 모드에서 **clear bgp ipv4** 명령을 사용합니다.

clear bgp ipv4 unicast {autonomous-system-number [in |out | soft [in|out]}

구문 설명

autonomous-system-number	모든 BGP 피어 세션이 재설정될 자율 시스템 번호. 1~65535 범위의 숫자입니다. 4바이트 자율 시스템 번호의 지원 범위는 asplain 표기법에서 65536~4294967295, asdot 표기법에서는 1.0~65535.65535입니다. 자율 시스템 번호 형식에 대한 자세한 내용은 router bgp 명령을 참조하십시오.
in	(선택 사항) 인바운드 리컨피그레이션을 시작합니다. in 및 out 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
out	(선택 사항) 인바운드 또는 아웃바운드 리컨피그레이션을 시작합니다. in 및 out 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
soft	(선택 사항) 저속 피어(slow-peer) 상태를 강제로 해제하고 원래의 업데이트 그룹으로 이동합니다.
unicast	(선택 사항) 유니캐스트 주소군 세션을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

clear bgp ipv4 명령을 사용하여 하드 리셋 또는 소프트 리컨피그레이션을 시작할 수 있습니다. 하드 리셋은 지정된 피어링 세션을 해제하고 재구성하며 BGP 라우팅 테이블을 재구성합니다. 소프트 리컨피그레이션은 기존 피어링 세션을 해제하지 않고 저장된 접두사 정보를 사용하여 BGP 라우팅 테이블을 재구성하고 활성화합니다. 소프트 리컨피그레이션에서는 저장된 업데이트 정보를 사용하므로 메모리를 추가로 사용합니다. 이와 같이 업데이트를 저장함으로써 네트워크 중단 없이 새 BGP 정책을 적용할 수 있습니다. 소프트 리컨피그레이션은 인바운드 또는 아웃바운드 세션에 대해 구성할 수 있습니다.

이 명령은 시스템 컨텍스트에서는 작동하지 않습니다.

예

1. 다음 예에서는 자율 시스템 65400, IPv4 유니캐스트 주소군 세션에 속하는 BGP 네이버와의 인바운드 세션에 대해 소프트 리컨피그레이션이 시작됩니다. 아웃바운드 세션은 영향을 받지 않습니다.

```
ciscoasa(config)# clear bgp ipv4 unicast 65400 soft in (Single mode)
ciscoasa/c1(config)# clear bgp ipv4 unicast 65400 soft in (Multiple mode user context)
```

2. 다음 예에서는 asplain 표기법 4바이트 자율 시스템 번호가 65538이고 IPv4 유니캐스트 주소군 세션에 속하는 BGP 네이버에 대해 하드 리셋이 시작됩니다.

```
ciscoasa(config)# clear bgp ipv4 unicast 65538 (Single mode)
ciscoasa/c1(config)# clear bgp ipv4 unicast 65538 (Multiple mode user context)
```

3. 다음 예에서는 asdot 표기법 4바이트 자율 시스템 번호가 1.2이고 IPv4 유니캐스트 주소군 세션에 속하는 BGP 네이버에 대해 하드 리셋이 시작됩니다.

```
ciscoasa(config)# clear bgp ipv4 unicast 1.2 (Single mode)
ciscoasa/c1(config)# clear bgp ipv4 unicast 1.2 (Multiple mode user context)
```

관련 명령

명령	설명
clear bgp	하드 또는 소프트 리컨피그레이션을 통해 BGP 피어링 세션을 재설정합니다.
clear bgp external	하드 또는 소프트 리컨피그레이션을 통해 eBGP 연결을 재설정합니다.
clear bgp table-map	BGP 라우팅 테이블에서 테이블-맵 컨피그레이션 정보를 새로 고칩니다.

clear bgp table-map

BGP 라우팅 테이블에서 테이블-맵 컨피그레이션 정보를 새로 고치려면 특별 권한 EXEC 모드에서 **clear bgp table-map** 명령을 사용합니다.

clear bgp [ipv4 unicast] table-map

구문 설명

ipv4	(선택 사항) IPv4 주소군 세션에 대해 테이블-맵 컨피그레이션 정보를 새로 고칩니다.
unicast	(선택 사항) 유니캐스트 주소군 세션에 대해 테이블-맵 컨피그레이션 정보를 새로 고칩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

clear bgp table-map 명령은 BGP 라우팅 테이블에서 테이블-맵 컨피그레이션 정보를 지우거나 새로 고치는 데 사용합니다. BGP 정책 어카운팅 기능으로 구성했던 트래픽-색인 정보를 지우는 데 이 명령을 사용할 수 있습니다.

이 명령은 시스템 컨텍스트에서는 작동하지 않습니다.

예

1. 다음 예에서는 테이블 맵을 구성하고 트래픽 색인을 설정합니다. clear bgp table-map 명령을 입력한 다음 새 정책을 적용합니다.

```
ciscoasa(config)# route-map SET_BUCKET permit 10
ciscoasa (config-route-map)# match community 1
ciscoasa (config-route-map)# set origin incomplete
ciscoasa (config-route-map)# exit
ciscoasa (config)# router bgp 50000
ciscoasa (config-router)# address-family ipv4
ciscoasa (config-router-af)# table-map SET_BUCKET
ciscoasa (config-router-af)# end
ciscoasa # clear  bgp table-map
```

2. 다음 예에서는 IPv4 유니캐스트 피어링 세션에 대해 테이블 맵을 지웁니다.

```
ciscoasa # clear bgp ipv4 unicast table-map.
```

관련 명령

명령	설명
clear bgp	하드 또는 소프트 리컨피그레이션을 통해 BGP 피어링 세션을 재설정합니다.
clear bgp external	하드 또는 소프트 리컨피그레이션을 통해 eBGP 연결을 재설정합니다.
clear bgp ipv4	IPv4 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션으로 BGP 피어링 세션을 재설정합니다.

clear blocks

최저 수위와 같은 패킷 버퍼 카운터와 기록 정보를 재설정하려면 특별 권한 EXEC 모드에서 **clear blocks** 명령을 사용합니다.

clear blocks [snapshot | history]

구문 설명

history	모든 스냅샷의 기록을 지웁니다.
snapshot	모든 스냅샷을 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.1(5)	**history** 및 **snapshot** 옵션을 추가했습니다.

사용 지침

각 풀에서 최저 수위 카운터를 현재 사용 가능 블록으로 재설정합니다. 또한 이 명령은 마지막 버퍼 할당 실패 과정에서 저장된 기록 정보를 지웁니다.

예

다음 예에서는 블록을 지웁니다.

```
ciscoasa# clear blocks
```

관련 명령

명령	설명
blocks	블록 진단에 할당된 메모리를 늘립니다.
show blocks	시스템 버퍼 사용률을 표시합니다.

clear-button

WebVPN 사용자가 ASA에 연결할 때 표시되는 WebVPN 페이지 로그인 필드의 Clear 버튼을 사용자 지정하려면 사용자 지정 컨피그레이션 모드에서 **clear-button** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

clear-button {**text** | **style**} *value*

no clear-button [{**text** | **style**}] *value*

구문 설명

style	스타일을 변경하고 있음을 나타냅니다.
text	텍스트를 변경하고 있음을 나타냅니다.
value	표시할 실제 텍스트 또는 CSS 매개변수. 각각 최대 256자입니다.

기본값

기본 텍스트는 "Clear"입니다.

기본 스타일은 border:1px solid black;background-color:white;font-weight:bold;font-size:80%입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

style 옵션은 유효한 CSS 매개변수로 나타냅니다. 이 매개변수에 대한 설명은 본 설명서의 범위에 속하지 않습니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹 사이트(www.w3.org)의 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F는 편리한 CSS 매개변수 목록을 포함하고 있으며 www.w3.org/TR/CSS21/propidx.html에서 이용할 수 있습니다.

WebVPN 페이지 - 페이지 색상의 가장 대표적인 변경 방법에 대한 몇 가지 팁을 소개합니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 (HTML에서 인식된다면) 색상의 이름을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며, 각 색상(빨강, 녹색, 파랑)을 나타내는 0~255 범위의 10진수입니다. 쉼표로 구분하여 입력한 값은 해당 강도의 각 색상이 나머지 색상과 조합되는 것을 의미합니다.
- HTML 형식은 #000000이며, 6자리의 16진수입니다. 1번째와 2번째 자리는 빨강을, 3번째와 4번째 자리는 녹색을, 5번째와 6번째는 파랑을 나타냅니다.

참고 손쉽게 WebVPN 페이지를 사용자 지정하려면 ASDM을 사용하는 것이 좋습니다. 색 견본, 미리 보기 등 스타일 요소를 편리하게 구성할 수 있는 기능을 제공합니다.

예

다음 예에서는 Clear 버튼의 기본 배경색을 검정에서 파랑으로 변경합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# clear-button style background-color:blue
```

관련 명령

명령	설명
group-prompt	WebVPN 페이지 Login 필드의 그룹 프롬프트를 사용자 지정합니다.
login-button	WebVPN 페이지 Login 필드의 로그인 버튼을 사용자 지정합니다.
login-title	WebVPN 페이지 Login 필드의 제목을 사용자 지정합니다.
password-prompt	WebVPN 페이지 Login 필드의 비밀번호 프롬프트를 사용자 지정합니다.
username-prompt	WebVPN 페이지 Login 필드의 사용자 이름 프롬프트를 사용자 지정합니다.

clear capture

캡처 버퍼를 지우려면 특별 권한 EXEC 컨피그레이션 모드에서 **clear capture** *capture_name* 명령을 사용합니다.

clear capture *capture_name*

구문 설명

capture_name	패킷 캡처의 이름

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
특별 권한 EXEC	•	•	•	•	•

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

모든 패킷 캡처를 실수로 삭제할 위험을 방지하고자 **clear capture**의 축약 형태(예: **cl cap** 또는 **clear cap**)는 지원하지 않습니다.

예

이 예에서는 "example"이라는 캡처 버퍼를 지우는 방법을 보여줍니다.

```
ciscoasa(config)# clear capture example
```

관련 명령

명령	설명
capture	패킷 스니핑 및 네트워크 오류 격리를 위해 패킷 캡처 기능을 활성화합니다.
show capture	어떤 옵션도 지정되지 않으면 캡처 컨피그레이션을 표시합니다.

clear cluster info

클러스터 통계를 지우려면 특별 권한 EXEC 모드에서 **clear cluster info** 명령을 사용합니다.

clear cluster info {trace | transport}

구문 설명

trace	클러스터 이벤트 추적 정보를 지웁니다.
transport	클러스터 전송 통계를 지웁니다..

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

클러스터 통계를 보려면 **show cluster info** 명령을 사용합니다.

예

다음 예에서는 클러스터 이벤트 추적 정보를 지웁니다.

```
ciscoasa# clear cluster info trace
```

관련 명령

명령	설명
show cluster info	클러스터 통계를 표시합니다.

clear compression

모든 SVC 및 WebVPN 연결에 대한 압축 통계를 지우려면 특별 권한 EXEC 모드에서 **clear compression** 명령을 사용합니다.

clear compression {**all** | **svc** | **http-comp**}

구문 설명

all	모든 압축 통계를 지웁니다.
http-comp	HTTP-COMP 통계를 지웁니다.
svc	SVC 압축 통계를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

예

다음 예에서는 사용자에 대한 압축 컨피그레이션을 지웁니다.

```
hostname# clear configure compression
```

관련 명령

명령	설명
compression	모든 SVC 및 WebVPN 연결에 대한 압축을 활성화합니다.
svc compression	특정 그룹 또는 사용자에 대해 SVC 연결을 통한 데이터 압축을 활성화합니다.

6 장

clear configure ~ clear isakmp sa 명령

clear configuration session

컨피그레이션 세션을 삭제하려면 글로벌 컨피그레이션 모드에서 **clear configuration session** 명령을 사용합니다.

clear configuration session [*session_name*]

구문 설명

session_name	기존 컨피그레이션 세션의 이름. 현재 세션의 목록을 보려면 **show configuration session** 명령을 사용합니다. 이 매개변수를 생략하면 기존의 모든 세션이 삭제됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 ACL과 그 객체를 수정할 수 있는 별도의 세션을 만드는 **configure session** 명령과 함께 사용합니다. 생성한 세션이 더 이상 필요하지 않고 세션에서 정의한 변경 사항을 커밋하지 않으려는 경우 이 명령을 사용하여 세션 및 여기에 포함된 변경 사항을 제거합니다.

세션을 삭제하지 않고 그 세션에서 변경한 사항만 지우려는 경우 이 명령이 아니라 **clear session** 명령을 사용합니다.

예

다음 예에서는 old-session이라는 세션을 삭제합니다.

```
ciscoasa(config)# clear configuration session old-session
```

관련 명령

명령	설명
clear session	컨피그레이션 세션의 내용을 지우거나 그 액세스 플래그를 재설정합니다.
configure session	세션을 만들거나 엽니다.
show configuration session	현재 세션 각각에서 변경한 사항을 표시합니다.

clear configure

실행 중인 컨피그레이션을 지우려면 글로벌 컨피그레이션 모드에서 **clear configure** 명령을 사용합니다.

clear configure {primary | secondary | all | *command***}**

구문 설명

all	실행 중인 컨피그레이션 전체를 지웁니다.
command	지정된 명령에 대한 컨피그레이션을 지웁니다. 사용 가능한 명령을 보려면 **clear configure ?** 명령을 사용하여 CLI 도움말을 표시합니다.
primary	장애 조치 쌍의 경우 기본 유닛 컨피그레이션을 지웁니다.
secondary	장애 조치 쌍의 경우 보조 유닛 컨피그레이션을 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

보안 컨텍스트에서 이 명령을 입력하면 컨텍스트 컨피그레이션만 지웁니다. 시스템 실행 영역에서 이 명령을 입력할 경우 시스템 실행 컨피그레이션 및 모든 컨텍스트 실행 컨피그레이션을 지우게 됩니다. 시스템 컨피그레이션에서 모든 컨텍스트 엔트리를 지웠기 때문에(**context** 명령 참조) 그 컨텍스트는 더 이상 실행 중이 아닙니다. 그리고 컨텍스트 실행 영역은 변경할 수 없습니다.

컨피그레이션을 지우기 전에 **boot config** 명령(시작 컨피그레이션의 위치를 지정하는 명령)의 모든 변경 사항을 시작 컨피그레이션에 저장해야 합니다. 실행 중인 컨피그레이션에서만 시작 컨피그레이션 위치를 변경했다면 재시작할 때 컨피그레이션이 기본 위치로부터 로드됩니다.

참고 **clear configure all** 명령을 입력할 때 비밀번호 암호화에 사용된 마스터 패스프레이즈는 제거되지 않습니다. 마스터 패스프레이즈에 대한 자세한 내용은 **config key password-encryption** 명령을 참조하십시오.

예

다음 예에서는 실행 중인 컨피그레이션 전체를 지웁니다.

```
ciscoasa(config)# clear configure all
```

다음 예에서는 AAA 컨피그레이션을 지웁니다.

```
ciscoasa(config)# clear configure aaa
```

관련 명령

명령	설명
show running-config	실행 중인 컨피그레이션을 표시합니다.

clear conn

특정 연결 또는 여러 연결을 지우려면 특별 권한 EXEC 모드에서 **clear conn** 명령을 사용합니다.

clear conn [all] [protocol {tcp | udp}] [address *src_ip*[**-***src_ip*] **[netmask** *mask*]]
[port *src_port*[**-***src_port*]] **[address** *dest_ip*[**-***dest_ip*] **[netmask** *mask*]]
[port *dest_port*[**-***dest_port*] **[user [***domain_nickname*\]*user_name* **| user-group**
[*domain_nickname*\\]*user_group_name*] **| zone [***zone_name*]]

구문 설명

address	(선택 사항) 지정된 소스 또는 목적지 IP 주소와의 연결을 지웁니다.
all	(선택 사항) to-the-box 연결을 포함한 모든 연결을 지웁니다. **all** 키워드를 사용하지 않으면 through-the-box 연결만 지워집니다.
dest_ip	(선택 사항) 목적지 IP 주소(IPv4 또는 IPv6)를 지정합니다. 범위를 지정하려면 대시(-)로 IP 주소를 구분합니다. 예: `10.1.1.1-10.1.1.5`
dest_port	(선택 사항) 목적지 포트 번호를 지정합니다. 범위를 지정하려면 대시(-)로 포트 번호를 구분합니다. 예: `1000-2000`
netmask *mask*	(선택 사항) 해당 IP 주소로 사용할 서브넷 마스크를 지정합니다.
port	(선택 사항) 지정된 소스 또는 목적지 포트와의 연결을 지웁니다.
protocol {tcp | udp}	(선택 사항) 프로토콜 **tcp** 또는 **udp** 연결을 지웁니다.
src_ip	(선택 사항) 소스 IP 주소(IPv4 또는 IPv6)를 지정합니다. 범위를 지정하려면 대시(-)로 IP 주소를 구분합니다. 예: `10.1.1.1-10.1.1.5`
src_port	(선택 사항) 소스 포트 번호를 지정합니다. 범위를 지정하려면 대시(-)로 포트 번호를 구분합니다. 예: `1000-2000`
user [*domain_nickname*\]*user_name*	(선택 사항) 지정된 사용자에 속한 연결을 지웁니다. *domain_nickname* 인수를 포함하지 않으면 ASA는 기본 도메인에서 해당 사용자의 연결을 지웁니다.
user-group [*domain_nickname*\\]*user_group_name*	(선택 사항) 지정된 사용자 그룹에 속한 연결을 지웁니다. *domain_nickname* 인수를 포함하지 않으면 ASA는 기본 도메인에서 해당 사용자 그룹의 연결을 지웁니다.
zone [*zone_name*]	트래픽 영역에 속한 연결을 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(8)/7.2(4)/8.0(4)	이 명령을 도입했습니다.
8.4(2)	ID 방화벽을 지원하기 위해 **user** 및 **user-group** 키워드를 추가했습니다.
9.3(2)	**zone** 키워드를 추가했습니다.

사용 지침

이 명령은 IPv4 및 IPv6 주소를 지원합니다.

컨피그레이션에 대한 보안 정책을 변경하면 모든 *새* 연결에서는 새로운 보안 정책을 사용합니다. 기존 연결에서는 연결을 설정할 당시 구성된 정책을 계속 사용합니다. 모든 연결에서 새 정책을 사용하게 하려면 **clear conn** 명령을 사용하여 현재의 연결을 끊고 새 정책을 통해 다시 연결하게 해야 합니다. 또는 **clear local-host** 명령을 사용하여 호스트별로 연결을 지우거나, 동적 NAT를 사용하는 연결에 대해서는 **clear xlate** 연결을 사용할 수 있습니다.

ASA에서 보조 연결을 허용하기 위해 핀홀을 생성할 경우 이는 **show conn** 명령 출력에서 불완전한 연결로 표시됩니다. 이 불완전한 연결을 지우려면 **clear conn** 명령을 사용합니다.

예

다음 예에서는 모든 연결을 제거한 다음 10.10.10.108:4168과 10.0.8.112:22 간의 관리 연결을 지우는 방법을 보여줍니다.

```
ciscoasa# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB

ciscoasa# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

관련 명령

명령	설명
clear local-host	특정 로컬 호스트 또는 모든 로컬 호스트에 의한 연결을 모두 지웁니다.
clear xlate	동적 NAT 세션 및 NAT를 사용하는 모든 연결을 지웁니다.
show conn	연결 정보를 표시합니다.
show local-host	로컬 호스트의 네트워크 상태를 표시합니다.
show xlate	NAT 세션을 표시합니다.

clear console-output

현재 캡처된 콘솔 출력을 제거하려면 특별 권한 EXEC 모드에서 **clear console-output** 명령을 사용합니다.

clear console-output

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 현재 캡처된 콘솔 출력을 제거하는 방법을 보여줍니다.

```
ciscoasa# clear console-output
```

관련 명령

명령	설명
console timeout	ASA와의 콘솔 연결에 대한 유휴 타이머를 설정합니다.
show console-output	캡처된 콘솔 출력을 표시합니다.
show running-config console timeout	ASA와의 콘솔 연결에 대한 유휴 타이머를 표시합니다.

clear coredump

코어덤프 로그를 지우려면 글로벌 컨피그레이션 모드에서 **clear coredump** 명령을 사용합니다.

clear coredump

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본적으로 코어덤프는 활성화되어 있지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 코어덤프 파일 시스템의 내용과 코어덤프 로그를 제거합니다. 코어덤프 파일 시스템은 그대로 유지됩니다. 현재 코어덤프 컨피그레이션은 변함없이 유지됩니다.

예

다음 예에서는 코어덤프 파일 시스템의 내용 및 코어덤프 로그를 제거합니다.

```
ciscoasa(config)# clear coredump
Proceed with removing the contents of the coredump filesystem on 'disk0:' [confirm]
```

관련 명령

명령	설명
coredump enable	코어덤프 기능을 활성화합니다.
clear configure coredump	시스템에서 코어덤프 파일 시스템과 그 내용을 제거합니다.
show coredump filesystem	코어덤프 파일 시스템의 파일을 표시합니다.
show coredump log	코어덤프 로그를 표시합니다.

clear counters

프로토콜 스택 카운터를 지우려면 글로벌 컨피그레이션 모드에서 **clear counters** 명령을 사용합니다.

clear counters [all | context *context-name* **| summary | top** *N* **] [detail] [protocol** *protocol_name* [*:counter_name*]] [**threshold** *N*]

구문 설명

all	(선택 사항) 모든 필터 세부사항을 지웁니다.
context *context-name*	(선택 사항) 컨텍스트 이름을 지정합니다.
:*counter_name*	(선택 사항) 이름을 기준으로 카운터를 지정합니다.
detail	(선택 사항) 자세한 카운터 정보를 지웁니다.
protocol *protocol_name*	(선택 사항) 지정된 프로토콜의 카운터를 지웁니다.
summary	(선택 사항) 카운터 요약을 지웁니다.
threshold *N*	(선택 사항) 지정된 임계값에 도달하거나 이를 초과할 때 카운터를 지웁니다. 범위는 1~4294967295입니다.
top *N*	(선택 사항) 지정된 임계값에 도달하거나 이를 초과할 때 카운터를 지웁니다. 범위는 1~4294967295입니다.

기본값

clear counters summary detail 명령이 기본 설정입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 프로토콜 스택 카운터를 지우는 방법을 보여줍니다.

```
ciscoasa(config)# clear counters
```

관련 명령

명령	설명
show counters	프로토콜 스택 카운터를 표시합니다.

clear crashinfo

플래시 메모리에서 충돌 파일의 내용을 삭제하려면 특별 권한 EXEC 모드에서 **clear crashinfo** 명령을 사용합니다.

clear crashinfo

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 충돌 파일을 삭제하는 방법을 보여줍니다.

```
ciscoasa# clear crashinfo
```

관련 명령

crashinfo force	강제로 ASA에서 충돌이 일어나게 합니다.
crashinfo save disable	충돌 정보를 플래시 메모리에 기록할 수 없게 합니다.
crashinfo test	ASA에서 플래시 메모리의 파일에 충돌 정보를 저장하는 기능을 테스트합니다.
show crashinfo	플래시 메모리에 저장된 충돌 파일의 내용을 표시합니다.

clear crypto accelerator statistics

crypto accelerator MIB의 전역 및 가속기 관련 통계를 지우려면 특별 권한 EXEC 모드에서 **clear crypto accelerator statistics** 명령을 사용합니다.

clear crypto accelerator statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 crypto accelerator 통계를 표시합니다.

```
ciscoasa(config)# clear crypto accelerator statistics
ciscoasa(config)#
```

관련 명령

명령	설명
clear crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 지웁니다.
show crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 표시합니다.
show crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 표시합니다.

clear crypto ca crls

지정된 신뢰 지점과 연결된 모든 CRL을 CRL 캐시에서 없애거나 신뢰 풀과 연결된 모든 CRL을 캐시에서 없애거나 모든 CRL의 CRL 캐시를 제거하려면 특별 권한 EXEC 모드에서 **clear crypto ca crls** 명령을 사용합니다.

clear crypto ca crls [trustpool | trustpoint *trustpointname*]

구문 설명

trustpointname	신뢰 지점의 이름. 이름을 지정하지 않을 경우 이 명령은 시스템에 캐싱된 모든 CRL을 지웁니다. 신뢰 지점 이름 없이 신뢰 지점 키워드를 지정할 경우 명령은 실패합니다.
trustpool	신뢰 풀의 인증서와 연결된 CRL에만 해당 작업을 적용하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

예

특별 권한 EXEC 컨피그레이션 모드에서 입력한 별도의 다음 예에서는 모든 신뢰 풀 CRL 및 trustpoint123과 연결된 모든 CRL을 지우고 캐싱된 모든 CRL을 ASA에서 제거합니다.

```
ciscoasa# clear crypto ca crl trustpool
ciscoasa# clear crypto ca crl trustpoint trustpoint123
ciscoasa# clear crypto ca crl
```

관련 명령

명령	설명
crypto ca crl request	신뢰 지점의 CRL 컨피그레이션을 기반으로 한 CRL을 다운로드합니다.
show crypto ca crl	캐싱된 모든 CRL 또는 지정된 신뢰 지점에 대해 캐싱된 CRL을 표시합니다.

clear crypto ca trustpool

신뢰 풀에서 모든 인증서를 제거하려면 글로벌 컨피그레이션 모드에서 **clear crypto ca trustpool** 명령을 사용합니다.

clear crypto ca trustpool [noconfirm]

구문 설명

noconfirm	사용자 확인 프롬프트를 억제합니다. 명령은 요청대로 처리됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

사용자가 이 작업을 수행하기 전에 확인 메시지를 표시합니다.

예

```
ciscoasa# clear crypto ca trustpool
You are about to clear the trusted certificate pool. Do you want to continue? (y/n)
ciscoasa#
```

관련 명령

명령	설명
crypto ca trustpool export	PKI 신뢰 풀을 구성하는 인증서를 내보냅니다.
crypto ca trustpool import	PKI 신뢰 풀을 구성하는 인증서를 가져옵니다.
crypto ca trustpool remove	신뢰 풀에서 지정된 단일 인증서를 제거합니다.

clear crypto ikev1

IPsec IKEv1 SA 또는 통계를 제거하려면 특별 권한 EXEC 모드에서 **clear crypto ikev1** 명령을 사용합니다. 모든 IKEv1 SA를 지우려면 인수 없이 이 명령을 사용합니다.

clear crypto ikev1 {**sa** *IP_address_hostname* | **stats**}

구문 설명

sa	SA를 지웁니다.
IP_address_hostname	IP 주소 또는 호스트 이름.
stats	IKEv1 통계를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

모든 IPsec IKEv1 SA를 지우려면 인수 없이 이 명령을 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 모든 IPsec IKEv1 통계를 ASA에서 지웁니다.

```
ciscoasa# clear crypto ikev1 stats
ciscoasa#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
ciscoasa# clear crypto ikev1 peer 10.86.1.1
ciscoasa#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호 맵 또는 지정된 암호 맵을 컨피그레이션에서 지웁니다.
clear configure isakmp	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 컨피그레이션을 표시합니다.

clear crypto ikev2

IPsec IKEv2 SA 또는 통계를 제거하려면 특별 권한 EXEC 모드에서 **clear crypto ikev2** 명령을 사용합니다. 모든 IKEv2 SA를 지우려면 인수 없이 이 명령을 사용합니다.

clear crypto ikev2 {sa *IP_address_hostname* **| stats}**

구문 설명

sa	SA를 지웁니다.
IP_address_hostname	IP 주소 또는 호스트 이름.
stats	IKEv2 통계를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

모든 IPsec IKEv2 SA를 지우려면 인수 없이 이 명령을 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 모든 IPsec IKEv2 통계를 ASA에서 지웁니다.

```
ciscoasa# clear crypto ikev2 stats
ciscoasa#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
ciscoasa# clear crypto ikev2 peer 10.86.1.1
ciscoasa#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호 맵 또는 지정된 암호 맵을 컨피그레이션에서 지웁니다.
clear configure isakmp	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 컨피그레이션을 표시합니다.

clear crypto ipsec sa

IPsec SA 카운터, 엔트리, 암호 맵 또는 피어 연결을 제거하려면 특별 권한 EXEC 모드에서 **clear crypto ipsec sa** 명령을 사용합니다. 모든 IPsec SA를 지우려면 인수 없이 이 명령을 사용합니다.

clear [crypto] ipsec sa [counters | entry {*hostname* **|** *ip_address***} {esp | ah}** *spi* **| map** *map name* **| peer {***hostname* **|** *ip_address***}]**

구문 설명

ah	인증 헤더.
counters	모든 SAP별 IPsec 통계를 지웁니다.
entry	지정된 IP 주소/호스트 이름, 프로토콜, SPI 값과 매칭하는 터널을 삭제합니다.
esp	암호화 보안 프로토콜.
hostname	IP 주소에 지정된 호스트 이름을 식별합니다.
ip_address	IP 주소를 식별합니다.
map	맵 이름으로 식별되는 지정된 암호 맵과 연결된 모든 터널을 삭제합니다.
map name	암호 맵을 식별하는 영숫자 문자열. 최대 길이는 64자입니다.
peer	지정된 호스트 이름 또는 IP 주소로 식별되는 피어에 대한 모든 IPsec SA를 삭제합니다.
spi	SPI(Security Parameters Index)(16진수)를 식별합니다. 이는 인바운드 SPI여야 합니다. 아웃바운드 SPI에 대해서는 이 명령을 지원하지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

모든 IPsec SA를 지우려면 인수 없이 이 명령을 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 모든 IPsec SA를 ASA에서 지웁니다.

```
ciscoasa# clear crypto ipsec sa
ciscoasa#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
ciscoasa# clear crypto ipsec peer 10.86.1.1
ciscoasa#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호 맵 또는 지정된 암호 맵을 컨피그레이션에서 지웁니다.
clear configure isakmp	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 컨피그레이션을 표시합니다.

clear crypto protocol statistics

crypto accelerator MIB의 프로토콜 관련 통계를 지우려면 특별 권한 EXEC 모드에서 **clear crypto protocol statistics** 명령을 사용합니다.

clear crypto protocol statistics *protocol*

구문 설명

protocol	통계를 지우려는 프로토콜의 이름을 지정합니다. 다음과 같은 프로토콜을 선택할 수 있습니다. • **all**—현재 지원되는 모든 프로토콜 • **ikev1**—IKE(Internet Key Exchange) 버전 1 • **ikev2**—IKE(Internet Key Exchange) 버전 2 • **ipsec-client**—IPsec(IP Security) 2단계 프로토콜 • **other**—새 프로토콜용으로 예약 • **srtp**—SRTP(Secure RTP) 프로토콜 • **ssh**—SSH(Secure Shell) 프로토콜 • **ssl-client**—SSL(Secure Socket Layer) 프로토콜

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.4(1)	**ikev1** 및 **ikev2** 키워드를 추가했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 모든 crypto accelerator 통계를 지웁니다.

```
ciscoasa# clear crypto protocol statistics all
ciscoasa#
```

관련 명령

명령	설명
clear crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 지웁니다.
show crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 표시합니다.
show crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 표시합니다.

clear cts

Cisco TrustSec과 통합될 때 ASA에서 사용하는 데이터를 지우려면 글로벌 컨피그레이션 모드에서 **clear cts** 명령을 사용합니다.

clear cts {environment-data | pac}

구문 설명

environment-data	모든 CTS 환경 데이터를 지웁니다.
pac	저장된 CTS PAC를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

environment-data 키워드를 **clear cts** 명령과 함께 사용하면 Cisco ISE에서 다운로드한 Cisco TrustSec 환경 데이터를 지웁니다. 다음 환경 데이터 새로 고침을 수동으로 트리거할 수 있습니다. 또는 ASA에서 새로 고침 타이머가 만료될 때 데이터를 새로 고칩니다. **clear cts environment-data**를 실행하더라도 Cisco TrustSec PAC가 ASA에서 제거되지 않습니다. **clear cts nvironment-data** 명령을 실행하면 트래픽 정책에 영향을 주므로 이 작업에 대한 확인 프롬프트가 표시됩니다.

pac 키워드를 **clear cts** 명령과 함께 사용하면 ASA의 NVRAM에 저장된 PAC 정보를 지웁니다. PAC가 없을 경우 ASA는 Cisco TrustSec 환경 데이터를 다운로드할 수 없습니다. 그러나 이미 ASA에 있는 환경 데이터는 계속 사용됩니다. **clear cts pac** 명령을 실행하면 ASA에서 환경 데이터 업데이트를 검색할 수 없게 되므로 이 작업을 확인하는 프롬프트가 표시됩니다.

제한 사항

- HA: HA 컨피그레이션의 스탠바이 디바이스에서는 이 명령을 지원하지 않습니다. 스탠바이 디바이스에서 **clear cts** [**environment-data | pac**]를 실행하면 다음 오류 메시지가 표시됩니다.

  This command is only permitted on the primary device.

- 클러스터링: 마스터 디바이스에서만 이 명령을 지원합니다. 슬레이브 디바이스에서 **clear cts** [**environment-data | pac**]를 실행하면 다음 오류 메시지가 표시됩니다.

  This command is only permitted on the master device.

예

다음 예에서는 ASA와 Cisco TrustSec과의 통합에 사용되는 데이터를 ASA에서 지우는 방법을 보여줍니다.

```
ciscoasa# clear cts pac
Are you sure you want to delete the cts PAC? (y/n)

ciscoasa# clear cts environment-data
Are you sure you want to delete the cts environment data? (y/n)
```

관련 명령

명령	설명
clear configure all	ASA에서 실행 중인 컨피그레이션 전체를 지웁니다.
clear configure cts	ASA와 Cisco TrustSec의 통합에 대한 컨피그레이션을 지웁니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

clear dhcpd

DHCP 서버 바인딩 및 통계를 지우려면 특별 권한 EXEC 모드에서 **clear dhcp** 명령을 사용합니다.

clear dhcpd {binding [*ip_address***] | statistics}**

구문 설명

binding	모든 클라이언트 주소 바인딩을 지웁니다.
ip_address	(선택 사항) 지정된 IP 주소에 대한 바인딩을 지웁니다.
statistics	통계 정보 카운터를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear dhcpd binding 명령에 선택적 IP 주소를 포함할 경우 그 IP 주소에 대한 바인딩만 지워집니다. 모든 DHCP 서버 명령을 지우려면 **clear configure dhcpd** 명령을 사용합니다.

예

다음 예에서는 **dhcpd** 통계를 지우는 방법을 보여줍니다.

```
ciscoasa# clear dhcpd statistics
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
show dhcpd	DHCP 바인딩, 통계 또는 상태 정보를 표시합니다.

clear dhcprelay statistics

DHCP 릴레이 통계 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear dhcprelay statistics** 명령을 사용합니다.

clear dhcprelay statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear dhcprelay statistics 명령은 DHCP 릴레이 통계 카운터만 지웁니다. DHCP 릴레이 컨피그레이션 전체를 지우려면 **clear configure dhcprelay** 명령을 사용합니다.

예

다음 예에서는 DHCP 릴레이 통계를 지우는 방법을 보여줍니다.

```
ciscoasa# clear dhcprelay statistics
ciscoasa#
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
debug dhcprelay	DHCP 릴레이 에이전트의 디버깅 정보를 표시합니다.
show dhcprelay statistics	DHCP 릴레이 에이전트 통계 정보를 표시합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

clear dns

지정된 FQDN(정규화된 도메인 이름) 호스트와 연결된 모든 IP 주소를 지우려면 특별 권한 EXEC 모드에서 **clear dns** 명령을 사용합니다.

clear dns [host *fqdn_name***]**

구문 설명

fqdn_name	(선택 사항) 선택된 호스트의 FQDN을 지정합니다.
host	(선택 사항) 지정된 호스트의 IP 주소를 나타냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

예

다음 예에서는 지정된 FQDN 호스트와 연결된 IP 주소를 지웁니다.

```
ciscoasa# clear dns 10.1.1.2 www.example.com
```

참고 이 명령에서는 **dns expire-entry** 키워드 설정이 무시됩니다. 활성화된 각 FQDN 호스트에 대해 새 DNS 쿼리가 전송됩니다.

관련 명령

명령	설명
dns domain-lookup	ASA에서 이름 조회를 할 수 있게 합니다.
dns name-server	DNS 서버 주소를 구성합니다.
dns retries	ASA에서 응답을 받지 않을 때 DNS 서버의 목록을 재시도하는 횟수를 지정합니다.
dns timeout	다음 DNS 서버를 시도하기 전에 대기하는 시간을 지정합니다.
show dns-hosts	DNS 캐시를 표시합니다.

clear dns-hosts cache

DNS 캐시를 지우려면 특별 권한 EXEC 모드에서 **clear dns-hosts cache** 명령을 사용합니다.

clear dns-hosts cache

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 **name** 이름으로 추가한 고정 엔트리를 지우지 않습니다.

예

다음 예에서는 DNS 캐시를 지웁니다.

```
ciscoasa# clear dns-hosts cache
```

관련 명령

명령	설명
dns domain-lookup	ASA에서 이름 조회를 할 수 있게 합니다.
dns name-server	DNS 서버 주소를 구성합니다.
dns retries	ASA에서 응답을 받지 않을 때 DNS 서버의 목록을 재시도하는 횟수를 지정합니다.
dns timeout	다음 DNS 서버를 시도하기 전에 대기하는 시간을 지정합니다.
show dns-hosts	DNS 캐시를 표시합니다.

clear dynamic-filter dns-snoop

봇넷 트래픽 필터 DNS 스누핑 데이터를 지우려면 특별 권한 EXEC 모드에서 **clear dynamic-filter dns-snoop** 명령을 사용합니다.

clear dynamic-filter dns-snoop

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 모든 봇넷 트래픽 필터 DNS 스누핑 데이터를 지웁니다.

```
ciscoasa# clear dynamic-filter dns-snoop
```

관련 명령

명령	설명
address	블랙리스트 또는 화이트리스트에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇넷 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter reports	봇넷 트래픽 필터 보고서 데이터를 지웁니다.
clear dynamic-filter statistics	봇넷 트래픽 필터 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	봇넷 트래픽 필터 블랙리스트를 수정합니다.
dynamic-filter database fetch	봇넷 트래픽 필터 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇넷 트래픽 필터 동적 데이터베이스를 직접 삭제합니다.

명령	설명
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	어떤 트래픽 클래스에 대해 또는 액세스 목록을 지정하지 않았다면 모든 트래픽에 대해 봇넷 트래픽 필터를 활성화합니다.
dynamic-filter updater-client enable	동적 데이터베이스의 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스의 사용을 활성화합니다.
dynamic-filter whitelist	봇넷 트래픽 필터 화이트리스트를 수정합니다.
inspect dns dynamic-filter-snoop	봇넷 트래픽 필터 스누핑과 함께 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇넷 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇넷 트래픽 필터로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매칭하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	봇넷 트래픽 필터의 실행 중인 컨피그레이션을 표시합니다.

clear dynamic-filter reports

봇넷 트래픽 필터에 대한 보고서 데이터를 지우려면 특별 권한 EXEC 모드에서 **clear dynamic-filter reports** 명령을 사용합니다.

clear dynamic-filter reports {top [malware-sites | malware-ports | infected-hosts] | infected-hosts}

구문 설명

malware-ports	(선택 사항) 상위 10개 악성코드 포트에 대한 보고서 데이터를 지웁니다.
malware-sites	(선택 사항) 상위 10개 악성코드 사이트에 대한 보고서 데이터를 지웁니다.
infected-hosts (**top**)	(선택 사항) 상위 10개 감염 호스트에 대한 보고서 데이터를 지웁니다.
top	상위 10개 악성코드 사이트, 포트, 감염 호스트에 대한 보고서 데이터를 지웁니다.
infected-hosts	감염 호스트에 대한 보고서 데이터를 지웁니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.
8.2(2)	**botnet-sites** 및 **botnet-ports** 키워드를 **malware-sites** 및 **malware-ports**로 변경했습니다. 상위 10개 보고서 지우기와 새 감염 호스트 보고서 지우기를 구별하기 위해 **top** 키워드를 추가했습니다. **infected-hosts** 키워드를 추가했습니다(**top** 없음).

예

다음 예에서는 모든 봇넷 트래픽 필터 상위 10개 보고서 데이터를 지웁니다.

```
ciscoasa# clear dynamic-filter reports top
```

다음 예에서는 상위 10개 악성코드 사이트 보고서 데이터만 지웁니다.

```
ciscoasa# clear dynamic-filter reports top malware-sites
```

다음 예에서는 모든 감염 호스트 보고서 데이터를 지웁니다.

```
ciscoasa# clear dynamic-filter reports infected-hosts
```

관련 명령

명령	설명
address	블랙리스트 또는 화이트리스트에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇넷 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter statistics	봇넷 트래픽 필터 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	봇넷 트래픽 필터 블랙리스트를 수정합니다.
dynamic-filter database fetch	봇넷 트래픽 필터 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇넷 트래픽 필터 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	어떤 트래픽 클래스에 대해 또는 액세스 목록을 지정하지 않았다면 모든 트래픽에 대해 봇넷 트래픽 필터를 활성화합니다.
dynamic-filter updater-client enable	동적 데이터베이스의 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스의 사용을 활성화합니다.
dynamic-filter whitelist	봇넷 트래픽 필터 화이트리스트를 수정합니다.
inspect dns dynamic-filter-snoop	봇넷 트래픽 필터 스누핑과 함께 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇넷 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports infected-hosts	감염 호스트 보고서를 생성합니다.
show dynamic-filter reports top	상위 10개 악성코드 사이트, 포트, 감염 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇넷 트래픽 필터로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매칭하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	봇넷 트래픽 필터의 실행 중인 컨피그레이션을 표시합니다.

clear dynamic-filter statistics

봇넷 트래픽 필터 통계를 지우려면 특별 권한 EXEC 모드에서 **clear dynamic-filter statistics** 명령을 사용합니다.

clear dynamic-filter statistics [interface *name***]**

구문 설명

interface *name*	(선택 사항) 특정 인터페이스에 대한 통계를 지웁니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 모든 봇넷 트래픽 필터 DNS 통계를 지웁니다.

```
ciscoasa# clear dynamic-filter statistics
```

관련 명령

명령	설명
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
address	블랙리스트 또는 화이트리스트에 IP 주소를 추가합니다.
clear configure dynamic-filter	실행 중인 봇넷 트래픽 필터 컨피그레이션을 지웁니다.
clear dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 데이터를 지웁니다.
clear dynamic-filter reports	봇넷 트래픽 필터 보고서 데이터를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter blacklist	봇넷 트래픽 필터 블랙리스트를 수정합니다.
dynamic-filter database fetch	봇넷 트래픽 필터 동적 데이터베이스를 직접 검색합니다.

명령	설명
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	봇넷 트래픽 필터 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter enable	어떤 트래픽 클래스에 대해 또는 액세스 목록을 지정하지 않았다면 모든 트래픽에 대해 봇넷 트래픽 필터를 활성화합니다.
dynamic-filter updater-client enable	동적 데이터베이스의 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스의 사용을 활성화합니다.
dynamic-filter whitelist	봇넷 트래픽 필터 화이트리스트를 수정합니다.
inspect dns dynamic-filter-snoop	봇넷 트래픽 필터 스누핑과 함께 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속화된 보안 경로에 설치된 봇넷 트래픽 필터 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	봇넷 트래픽 필터 DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports infected-hosts	감염 호스트 보고서를 생성합니다.
show dynamic-filter reports top	상위 10개 악성코드 사이트, 포트, 감염 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	봇넷 트래픽 필터로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매칭하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	봇넷 트래픽 필터의 실행 중인 컨피그레이션을 표시합니다.

clear eigrp events

EIGRP 이벤트 로그를 지우려면 특별 권한 EXEC 모드에서 **clear eigrp events** 명령을 사용합니다.

clear eigrp [*as-number***] events**

구문 설명

as-number	(선택 사항) 이벤트 로그를 지우려는 EIGRP 프로세스의 자율 시스템 번호를 지정합니다. ASA는 단일 EIGRP 라우팅 프로세스만 지원하므로 자율 시스템 번호(프로세스 ID)를 지정할 필요 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

EIGRP 이벤트 로그를 보기 위해 **show eigrp events** 명령을 사용할 수 있습니다.

예

다음 예에서는 EIGRP 이벤트 로그를 지웁니다.

```
ciscoasa# clear eigrp events
```

관련 명령

명령	설명
show eigrp events	EIGRP 이벤트 로그를 표시합니다.

clear eigrp neighbors

EIGRP 네이버 테이블에서 엔트리를 삭제하려면 특별 권한 EXEC 모드에서 **clear eigrp neighbors** 명령을 사용합니다.

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] **[soft]**

구문 설명

as-number	(선택 사항) 네이버 엔트리를 삭제하려는 EIGRP 프로세스의 자율 시스템 번호를 지정합니다. ASA는 단일 EIGRP 라우팅 프로세스만 지원하므로 프로세스 ID인 자율 시스템 번호(AS)를 지정할 필요 없습니다.
if-name	(선택 사항) **nameif** 명령에 의해 지정되는 인터페이스의 이름. 인터페이스 이름을 지정하면 이 인터페이스를 통해 학습한 모든 네이버 테이블 엔트리를 제거합니다.
ip-addr	(선택 사항) 네이버 테이블에서 제거하려는 네이버의 IP 주소.
soft	ASA에서 인접성의 재설정 없이 네이버와 다시 동기화하게 합니다.

기본값

네이버 IP 주소 또는 인터페이스 이름을 지정하지 않을 경우 모든 동적 엔트리가 네이버 테이블에서 제거됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

clear eigrp neighbors 명령은 **neighbor** 명령으로 정의된 네이버를 네이버 테이블에서 제거하지 않습니다. 동적으로 검색된 네이버만 제거됩니다.

EIGRP 네이버 테이블을 보기 위해 **show eigrp neighbors** 명령을 사용할 수 있습니다.

예

다음 예에서는 EIGRP 네이버 테이블에서 모든 엔트리를 제거합니다.

```
ciscoasa# clear eigrp neighbors
```

다음 예에서는 "outside"라는 이름의 인터페이스를 통해 학습한 모든 엔트리를 EIGRP 네이버 테이블에서 제거합니다.

```
ciscoasa# clear eigrp neighbors outside
```

관련 명령

명령	설명
debug eigrp neighbors	EIGRP 네이버에 대한 디버깅 정보를 표시합니다.
debug ip eigrp	EIGRP 프로토콜 패킷에 대한 디버깅 정보를 표시합니다.
show eigrp neighbors	EIGRP 인접 디바이스 테이블을 표시합니다.

clear eigrp topology

EIGRP 토폴로지 테이블에서 엔트리를 삭제하려면 특별 권한 EXEC 모드에서 **clear eigrp topology** 명령을 사용합니다.

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

구문 설명

as-number	(선택 사항) EIGRP 프로세스의 자율 시스템 번호를 지정합니다. ASA는 단일 EIGRP 라우팅 프로세스만 지원하므로 프로세스 ID인 자율 시스템 번호(AS)를 지정할 필요 없습니다.
ip-addr	토폴로지 테이블에서 지울 IP 주소.
mask	(선택 사항) *ip-addr* 인수에 적용할 네트워크 마스크.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

이 명령은 EIGRP 토폴로지 테이블에서 기존 EIGRP 엔트리를 지웁니다. 토폴로지 테이블 엔트리를 보기 위해 **show eigrp topology** 명령을 사용할 수 있습니다.

예

다음 예에서는 192.168.1.0 네트워크의 엔트리를 EIGRP 토폴로지 테이블에서 제거합니다.

```
ciscoasa# clear eigrp topology 192.168.1.0 255.255.255.0
```

관련 명령

명령	설명
show eigrp topology	EIGRP 토폴로지 테이블을 표시합니다.

clear failover statistics

장애 조치 통계 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear failover statistics** 명령을 사용합니다.

clear failover statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 **show failover statistics** 명령으로 표시되는 통계 및 **show failover** 명령 출력에서 Stateful Failover Logical Update Statistics 섹션에 있는 카운터를 지웁니다. 장애 조치 컨피그레이션을 제거하려면 **clear configure failover** 명령을 사용합니다.

예

다음 예에서는 장애 조치 통계 카운터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear failover statistics
ciscoasa#
```

관련 명령

명령	설명
debug fover	장애 조치 디버깅 정보를 표시합니다.
show failover	장애 조치 컨피그레이션 및 운영 통계에 대한 정보를 표시합니다.

clear flow-export counters

NetFlow 데이터와 연결된 런타임 카운터를 0으로 재설정하려면 특별 권한 EXEC 모드에서 **clear flow-export counters** 명령을 사용합니다.

clear flow-export counters

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.1(1)	이 명령을 도입했습니다.

사용 지침

런타임 카운터는 통계 데이터와 오류 데이터를 모두 포함합니다.

예

다음 예에서는 NetFlow 데이터와 연결된 런타임 카운터를 재설정하는 방법을 보여줍니다.

```
ciscoasa# clear flow-export counters
```

관련 명령

명령	설명
flow-export destination *interface-name ipv4-address* | *hostname udp-port*	NetFlow 컬렉터의 IP 주소 또는 호스트 이름 및 NetFlow 컬렉터가 수신하는 UDP 포트를 지정합니다.
flow-export template timeout-rate *minutes*	템플릿 정보가 NetFlow 컬렉터에 보내지는 간격을 제어합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 다음 표시되는 syslog 메시지 및 NetFlow 데이터와 관련된 syslog 메시지를 활성화합니다.
show flow-export counters	NetFlow의 모든 런타임 카운터를 표시합니다.

clear fragment

IP 프래그먼트 재결합 모듈의 운영 데이터를 지우려면 특별 권한 EXEC 모드에서 **clear fragment** 명령을 입력합니다.

clear fragment {**queue** | **statistics**} [*interface*]

구문 설명

interface	(선택 사항) ASA 인터페이스를 지정합니다.
queue	IP 프래그먼트 재결합 대기열을 지웁니다.
statistics	IP 프래그먼트 재결합 통계를 지웁니다.

기본값

*interface*가 지정되지 않을 경우 이 명령은 모든 인터페이스에 적용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	컨피그레이션 데이터 지우기와 운영 데이터 지우기를 분리하기 위해 이 명령을 **clear fragment**와 **clear configure fragment**로 나누었습니다.

사용 지침

이 명령은 현재 대기열에서 재결합을 기다리는 프래그먼트를 지우거나(**queue** 키워드를 입력할 경우) 모든 IP 프래그먼트 재결합 통계를 지웁니다(**statistics** 키워드를 입력할 경우). 통계는 카운터로서 성공적으로 재결합한 프래그먼트 체인 수, 재결합하지 못한 체인 수, 최대 크기를 초과하여 버퍼 오버플로가 발생한 횟수를 알려줍니다.

예

다음 예에서는 IP 프래그먼트 재결합 모듈의 운영 데이터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear fragment queue
```

관련 명령

명령	설명
clear configure fragment	IP 프래그먼트 재결합 컨피그레이션을 지우고 기본값을 재설정합니다.
fragment	패킷 단편화를 추가적으로 관리하며 NFS와의 호환성을 향상시킵니다.
show fragment	IP 프래그먼트 재결합 모듈의 작업 데이터를 표시합니다.
show running-config fragment	IP 프래그먼트 재결합 컨피그레이션을 표시합니다.

clear gc

GC(garbage collection) 프로세스 통계를 제거하려면 특별 권한 EXEC 모드에서 **clear gc** 명령을 사용합니다.

clear gc

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 GC 프로세스 통계를 제거하는 방법을 보여줍니다.

```
ciscoasa# clear gc
```

관련 명령

명령	설명
show gc	GC 프로세스 통계를 표시합니다.

clear igmp counters

모든 IGMP 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear igmp counters** 명령을 사용합니다.

clear igmp counters [*if_name*]

구문 설명

if_name	**nameif** 명령에 의해 지정된 인터페이스 이름. 이 명령에 인터페이스 이름을 포함하면 지정된 인터페이스의 카운터만 지워집니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 IGMP 통계 카운터를 지웁니다.

```
ciscoasa# clear igmp counters
```

관련 명령

명령	설명
clear igmp group	검색된 그룹을 IGMP 그룹 캐시에서 지웁니다.
clear igmp traffic	IGMP 트래픽 카운터를 지웁니다.

clear igmp group

검색된 그룹을 IGMP 그룹 캐시에서 지우려면 특별 권한 EXEC 모드에서 **clear igmp** 명령을 사용합니다.

clear igmp group [*group* **| interface** *name***]**

구문 설명

group	IGMP 그룹 주소. 특정 그룹을 지정하면 이 그룹이 캐시에서 제거됩니다.
interface *name*	**nameif** 명령에 의해 지정된 인터페이스 이름. 지정하면 이 인터페이스와 연결된 모든 그룹이 제거됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

그룹 또는 인터페이스를 지정하지 않을 경우 모든 그룹이 모든 인터페이스에서 지워집니다. 그룹을 지정할 경우 그 그룹의 엔트리만 지워집니다. 인터페이스를 지정할 경우 그 인터페이스의 모든 그룹이 지워집니다. 그룹과 인터페이스를 모두 지정할 경우 지정된 인터페이스의 지정된 그룹만 지워집니다.

이 명령은 통계적으로 구성된 그룹을 지우지 않습니다.

예

다음 예에서는 검색된 모든 IGMP 그룹을 IGMP 그룹 캐시에서 지우는 방법을 보여줍니다.

```
ciscoasa# clear igmp group
```

관련 명령

명령	설명
clear igmp counters	모든 IGMP 카운터를 지웁니다.
clear igmp traffic	IGMP 트래픽 카운터를 지웁니다.

clear igmp traffic

IGMP 트래픽 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear igmp traffic** 명령을 사용합니다.

clear igmp traffic

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 IGMP 통계 트래픽 카운터를 지웁니다.

```
ciscoasa# clear igmp traffic
```

관련 명령

명령	설명
clear igmp group	검색된 그룹을 IGMP 그룹 캐시에서 지웁니다.
clear igmp counters	모든 IGMP 카운터를 지웁니다.

clear interface

인터페이스 통계를 지우려면 특별 권한 EXEC 모드에서 **clear interface** 명령을 사용합니다.

clear interface [*physical_interface***[.***subinterface***] | *mapped_name* | *interface_name*]**

구문 설명

interface_name	(선택 사항) **nameif** 이름으로 설정된 인터페이스 이름을 나타냅니다.
mapped_name	(선택 사항) 다중 컨텍스트 모드에서 **allocate-interface** 명령으로 지정된 매핑된 이름을 나타냅니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet0/1**)를 나타냅니다. 허용되는 값에 대해서는 **interface** 명령을 참조하십시오.
subinterface	(선택 사항) 1~4294967293 범위의 정수로 논리적 하위 인터페이스를 지정합니다.

기본값

기본적으로 이 명령은 모든 인터페이스 통계를 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

여러 컨텍스트에서 인터페이스를 공유할 경우 어떤 컨텍스트 내에서 이 명령을 입력하면 ASA는 현재 컨텍스트의 통계만 지웁니다. 시스템 실행 영역에서 이 명령을 입력할 경우 ASA는 종합 통계를 지웁니다.

시스템 실행 영역에서 인터페이스 이름을 사용할 수 없습니다. **nameif** 명령은 컨텍스트 내에서만 사용 가능하기 때문입니다. 또한 **allocate-interface** 명령을 사용하여 인터페이스 ID를 어떤 이름에 매핑한 경우 컨텍스트에서 그 매핑된 이름만 사용할 수 있습니다.

예

다음 예에서는 모든 인터페이스 통계를 지웁니다.

```
ciscoasa# clear interface
```

관련 명령

명령	설명
clear configure interface	인터페이스 컨피그레이션을 지웁니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show running-config interface	인터페이스 컨피그레이션을 표시합니다.

clear ip audit count

어떤 감사 정책에 대한 시그니처 매칭의 수를 지우려면 특별 권한 EXEC 모드에서 **clear ip audit count** 명령을 사용합니다.

clear ip audit count [global | interface *interface_name***]**

구문 설명

global	(기본값) 모든 인터페이스의 매칭 수를 지웁니다.
interface *interface_name*	(선택 사항) 지정된 인터페이스의 매칭 수를 지웁니다.

기본값

키워드를 지정하지 않을 경우 이 명령은 모든 인터페이스의 매칭을 제거합니다(**global**).

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 모든 인터페이스에서 수를 지웁니다.

```
ciscoasa# clear ip audit count
```

관련 명령

명령	설명
ip audit interface	인터페이스에 감사 정책을 지정합니다.
ip audit name	패킷이 공격 시그니처 또는 참조용 시그니처와 매칭할 때 수행할 작업을 지정하는 명명된 감사 정책을 만듭니다.
show ip audit count	감사 정책에 대한 시그니처 매칭 수를 표시합니다.
show running-config ip audit attack	**ip audit attack** 공격에 대한 컨피그레이션을 표시합니다.

clear ip verify statistics

유니캐스트 RPF 통계를 지우려면 특별 권한 EXEC 모드에서 **clear ip verify statistics** 명령을 사용합니다.

clear ip verify statistics [interface *interface_name***]**

구문 설명

interface *interface_name*	유니캐스트 RPF 통계를 지울 인터페이스를 설정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

유니캐스트 RPF를 활성화하려면 **ip verify reverse-path** 명령을 참조하십시오.

예

다음 예에서는 유니캐스트 RPF 통계를 지웁니다.

```
ciscoasa# clear ip verify statistics
```

관련 명령

명령	설명
clear configure ip verify reverse-path	**ip verify reverse-path** 컨피그레이션을 지웁니다.
ip verify reverse-path	IP 스푸핑을 방지하기 위해 유니캐스트 RPF 기능을 활성화합니다.
show ip verify statistics	유니캐스트 RPF 통계를 표시합니다.
show running-config ip verify reverse-path	**ip verify reverse-path** 컨피그레이션을 표시합니다.

clear ipsec sa

IPsec SA를 완전히 또는 지정된 매개변수에 따라 지우려면 특별 권한 EXEC 모드에서 **clear ipsec sa** 명령을 사용합니다.

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

구문 설명

counters	(선택 사항) 모든 카운터를 지웁니다.
entry	(선택 사항) 지정된 IPsec 피어, 프로토콜, SPI의 IPsec SA를 지웁니다.
inactive	(선택 사항) 트래픽을 전달할 수 없는 IPsec SA를 지웁니다.
map *map-name*	(선택 사항) 지정된 암호 맵의 IPsec SA를 지웁니다.
peer	(선택 사항) 지정된 피어의 IPsec SA를 지웁니다.
peer-addr	IPsec 피어의 IP 주소를 지정합니다.
protocol	IPsec 프로토콜을 **esp** 또는 **ah**로 지정합니다.
spi	IPsec SPI를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령의 대체 형식인 **clear crypto ipsec sa**를 사용하여 동일한 기능을 수행할 수 있습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 모든 IPsec SA 카운터를 지웁니다.

```
ciscoasa# clear ipsec sa counters
ciscoasa#
```

관련 명령

명령	설명
show ipsec sa	지정된 매개변수에 따라 IPsec SA를 표시합니다.
show ipsec stats	IPsec 플로우 MIB의 전역 IPsec 통계를 표시합니다.

clear ipv6 access-list counters

IPv6 액세스 목록 통계 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear ipv6 access-list counters** 명령을 사용합니다.

clear ipv6 access-list *id* **counters**

구문 설명

id	IPv6 액세스 목록 식별자

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 IPv6 액세스 목록 2의 통계 데이터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear ipv6 access-list 2 counters
ciscoasa#
```

관련 명령

명령	설명
clear configure ipv6	현재 컨피그레이션에서 **ipv6 access-list** 명령을 지웁니다.
ipv6 access-list	IPv6 액세스 목록을 구성합니다.
show ipv6 access-list	현재 컨피그레이션의 **ipv6 access-list** 명령을 표시합니다.

clear ipv6 dhcprelay binding

IPv6 DHCP 릴레이 바인딩 엔트리를 지우려면 특별 권한 EXEC 모드에서 **clear ipv6 dhcprelay binding** 명령을 사용합니다.

clear ipv6 dhcprelay binding [ip]

구문 설명

ip	(선택 사항) DHCP 릴레이 바인딩을 위한 IPv6 주소를 지정합니다. IP 주소가 지정될 경우 그 IP 주소와 연결된 릴레이 바인딩 엔트리만 지워집니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 IPv6 DHCP 릴레이 바인딩의 통계 데이터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear ipv6 dhcprelay binding
ciscoasa#
```

관련 명령

명령	설명
show ipv6 dhcprelay binding	릴레이 에이전트에 의해 생성된 릴레이 바인딩 엔트리를 표시합니다.
show ipv6 dhcprelay statistics	IPv6 DHCP 릴레이 에이전트 정보를 표시합니다.

clear ipv6 dhcprelay statistics

IPv6 DHCP 릴레이 에이전트 통계를 지우려면 특별 권한 EXEC 모드에서 **clear ipv6 dhcprelay statistics** 명령을 사용합니다.

clear ipv6 dhcprelay statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 IPv6 DHCP 릴레이 에이전트의 통계 데이터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear ipv6 dhcprelay statistics
ciscoasa#
```

관련 명령

명령	설명
show ipv6 dhcprelay binding	릴레이 에이전트에 의해 생성된 릴레이 바인딩 엔트리를 표시합니다.
show ipv6 dhcprelay statistics	IPv6의 DHCP 릴레이 에이전트 정보를 표시합니다.

clear ipv6 mld traffic

IPv6 MLD(Multicast Listener Discovery) 트래픽 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear ipv6 mld traffic** 명령을 사용합니다.

clear ipv6 mld traffic

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(4)	이 명령을 도입했습니다.

사용 지침

clear ipv6 mld traffic 명령을 사용하면 모든 MLD 트래픽 카운터를 재설정할 수 있습니다.

예

다음 예에서는 IPv6 MLD에 대한 트래픽 카운터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear ipv6 mld traffic
ciscoasa#
```

관련 명령

명령	설명
debug ipv6 mld	MLD에 대한 모든 디버깅 메시지를 표시합니다.
show debug ipv6 mld	현재 컨피그레이션에서 IPv6를 위한 MLD 명령을 표시합니다.

clear ipv6 neighbors

IPv6 네이버 검색 캐시를 지우려면 특별 권한 EXEC 모드에서 **clear ipv6 neighbors** 명령을 사용합니다.

clear ipv6 neighbors

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 검색된 모든 IPv6 네이버를 캐시에서 삭제합니다. 고정 엔트리는 제거하지 않습니다.

예

다음 예에서는 IPv6 네이버 검색 캐시에서 고정 엔트리를 제외한 모든 엔트리를 삭제합니다.

```
ciscoasa# clear ipv6 neighbors
ciscoasa#
```

관련 명령

명령	설명
ipv6 neighbor	IPv6 인접 디바이스 탐색 캐시에서 고정 엔트리를 구성합니다.
show ipv6 neighbor	IPv6 네이버 캐시 정보를 표시합니다.

clear ipv6 ospf

OSPFv3 라우팅 매개변수를 지우려면 특별 권한 EXEC 모드에서 **clear ipv6 ospf** 명령을 사용합니다.

clear ipv6 [*process_id*] **[counters] [events] [force-spf] [process] [redistribution] [traffic]**

구문 설명

counters	OSPF 프로세스 카운터를 재설정합니다.
events	OSPF 이벤트 로그를 지웁니다.
force-ospf	OSPF 프로세스에 대한 SPF를 지웁니다.
process	OSPFv3 프로세스를 재설정합니다.
process_id	프로세스 ID 번호를 지웁니다. 유효한 값의 범위는 1~65535입니다.
redistribution	OSPFv3 경로 재배포를 지웁니다.
traffic	트래픽 관련 통계를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 모든 OSPFv3 라우팅 매개변수를 제거합니다.

예

다음 예에서는 모든 OSPFv3 경로 재배포를 지우는 방법을 보여줍니다.

```
ciscoasa# clear ipv6 ospf redistribution
ciscoasa#
```

관련 명령

명령	설명
show running-config ipv6 router	OSPFv3 프로세스의 실행 중인 컨피그레이션을 표시합니다.
clear configure ipv6 router	OSPFv3 라우팅 프로세스를 지웁니다.

clear ipv6 traffic

IPv6 트래픽 카운터를 재설정하려면 특별 권한 EXEC 모드에서 **clear ipv6 traffic** 명령을 사용합니다.

clear ipv6 traffic

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령을 사용하면 **show ipv6 traffic** 명령의 출력에서 카운터를 재설정합니다.

예

다음 예에서는 IPv6 트래픽 카운터를 재설정합니다. **ipv6 traffic** 명령의 출력에서 카운터가 재설정되었음을 알 수 있습니다.

```
ciscoasa# clear ipv6 traffic
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
```

```
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

관련 명령

명령	설명
show ipv6 traffic	IPv6 트래픽 통계를 표시합니다.

clear isakmp sa

모든 IKE 런타임 SA 데이터베이스를 제거하려면 글로벌 컨피그레이션 또는 특별 권한 EXEC 모드에서 **clear isakmp sa** 명령을 사용합니다.

clear isakmp sa

구문 설명

이 명령은 키워드 또는 인수가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	—	• 예	• 예	—
글로벌 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	**clear isakmp sa** 명령을 **clear crypto isakmp sa**로 변경했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 예에서는 컨피그레이션에서 IKE 런타임 SA 데이터베이스를 제거합니다.

```
ciscoasa# clear isakmp sa
ciscoasa#
```

관련 명령

명령	설명
clear isakmp	IKE 런타임 SA 데이터베이스를 지웁니다.
isakmp enable	IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP 협상을 활성화합니다.
show isakmp stats	런타임 통계를 표시합니다.
show isakmp sa	추가 정보와 함께 IKE 런타임 SA 데이터베이스를 표시합니다.
show running-config isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

7 장

clear local-host ~ clear xlate 명령

clear local-host

클라이언트별 런타임 상태(예: 연결 제한, 초기 제한)를 다시 초기화하려면 특별 권한 EXEC 모드에서 **clear local-host** 명령을 사용합니다. t

clear local-host [*ip_address*] [**all**]

구문 설명

all	(선택 사항) to-the-box 트래픽을 포함한 모든 연결을 지웁니다. **all** 키워드를 사용하지 않으면 through-the-box 트래픽만 지워집니다.
ip_address	(선택 사항) 로컬 호스트 IP 주소를 지정합니다.

기본값

모든 through-the-box 런타임 상태를 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

컨피그레이션에 대한 보안 정책을 변경하면 모든 *새* 연결에서는 새로운 보안 정책을 사용합니다. 기존 연결에서는 연결을 설정할 당시 구성된 정책을 계속 사용합니다. 모든 연결에서 새 정책을 사용하게 하려면 **clear local-host** 명령을 사용하여 현재의 연결을 끊고 새 정책을 통해 다시 연결하게 해야 합니다. 또는 더 세부적인 연결 지우기를 위해 **clear conn** 명령을 사용하거나 동적 NAT를 사용하는 연결을 위해 **clear xlate** 명령을 사용할 수 있습니다.

clear local-host 명령은 호스트 라이센스 제한에서 호스트를 릴리스합니다. **show local-host** 명령을 입력하여 라이센스 한도 대비 호스트 수를 확인할 수 있습니다.

예

다음 예에서는 호스트 10.1.1.15의 런타임 상태 및 해당 연결을 지웁니다.

```
ciscoasa# clear local-host 10.1.1.15
```

관련 명령

명령	설명
clear conn	어떤 상태의 연결도 종료합니다.
clear xlate	동적 NAT 세션 및 NAT를 사용하는 모든 연결을 지웁니다.
show local-host	로컬 호스트의 네트워크 상태를 표시합니다.

clear logging asdm

ASDM 로깅 버퍼를 지우려면 특별 권한 EXEC 모드에서 **clear logging asdm** 명령을 사용합니다.

clear logging asdm

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**clear pdm logging** 명령을 **clear asdm log** 명령으로 변경했습니다.

사용 지침

ASDM 시스템 로그 메시지는 ASA 시스템 로그 메시지와 다른 버퍼에 저장됩니다. ASDM 로깅 버퍼를 지우면 ASDM 시스템 로그 메시지만 지웁니다. ASA 시스템 로그 메시지는 지워지지 않습니다. ASDM 시스템 로그 메시지를 보려면 **show asdm log** 명령을 사용합니다.

예

다음 예에서는 ASDM 로깅 버퍼를 지웁니다.

```
ciscoasa(config)# clear logging asdm
ciscoasa(config)#
```

관련 명령

명령	설명
show asdm log_sessions	ASDM 로깅 버퍼의 내용을 표시합니다.

clear logging buffer

로그 버퍼를 지우려면 특별 권한 EXEC 모드에서 **clear logging buffer** 명령을 사용합니다.

clear logging buffer

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

이 예에서는 로그 버퍼의 내용을 지우는 방법을 보여줍니다.

```
ciscoasa# clear logging buffer
```

관련 명령

명령	설명
logging buffered	로그 버퍼를 구성합니다.
show logging	로깅 정보를 표시합니다.

clear logging queue bufferwrap

저장된 로그 버퍼(ASDM, 내부, FTP, 플래시)를 지우려면 특별 권한 EXEC 모드에서 **clear logging queue bufferwrap** 명령을 사용합니다.

clear logging queue bufferwrap

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 저장된 로그 버퍼의 내용을 지우는 방법을 보여줍니다.

```
ciscoasa# clear logging queue bufferwrap
```

관련 명령

명령	설명
logging buffered	로그 버퍼를 구성합니다.
show logging	로깅 정보를 표시합니다.

clear mac-address-table

동적 MAC 주소 테이블 엔트리를 지우려면 특별 권한 EXEC 모드에서 **clear mac-address-table** 명령을 사용합니다.

clear mac-address-table [*interface_name***]**

구문 설명

interface_name	(선택 사항) 선택된 인터페이스에 대한 MAC 주소 테이블 엔트리를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 동적 MAC 주소 테이블 엔트리를 지웁니다.

```
ciscoasa# clear mac-address-table
```

관련 명령

명령	설명
arp	고정 ARP 항목을 추가합니다.
firewall transparent	방화벽 모드를 투명 모드로 설정합니다.
mac-address-table aging-time	동적 MAC 주소 엔트리에 대한 시간 초과를 설정합니다.
mac-learn	MAC 주소 파악을 비활성화합니다.
show mac-address-table	MAC 주소 테이블 엔트리를 표시합니다.

clear mdm-proxy statistics

MDM 프록시 서비스 카운터를 0으로 설정하여 지웁니다.

clear mdm-proxy statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 도입했습니다.

예

```
ciscoasa (config)# clear mdm-proxy statistics<cr>
```

관련 명령

명령	설명
show mdm-proxy statistics	MDM 프록시 서비스 통계를 표시합니다.
mdm-proxy	MDM 프록시 서비스를 구성하기 위해 config-mdm-proxy 모드를 시작합니다.

clear memory delayed-free-poisoner

지연된 여유 메모리 포이즈너(poisoner) 툴 대기열 및 통계를 지우려면 특별 권한 EXEC 모드에서 **clear memory delayed-free-poisoner** 명령을 사용합니다.

clear memory delayed-free-poisoner

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear memory delayed-free-poisoner 명령은 지연된 여유 메모리 포이즈너 툴 대기열에 있던 모든 메모리를 유효성 검사 없이 시스템으로 반환하고 관련 통계 카운터를 지웁니다.

예

다음 예에서는 지연된 여유 메모리 포이즈너 툴 대기열 및 통계를 지웁니다.

```
ciscoasa# clear memory delayed-free-poisoner
```

관련 명령

명령	설명
memory delayed-free-poisoner enable	지연된 여유 메모리 포이즈너 툴을 활성화합니다.
memory delayed-free-poisoner validate	지연된 여유 메모리 포이즈너 툴 대기열에 대한 유효성 검사를 강제로 실행합니다.
show memory delayed-free-poisoner	지연된 여유 메모리 포이즈너 툴 대기열의 사용량 요약을 표시합니다.

clear memory profile

메모리 프로파일링 기능에서 보유한 메모리 버퍼를 지우려면 특별 권한 EXEC 모드에서 **clear memory profile** 명령을 사용합니다.

clear memory profile [peak]

구문 설명

peak	(선택 사항) 피크 메모리 버퍼의 내용을 지웁니다.

기본값

기본적으로 현재 "사용 중" 프로필 버퍼를 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear memory profile 명령은 프로파일링 기능에서 보유하던 메모리 버퍼를 릴리스합니다. 따라서 지우기 전에 프로파일링을 중지해야 합니다.

예

다음 예에서는 프로파일링 기능에서 보유하던 메모리 버퍼를 지웁니다.

```
ciscoasa# clear memory profile
```

관련 명령

명령	설명
memory profile enable	메모리 사용량(메모리 프로파일링)의 모니터링을 활성화합니다.
memory profile text	프로파일링할 메모리의 텍스트 범위를 구성합니다.
show memory profile	ASA의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.

clear mfib counters

MFIB 라우터 패킷 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear mfib counters** 명령을 사용합니다.

clear mfib counters [*group* [*source*]]

구문 설명

group	(선택 사항) 멀티캐스트 그룹의 IP 주소.
source	(선택 사항) 멀티캐스트 경로 소스의 IP 주소. 이는 점으로 구분된 4개의 십진수로 표기되는 고유한 IP 주소입니다.

기본값

이 명령을 인수 없이 사용하면 모든 경로의 경로 카운터가 지워집니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 모든 MFIB 라우터 패킷 카운터를 지웁니다.

```
ciscoasa# clear mfib counters
```

관련 명령

명령	설명
show mfib count	MFIB 경로 및 패킷 수 데이터를 표시합니다.

clear module

ASA의 SSM, ASA 5505의 SSC, ASA 5585-X에 설치된 SSP, ASA 5585-X에 설치된 IPS SSP, ASA Services Module에 대한 정보와 시스템 정보를 지우려면 특별 권한 EXEC 모드에서 **clear module** 명령을 사용합니다.

clear module [*mod_id* | *slot*] [**all** | [**details** | **recover** | **log** [**console**]]]

구문 설명

all	(기본값) 모든 SSM 정보를 지웁니다.
console	(선택 사항) 모듈의 콘솔 로그 정보를 지웁니다.
details	(선택 사항) SSM의 원격 관리 컨피그레이션(예: ASA-SSM-*x*0)을 포함한 추가 정보를 지웁니다.
log	(선택 사항) 모듈의 로그 정보를 지웁니다.
mod_id	IPS와 같은 소프트웨어 모듈에 사용된 모듈 이름을 지웁니다.
recover	(선택 사항) SSM에 대해 **hw-module module recover** 명령의 설정을 지웁니다. **참고** **recover** 키워드는 **configure** 키워드와 **hw-module module recover** 명령을 사용하여 SSM 에 대한 복구 컨피그레이션을 생성한 경우에만 유효합니다 . (선택 사항) ASA 5512-X, 5515-X, 5525-X, 5545-X 또는 5555-X에 설치된 IPS 모듈에 대해서는 **sw-module module** *mod_id* **recover configure image** *image_location* 명령의 설정을 지웁니다.
slot	모듈 슬롯 번호(0 또는 1)를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.2(1)	SSC를 지원합니다.
8.2(5)	ASA 5585-X 및 ASA 5585-X의 IPS SSP를 지원합니다.
8.4(2)	이중 SSP 설치를 지원합니다.
8.5(1)	ASASM을 지원합니다.
8.6(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X를 지원합니다.

사용 지침

이 명령은 SSC, SSM, ASASM, IPS SSP, 디바이스 인터페이스와 내장형 인터페이스에 대한 정보를 지웁니다.

예

다음 예에서는 SSM에 대한 복구 설정을 지웁니다.

```
ciscoasa# clear module 1 recover
```

관련 명령

명령	설명
hw-module module recover	TFTP 서버에서 복구 이미지를 로드하여 SSM을 복구합니다.
hw-module module reset	SSM를 종료하고 하드웨어 재설정을 수행합니다.
hw-module module reload	SSM 소프트웨어를 다시 로드합니다.
hw-module module shutdown	컨피그레이션 데이터를 잃지 않고 전원을 끄기 위한 준비 단계로 SSM 소프트웨어를 종료합니다.
show module	SSM 정보를 표시합니다.

clear nac-policy

NAC 정책 사용량 통계를 재설정하려면 글로벌 컨피그레이션 모드에서 **clear nac-policy** 명령을 사용합니다.

clear nac-policy [*nac-policy-name*]

구문 설명

nac-policy-name	(선택 사항) 사용량 통계를 재설정할 NAC 정책의 이름

기본값

이름을 지정하지 않을 경우 CLI는 모든 NAC 정책에 대한 사용량 통계를 재설정합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

예

다음 예에서는 framework1이라는 이름의 NAC 정책에 대한 사용량 통계를 재설정합니다.

```
ciscoasa(config)# clear nac-policy framework1
```

다음 예에서는 모든 NAC 정책 사용량 통계를 재설정합니다.

```
ciscoasa(config)# clear nac-policy
```

관련 명령

명령	설명
show nac-policy	ASA의 NAC 정책 사용량 통계를 표시합니다.
show vpn-session_summary.db	IPsec, WebVPN, NAC 세션의 수를 표시합니다.
show vpn-session.db	NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.

clear nat counters

NAT 정책 카운터를 지우려면 글로벌 컨피그레이션 모드에서 **clear nat counters** 명령을 사용합니다.

clear nat counters [*src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

구문 설명

dst_ifc	(선택 사항) 필터링할 목적지 인터페이스를 지정합니다.
dst_ip	(선택 사항) 필터링할 목적지 IP 주소를 지정합니다.
dst_mask	(선택 사항) 목적지 IP 주소의 마스크를 지정합니다.
src_ifc	(선택 사항) 필터링할 소스 인터페이스를 지정합니다.
src_ip	(선택 사항) 필터링할 소스 IP 주소를 지정합니다.
src_mask	(선택 사항) 소스 IP 주소의 마스크를 지정합니다.

기본값

이 명령은 기본 설정이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0 (4)	이 명령을 도입했습니다.

예

이 예에서는 NAT 정책 카운터를 지우는 방법을 보여줍니다.

```
ciscoasa(config)# clear nat counters
```

관련 명령

명령	설명
nat	어떤 인터페이스에 있는 주소로서 다른 인터페이스의 매핑된 주소로 변환된 것입니다.
nat-control	NAT 컨피그레이션 요구 사항을 활성화하거나 비활성화합니다.
show nat counters	프로토콜 스택 카운터를 표시합니다.

clear object-group

네트워크 객체 그룹에 속한 객체의 계수기를 지우려면 특별 권한 모드에서 **show object-group** 명령을 사용합니다.

clear object-group *obj-name* **counters**

구문 설명

counters	네트워크 객체 그룹의 카운터를 나타냅니다.
obj-name	기존 네트워크 객체 그룹을 나타냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

사용 지침

네트워크 객체 그룹에 속한 객체의 히트 수만 지울 때 이 명령을 사용합니다.

예

다음 예에서는 "Anet"라는 네트워크 객체 그룹의 네트워크 객체 히트 수를 지우는 방법을 보여줍니다.

```
ciscoasa# clear object-group Anet counters
```

관련 명령

명령	설명
show object-group	객체 그룹 정보를 표시하고, 지정된 객체 그룹이 네트워크 객체 그룹 유형일 경우 히트 수를 표시합니다.

clear ospf

OSPF 프로세스 정보를 지우려면 특별 권한 EXEC 모드에서 **clear ospf** 명령을 사용합니다.

clear ospf [*pid***] {process | counters}**

구문 설명

counters	OSPF 카운터를 지웁니다.
pid	(선택 사항) OSPF 라우팅 프로세스를 위한 식별 매개변수로서 내부에서 사용합니다. 유효한 값의 범위는 1~65535입니다.
process	OSPF 라우팅 프로세스를 다시 시작합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

이 명령은 컨피그레이션의 어느 부분도 제거하지 않습니다. 이 컨피그레이션 명령의 **no** 형식을 사용하여 특정 명령을 컨피그레이션에서 지우거나 **clear configure router ospf** 명령을 사용하여 모든 전역 OSPF 명령을 컨피그레이션에서 제거할 수 있습니다.

참고 **clear configure router ospf** 명령은 인터페이스 컨피그레이션 모드에서 입력한 OSPF 명령을 지우지 않습니다.

예

다음 예에서는 OSPF 네이버 카운터를 지우는 방법을 보여줍니다.

```
ciscoasa# clear ospf counters
```

관련 명령

명령	설명
clear configure router	실행 중인 컨피그레이션에서 모든 전역 라우터 명령을 지웁니다.

clear pclu

PC 논리적 업데이트 통계를 지우려면 특별 권한 EXEC 모드에서 **clear pclu** 명령을 사용합니다.

clear pclu

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 PC 정보를 지웁니다.

```
ciscoasa# clear pclu
```

clear phone-proxy secure-phones

전화 프록시 데이터베이스에서 보안 전화 엔트리를 지우려면 특별 권한 EXEC 모드에서 **clear phone-proxy secure-phones** 명령을 사용합니다.

clear phone-proxy secure-phones [*mac_address* **| noconfirm]**

구문 설명

mac_address	전화 프록시 데이터베이스에서 지정된 MAC 주소의 IP 전화기를 제거합니다.
noconfirm	확인 프롬프트 없이 전화 프록시 데이터베이스의 모든 보안 전화 엔트리를 제거합니다. **noconfirm** 키워드를 지정하지 않을 경우 모든 보안 전화 엔트리를 제거할지 묻는 프롬프트가 나타납니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

보안 전화기는 항상 부팅 시 CTL 파일을 필요로 하므로 전화기 프록시는 해당 전화기를 보안 상태로 표시하는 데이터베이스를 만듭니다. 보안 전화 데이터베이스의 엔트리는 (**timeout secure-phones** 명령으로 지정된) 시간 초과 이후에 제거됩니다. 또는 **clear phone-proxy secure-phones** 명령을 사용하여 구성된 시간 초과만큼 기다리지 않고 전화 프록시 데이터베이스를 지울 수 있습니다.

예

다음 예에서는 전화 프록시 데이터베이스의 보안 엔트리를 지웁니다.

```
ciscoasa# clear phone-proxy secure-phones 001c.587a.4000
```

관련 명령

명령	설명
timeout secure-phones	유휴 타이머를 구성합니다. 이 시간이 경과하면 보안 전화 엔트리가 전화 프록시 데이터베이스에서 제거됩니다.

clear pim counters

PIM 트래픽 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear pim counters** 명령을 사용합니다.

clear pim counters

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 트래픽 카운터만 지웁니다. PIM 토폴로지 테이블을 지우려면 **clear pim topology** 명령을 사용합니다.

예

다음 예에서는 PIM 트래픽 카운터를 지웁니다.

```
ciscoasa# clear pim counters
```

관련 명령

명령	설명
clear pim reset	강제적으로 재설정을 통한 MRIB 동기화를 수행합니다.
clear pim topology	PIM 토폴로지 테이블을 지웁니다.
show pim traffic	PIM 트래픽 카운터를 표시합니다.

clear pim reset

강제적으로 재설정을 통해 MRIB 동기화를 수행하려면 특별 권한 EXEC 모드에서 **clear pim reset** 명령을 사용합니다.

clear pim reset

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

토폴로지 테이블의 모든 정보가 지워지며 MRIB 연결이 재설정됩니다. 이 명령은 PIM 토폴로지 테이블과 MRIB 데이터베이스 간의 상태를 동기화하는 데 사용할 수 있습니다.

예

다음 예에서는 토폴로지 테이블을 지우고 MRIB 연결을 재설정합니다.

```
ciscoasa# clear pim reset
```

관련 명령

명령	설명
clear pim counters	PIM 카운터 및 통계를 지웁니다.
clear pim topology	PIM 토폴로지 테이블을 지웁니다.
clear pim counters	PIM 트래픽 카운터를 지웁니다.

clear pim topology

PIM 토폴로지 테이블을 지우려면 특별 권한 EXEC 모드에서 **clear pim topology** 명령을 사용합니다.

clear pim topology [*group*]

구문 설명

group	(선택 사항) 토폴로지 테이블에서 삭제할 멀티캐스트 주소 또는 이름을 지정합니다.

기본값

선택 사항인 *group* 인수가 없으면 토폴로지 테이블의 모든 엔트리가 지워집니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 PIM 토폴로지 테이블에서 기존 PIM 경로를 지웁니다. IGMP 로컬 멤버십과 같이 MRIB 테이블에서 얻은 정보는 보존됩니다. 멀티캐스트 그룹이 지정될 경우 그 그룹의 엔트리만 지워집니다.

예

다음 예에서는 PIM 토폴로지 테이블을 지웁니다.

```
ciscoasa# clear pim topology
```

관련 명령

명령	설명
clear pim counters	PIM 카운터 및 통계를 지웁니다.
clear pim reset	강제적으로 재설정을 통한 MRIB 동기화를 수행합니다.
clear pim counters	PIM 트래픽 카운터를 지웁니다.

clear priority-queue statistics

어떤 인터페이스 또는 구성된 모든 인터페이스의 우선 순위 대기열 통계 카운터를 지우려면 글로벌 컨피그레이션 또는 특별 권한 EXEC 모드 중 하나에서 **clear priority-queue statistics** 명령을 사용합니다.

clear priority-queue statistics [*interface-name***]**

구문 설명

interface-name	(선택 사항) BE(best-effort) 및 LLQ(low-latency queue) 세부 정보를 표시할 인터페이스의 이름을 지정합니다.

기본값

인터페이스 이름을 생략할 경우 이 명령은 구성된 모든 인터페이스의 우선 순위 대기열 통계를 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	• 예	—
글로벌 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 "test"라는 인터페이스의 우선 순위 대기열 통계를 제거하기 위해 특별 권한 EXEC 모드에서 **clear priority-queue statistics** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa# clear priority-queue statistics test
ciscoasa#
```

관련 명령

명령	설명
clear configure priority queue	명명된 인터페이스에서 우선 순위 대기열 컨피그레이션을 제거합니다.
priority-queue	인터페이스의 우선 순위 큐잉을 구성합니다.
show priority-queue statistics	지정된 인터페이스 또는 모든 인터페이스의 우선 순위 대기열 통계를 표시합니다.
show running-config priority-queue	명명된 인터페이스의 현재 우선 순위 대기열 컨피그레이션을 표시합니다.

clear process

ASA에서 실행 중인 지정된 프로세스의 통계를 지우려면 특별 권한 EXEC 모드에서 **clear process** 명령을 사용합니다.

clear process [cpu-hog | internals]

구문 설명

cpu-hog	CPU 과다 사용 통계를 지웁니다.
internals	프로세스 내부 통계를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 CPU 과다 사용 통계를 지우는 방법을 보여줍니다.

```
ciscoasa# clear process cpu-hog
ciscoasa#
```

관련 명령

명령	설명
cpu hog granular-detection	실시간 CPU 과다 사용 탐지 정보를 트리거합니다.
show processes	ASA에서 실행 중인 프로세스의 목록을 표시합니다.

clear resource usage

리소스 사용량 통계를 지우려면 특별 권한 EXEC 모드에서 **clear resource usage** 명령을 사용합니다.

clear resource usage [context *context_name* **| all | summary | system] [resource {[rate]** *resource_name* **| all}]**

구문 설명

context *context_name*	(다중 모드만) 통계를 지우려는 컨텍스트 이름을 지정합니다. 모든 컨텍스트에는 **all**(기본 설정)을 지정합니다.
resource [**rate**] *resource_name*	특정 리소스의 사용량을 지웁니다. 모든 리소스에는 **all**(기본 설정)을 지정합니다. 리소스의 사용률을 지우려면 **rate**를 지정합니다. **conns**, **inspects**, **syslogs**와 같은 리소스가 사용률을 기준으로 측정됩니다. 이 리소스 유형에는 **rate** 키워드를 지정해야 합니다. conns 리소스는 동시 연결 수로도 측정됩니다. 초당 연결 수를 볼 때만 **rate** 키워드를 사용합니다. 리소스는 다음과 같은 유형이 있습니다. • **asdm**—ASDM 관리 세션. • **conns**—임의의 두 호스트 간의 TCP 또는 UDP 연결. 어떤 호스트와 다른 여러 호스트 간의 연결도 포함됩니다. • **inspects**—애플리케이션 검사. • **hosts**—ASA를 통해 연결될 수 있는 호스트. • **mac-addresses**—투명 방화벽 모드의 경우 MAC 주소 테이블에서 허용되는 MAC 주소의 수. • **ssh**—SSH 세션. • **syslogs**—Syslog 메시지. • **telnet**—텔넷 세션. • (다중 모드만) **VPN Other**—사이트 대 사이트 VPN 세션. • (다중 모드만) **VPN Burst Other**—사이트 대 사이트 VPN 버스트 세션. • **xlates**—NAT 변환.
summary	(다중 모드만) 종합 컨텍스트 통계를 지웁니다.
system	(다중 모드만) 시스템 전반(전역) 사용량 통계를 지웁니다.

기본값

다중 컨텍스트 모드에서는 기본 컨텍스트가 **all**입니다. 즉 모든 컨텍스트의 리소스 사용량을 지웁니다. 단일 모드에서는 컨텍스트 이름이 무시되며 모든 리소스 통계가 지워집니다.

기본 리소스 이름은 **all**이며, 모든 리소스 유형을 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 모든 컨텍스트의 모든 리소스 사용량 통계를 지우지만, 시스템 전반 사용량 통계는 지우지 않습니다.

```
ciscoasa# clear resource usage
```

다음 예에서는 시스템 전반 사용량 통계를 지웁니다.

```
ciscoasa# clear resource usage system
```

관련 명령

명령	설명
context	보안 컨텍스트를 추가합니다.
show resource types	리소스 유형의 목록을 표시합니다.
show resource usage	ASA의 리소스 사용량을 표시합니다.

clear route all

동적으로 학습한 경로를 컨피그레이션에서 제거하려면 특별 권한 EXEC 모드에서 **clear route all** 명령을 사용합니다.

clear route all

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 동적으로 학습한 경로를 제거하는 방법을 보여줍니다.

```
ciscoasa# clear route all
```

관련 명령

명령	설명
clear route *network* <*mask*>	지정된 목적지 경로를 제거합니다.
show route	경로 정보를 표시합니다.
show running-config route	구성된 경로를 표시합니다.

clear route *network<mask>*

지정된 목적지 경로를 제거하려면 특별 권한 EXEC 모드에서 **clear route** *network* <*mask*> 명령을 사용합니다.

clear route [*ip_address ip_mask*]

구문 설명

ip_address ip_mask	제거할 목적지 IP 주소 및 서브넷 마스크를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 동적으로 학습한 경로를 제거하는 방법을 보여줍니다.

```
ciscoasa# clear route 10.118.86.3
```

관련 명령

명령	설명
clear route all	모든 경로를 제거하고 새로 고칩니다.
show route	경로 정보를 표시합니다.
show running-config route	구성된 경로를 표시합니다.

clear service-policy

활성화된 정책의 운영 데이터 또는 통계(있는 경우)를 지우려면 특별 권한 EXEC 모드에서 **clear service-policy** 명령을 사용합니다.

clear service-policy [global | interface *intf* **] [user-statistics]**

구문 설명

global	(선택 사항) 전역 서비스 모델의 통계를 지웁니다.
interface *intf*	(선택 사항) 특정 인터페이스의 서비스 정책 통계를 지웁니다.
user-statistics	(선택 사항) 사용자 통계에 대한 전역 카운터를 지우지만 사용자별 통계는 지우지 않습니다. 사용자별 또는 사용자 그룹별 통계는 **show user-identity statistics** 명령으로 계속 볼 수 있습니다. **accounting** 키워드가 **user-statistics** 명령에 대해 지정될 경우 전송된 패킷, 수신된 패킷, 전송되었으나 삭제된 패킷에 대한 모든 전역 카운터가 지워집니다. **scanning** 키워드 **user-statistics** 명령이 지정될 경우 전송되었으나 삭제된 패킷의 전역 카운터가 지워집니다. ASA에서 이 사용자 통계를 수집하려면 사용자 통계를 수집하도록 정책 맵을 구성해야 합니다. 본 설명서의 **user-statistics** 명령을 참조하십시오.

기본값

기본적으로 이 명령은 활성화된 모든 서비스 정책의 모든 통계를 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

검사 엔진에 대한 서비스 정책 통계를 지우려면 **clear service-policy inspect** 명령을 참조하십시오.

예

다음 예에서는 **clear service-policy** 명령의 구문을 보여줍니다.

```
ciscoasa# clear service-policy outside_security_map interface outside
```

관련 명령

명령	설명
clear service-policy inspect gtp	GTP 검사 엔진에 대한 서비스 정책 통계를 지웁니다.
clear service-policy inspect radius-accounting	RADIUS 어카운팅 검사 엔진에 대한 서비스 정책 통계를 지웁니다.
show service-policy	서비스 정책을 표시합니다.
show running-config service-policy	실행 중인 컨피그레이션에 구성된 서비스 정책을 표시합니다.
clear configure service-policy	서비스 정책 컨피그레이션을 지웁니다.
service-policy	서비스 정책을 구성합니다.

clear service-policy inspect gtp

전역 GTP 통계를 지우려면 특별 권한 EXEC 모드에서 **clear service-policy inspect gtp** 명령을 사용합니다.

clear service-policy inspect gtp {pdp-context [all | apn *ap_name* **| imsi** *IMSI_value* **| ms-addr** *IP_address* **| tid** *tunnel_ID* **| version** *version_num* **] | requests | statistics [gsn** *IP_address***] }**

구문 설명.

all	모든 GTP PDP 컨텍스트를 지웁니다.
apn	(선택 사항) 지정된 APN에 따라 PDP 컨텍스트를 지웁니다.
ap_name	특정 액세스 포인트 이름을 나타냅니다.
gsn	(선택 사항) GPRS 지원 노드를 나타냅니다. 이는 GPRS 무선 데이터 네트워크와 기타 네트워크 간의 인터페이스입니다.
gtp	(선택 사항) GTP의 서비스 정책을 지웁니다.
imsi	(선택 사항) 지정된 IMSI에 따라 PDP 컨텍스트를 지웁니다.
IMSI_value	특정 IMSI를 나타내는 16진수 값.
interface	(선택 사항) 특정 인터페이스를 나타냅니다.
int	정보를 지울 인터페이스를 나타냅니다.
IP_address	통계를 지울 IP 주소.
ms-addr	(선택 사항) 지정된 MS 주소에 따라 PDP 컨텍스트를 지웁니다.
pdp-context	(선택 사항) 패킷 데이터 프로토콜 컨텍스트를 나타냅니다.
requests	(선택 사항) GTP 요청을 지웁니다.
statistics	(선택 사항) **inspect gtp** 명령에 대한 GTP 통계를 지웁니다.
tid	(선택 사항) 지정된 TID에 따라 PDP 컨텍스트를 지웁니다.
tunnel_ID	특정 터널을 나타내는 16진수 값.
version	(선택 사항) GTP 버전에 따라 PDP 컨텍스트를 지웁니다.
version_num	PDP 컨텍스트의 버전을 지정합니다. 유효한 값의 범위는 0~255입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

패킷 데이터 프로토콜 컨텍스트는 터널 ID로 식별되며, 이는 IMSI와 NSAPI의 조합입니다. GTP 터널은 서로 다른 GSN 노드에 있는 두 개의 관련된 PDP 컨텍스트에 의해 정의되며 터널 ID로 식별됩니다. 외부 패킷 데이터 네트워크와 MS(모바일 스테이션) 사용자 간에 패킷을 전달하려면 GTP 터널이 필요합니다.

예

다음 예에서는 GTP 통계를 지웁니다.

```
ciscoasa# clear service-policy inspect gtp statistics
```

관련 명령

명령	설명
debug gtp	GTP 검사에 대한 세부 정보를 표시합니다.
gtp-map	GTP 맵을 정의하고 GTP 맵 컨피그레이션 모드를 활성화합니다.
inspect gtp	애플리케이션 검사에 사용할 GTP 맵을 적용합니다.
show service-policy inspect gtp	GTP 컨피그레이션을 표시합니다.
show running-config gtp-map	구성된 GTP 맵을 표시합니다.

clear service-policy inspect radius-accounting

RADIUS 어카운팅 사용자를 지우려면 특별 권한 EXEC 모드에서 **clear service-policy inspect radius-accounting** 명령을 사용합니다.

clear service-policy inspect radius-accounting users {all | *ip_address* | *policy_map*}

구문 설명.

all	모든 사용자를 지웁니다.
ip_address	이 IP 주소의 사용자를 지웁니다.
policy_map	이 정책 맵과 연관된 사용자를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 모든 RADIUS 어카운팅 사용자를 지웁니다.

```
ciscoasa# clear service-policy inspect radius-accounting users all
```

clear shared license

공유 라이센스 통계, 공유 라이센스 클라이언트 통계, 공유 라이센스 백업 서버 통계를 0으로 재설정하려면 특별 권한 EXEC 모드에서 **clear shared license** 명령을 사용합니다.

clear shared license [all | backup | client [*hostname***]]**

구문 설명

all	(선택 사항) 모든 통계를 지웁니다. 이는 기본 설정입니다.
backup	(선택 사항) 백업 서버의 통계를 지웁니다.
client	(선택 사항) 모든 참가자의 통계를 지웁니다.
hostname	(선택 사항) 특정 참가자의 통계를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

공유 라이센스 카운터는 통계 데이터 및 오류 데이터를 포함합니다.

예

다음 예에서는 모든 공유 라이센스 카운터를 재설정하는 방법을 보여줍니다.

```
ciscoasa# clear shared license all
```

관련 명령

명령	설명
activation-key	라이센스 활성화 키를 입력합니다.
clear configure license-server	공유 라이센스 서버 컨피그레이션을 지웁니다.
license-server address	어떤 참가자의 공유 라이센스 서버 IP 주소와 공유 암호를 식별합니다.
license-server backup address	어떤 참가자의 공유 라이센스 백업 서버를 나타냅니다.
license-server backup backup-id	기본 공유 라이센스 서버의 백업 서버 IP 주소 및 일련 번호를 나타냅니다.
license-server backup enable	어떤 유닛이 공유 라이센스 백업 서버가 될 수 있게 합니다.
license-server enable	어떤 유닛이 공유 라이센스 서버가 될 수 있게 합니다.
license-server port	서버가 참가자로부터 SSL 연결을 수신하는 포트를 설정합니다.
license-server refresh-interval	참가자와 서버의 통신 빈도를 설정하기 위해 사용자에게 제공되는 새로 고침 간격을 설정합니다.
license-server secret	공유 라이센스 서버에 대한 공유 암호를 설정합니다.
show activation-key	설치된 현재 라이센스를 표시합니다.
show running-config license-server	공유 라이센스 서버 컨피그레이션을 표시합니다.
show shared license	공유 라이센스 통계를 표시합니다.
show vpn-sessiondb	VPN 세션에 대한 라이센스 정보가 표시됩니다.

clear shun

현재 활성화된 모든 차단을 비활성화하고 차단 통계를 지우려면 특별 권한 EXEC 모드에서 **clear shun** 명령을 사용합니다.

clear shun [*statistics*]

구문 설명

statistics	(선택 사항) 인터페이스 카운터만 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 현재 활성화된 모든 차단을 비활성화하고 차단 통계를 지우는 방법을 보여줍니다.

```
ciscoasa(config)# clear shun
```

관련 명령

명령	설명
shun	신규 연결을 막고 기존 연결에서의 패킷 전송을 허용하지 않음으로써 공격 호스트에 대한 동적 응답을 활성화합니다.
show shun	차단 정보를 표시합니다.

clear snmp-server statistics

SNMP 서버 통계(SNMP 패킷 입력 및 출력 카운터)를 지우려면 특별 권한 EXEC 모드에서 **clear snmp-server statistics** 명령을 사용합니다.

clear snmp-server statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 SNMP 서버 통계를 지우는 방법을 보여줍니다.

```
ciscoasa# clear snmp-server statistics
```

관련 명령

명령	설명
clear configure snmp-server	SNMP 서버 컨피그레이션을 지웁니다.
show snmp-server statistics	SNMP 서버 컨피그레이션 정보를 표시합니다.

clear ssl

디버깅 목적으로 SSL 정보를 지우려면 특별 권한 EXEC 모드에서 **clear ssl** 명령을 사용합니다.

clear ssl {cache [**all**] | errors | mib | objects}

구문 설명

all	SSL 세션 캐시의 모든 세션 및 통계를 지웁니다.
cache	SSL 세션 캐시에서 만료된 세션을 지웁니다.
errors	ssl 오류를 지웁니다.
mib	SSL MIB 통계를 지웁니다.
objects	SSL 객체 통계를 지웁니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.

사용 지침

DTLS 캐시는 지우지 않습니다. AnyConnect 기능에 영향을 주기 때문입니다.

예

다음 예에서는 ssl 캐시를 지우고 SSL 세션 캐시의 모든 세션 및 통계를 지우는 것을 보여줍니다.

```
ciscoasa# clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared

ciscoasa# clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

clear startup-config errors

메모리에서 컨피그레이션 오류 메시지를 지우려면 특별 권한 EXEC 모드에서 **clear startup-config errors** 명령을 사용합니다.

clear startup-config errors

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서 시작 컨피그레이션을 로드했을 때 발생한 컨피그레이션 오류를 보려면 **show startup-config errors** 명령을 사용합니다.

예

다음 예에서는 메모리에서 모든 컨피그레이션 오류를 지웁니다.

```
ciscoasa# clear startup-config errors
```

관련 명령

명령	설명
show startup-config errors	ASA에서 시작 컨피그레이션을 로드했을 때 발생한 컨피그레이션 오류를 표시합니다.

clear sunrpc-server active

Sun RPC 애플리케이션 검사에서 연 핀홀을 지우려면 특별 권한 EXEC 모드에서 **clear sunrpc-server active** 명령을 사용합니다.

clear sunrpc-server active

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear sunrpc-server active 명령을 사용하면 Sun RPC 애플리케이션 검사에서 열었고 NFS, NIS와 같은 서비스 트래픽의 ASA 통과를 가능하게 하는 핀홀을 지울 수 있습니다.

예

다음 예에서는 SunRPC 서비스 테이블을 지우는 방법을 보여줍니다.

```
ciscoasa# clear sunrpc-server
```

관련 명령

명령	설명
clear configure sunrpc-server	Sun 원격 프로세서 통화 서비스를 ASA에서 지웁니다.
inspect sunrpc	Sun RPC 애플리케이션 검사를 활성화하거나 비활성화하고 사용된 포트를 구성합니다.
show running-config sunrpc-server	SunRPC 서비스 컨피그레이션에 대한 정보를 표시합니다.
show sunrpc-server active	활성 Sun RPC 서비스에 대한 정보를 표시합니다.

clear threat-detection rate

threat-detection basic-threat 명령을 사용하여 기본 위협 감지를 활성화할 때 통계를 지우려면 특별 권한 EXEC 모드에서 **clear threat detection rate** 명령을 사용합니다.

clear threat-detection rate

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

예

다음 예에서는 비율 통계를 지웁니다.

```
ciscoasa# clear threat-detection rate
```

관련 명령

명령	설명
show running-config all threat-detection	위협 감지 컨피그레이션(개별적으로 구성하지 않은 경우 기본 비율 설정 포함)을 표시합니다.
show threat-detection rate	기본 위협 감지 통계를 표시합니다.
threat-detection basic-threat	기본 위협 감지를 활성화합니다.
threat-detection rate	이벤트 유형별 위협 감지율 한도를 설정합니다.
threat-detection scanning-threat	위협 감지 검사를 활성화합니다.

clear threat-detection scanning-threat

threat-detection scanning-threat 명령으로 위협 감지 검사를 활성화한 다음 공격자 및 대상을 지우려면 특별 권한 EXEC 모드에서 **clear threat-detection scanning-threat** 명령을 사용합니다.

clear threat-detection scanning-threat [attacker [*ip_address* **[***mask***]] |**
target [*ip_address* **[***mask***]]**

구문 설명

attacker	(선택 사항) 공격자만 지웁니다.
ip_address	(선택 사항) 특정 IP 주소를 지웁니다.
mask	(선택 사항) 서브넷 마스크를 설정합니다.
target	(선택 사항) 대상만 지웁니다.

기본값

IP 주소를 지정하지 않을 경우 모든 호스트가 릴리스됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

현재 공격자 및 대상을 보려면 **show threat-detection scanning-threat** 명령을 사용합니다.

예

다음 예에서는 **show threat-detection scanning-threat** 명령으로 대상과 공격자를 표시한 다음 모든 대상을 지웁니다.

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
ciscoasa# clear threat-detection scanning-threat target
```

관련 명령

명령	설명
show threat-detection shun	현재 차단된 호스트를 표시합니다.
show threat-detection statistics host	호스트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
show threat-detection statistics top	상위 10개 통계를 표시합니다.
threat-detection scanning-threat	위협 감지 검사를 활성화합니다.

clear threat-detection shun

threat-detection scanning-threat 명령으로 위협 감지 검사를 활성화하고 공격 호스트 자동 차단을 활성화한 다음 현재 차단된 호스트를 릴리스하려면 특별 권한 EXEC 모드에서 **clear threat-detection shun** 명령을 사용합니다.

clear threat-detection shun [*ip_address* **[***mask***]]**

구문 설명

ip_address	(선택 사항) 특정 IP 주소를 차단에서 릴리스합니다.
mask	(선택 사항) 차단된 호스트 IP 주소에 대한 서브넷 마스크를 설정합니다.

기본값

IP 주소를 지정하지 않을 경우 모든 호스트가 릴리스됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

현재 차단된 호스트를 보려면 **show threat-detection shun** 명령을 사용합니다.

예

다음 예에서는 **show threat-detection shun** 명령으로 현재 차단된 호스트를 표시한 다음 호스트 10.1.1.6의 차단을 릴리스합니다.

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
ciscoasa# clear threat-detection shun 10.1.1.6 255.255.255.255
```

관련 명령

명령	설명
show threat-detection shun	현재 차단된 호스트를 표시합니다.
show threat-detection statistics host	호스트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
show threat-detection statistics top	상위 10개 통계를 표시합니다.
threat-detection scanning-threat	위협 감지 검사를 활성화합니다.

clear threat-detection statistics

threat-detection statistics tcp-intercept 명령으로 TCP 인터셉트 통계를 활성화한 다음 통계를 지우려면 특별 권한 EXEC 모드에서 **clear threat-detection scanning-threat** 명령을 사용합니다.

clear threat-detection statistics [tcp-intercept]

구문 설명

tcp-intercept	(선택 사항) TCP 인터셉트 통계를 지웁니다.

기본값

TCP 인터셉트 통계를 지웁니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

TCP 인터셉트 통계를 보려면 **show threat-detection statistics top** 명령을 입력합니다.

예

다음 예에서는 **show threat-detection statistics top tcp-intercept** 명령으로 TCP 인터셉트 통계를 표시한 다음 모든 통계를 지웁니다.

```
ciscoasa# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)

ciscoasa# clear threat-detection statistics
```

관련 명령

명령	설명
show threat-detection statistics top	상위 10개 통계를 표시합니다.
threat-detection statistics	위협 감지 통계를 활성화합니다.

clear traffic

전송 및 수신 활동에 대한 카운터를 재설정하려면 특별 권한 EXEC 모드에서 **clear traffic** 명령을 사용합니다.

clear traffic

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear traffic 명령은 **show traffic** 명령과 함께 표시된 전송 및 수신 활동의 카운터를 재설정합니다. 이 카운터는 마지막으로 clear traffic 명령을 입력한 이후 또는 ASA가 온라인 상태가 된 이후 각 인터페이스를 지난 패킷 및 바이트 수를 나타냅니다. 그리고 초 수는 ASA가 마지막 재부팅 후 온라인 상태를 유지한 기간을 나타냅니다.

예

다음 예에서는 **clear traffic** 명령을 보여줍니다.

```
ciscoasa# clear traffic
```

관련 명령

명령	설명
show traffic	전송 및 수신 활동에 대한 카운터를 표시합니다.

clear uauth

어떤 사용자 또는 모든 사용자에 대해 캐싱된 모든 인증 및 권한 부여 정보를 삭제하려면 특별 권한 EXEC 모드에서 **clear uauth** 명령을 사용합니다.

clear uauth [*username*]

구문 설명

username	(선택 사항) 사용자 이름을 기준으로 제거할 사용자 인증 정보를 지정합니다.

기본값

username 인수를 생략하면 모든 사용자의 인증 및 권한 부여 정보를 삭제합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear uauth 명령은 어떤 사용자 또는 모든 사용자의 AAA 권한 부여 및 인증 캐시를 삭제합니다. 그러면 해당 사용자는 다음에 연결을 생성할 때 다시 인증해야 합니다.

이 명령은 **timeout** 명령과 함께 사용합니다.

각 사용자 호스트 IP 주소에는 권한 부여 캐시가 연결되어 있습니다. 사용자가 올바른 호스트에서 캐싱된 서비스에 액세스할 경우 ASA는 이미 권한 부여된 것으로 간주하고 즉시 연결을 프록시합니다. 이를테면 어떤 웹 사이트에 대한 액세스 권한이 부여된 경우 로드되는 각 이미지에 대해 (그 이미지가 동일한 IP 주소에서 온 것이라는 가정 하에) 권한 부여 서버에 연결하지 않습니다. 이러한 프로세스를 통해 성능이 크게 향상되고 권한 부여 서버에 대한 로드가 줄어듭니다.

캐시는 사용자 호스트별로 최대 16개의 주소 및 서비스 쌍을 허용합니다.

참고 Xauth를 활성화하면 클라이언트에 지정된 IP 주소에 대해 (**show uauth** 명령으로 표시되는) uauth 테이블에 엔트리가 추가됩니다. 그러나 Network Extension Mode에서 Xauth를 Easy VPN Remote와 함께 사용할 경우 네트워크 간에 IPsec 터널이 생성됩니다. 따라서 방화벽 뒤의 사용자가 단일 IP 주소와 연결될 수 없습니다. 이런 이유로 Xauth 완료 시 uauth 엔트리가 생성될 수 없습니다. AAA 권한 부여 또는 어카운팅 서버가 필요할 경우 AAA 인증 프록시에서 방화벽 뒤의 사용자를 인증하게 할 수 있습니다. AAA 인증 프록시에 대한 자세한 내용은 AAA 명령을 참조하십시오.

사용자 연결이 유휴 상태가 된 후 캐시를 유지할 기간을 지정하려면 **timeout uauth** 명령을 사용합니다. 모든 사용자의 모든 권한 부여 캐시를 삭제하려면 **clear uauth** 명령을 사용합니다. 그러면 사용자가 다음에 연결을 생성할 때 다시 인증해야 합니다.

예

다음 예에서는 사용자가 다시 인증하게 하는 방법을 보여줍니다.

```
ciscoasa(config)# clear uauth user
```

관련 명령

명령	설명
aaa authentication	(**aaa-server** 명령에 의해 지정된 서버에서) LOCAL, TACACS+ 또는 RADIUS 사용자 인증을 활성화, 비활성화하거나 표시합니다.
aaa authorization	(**aaa-server** 명령에 의해 지정된 서버에서) TACACS+ 또는 RADIUS 사용자 권한 부여를 활성화, 비활성화하거나 표시합니다.
show uauth	현재 사용자 인증 및 권한 부여 정보를 표시합니다.
timeout	최대 유휴 기간을 설정합니다.

clear uc-ime

Cisco Intercompany Media Engine 프록시에 대한 통계를 표시하는 데 쓰이는 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear uc-ime** 명령을 사용합니다.

clear uc-ime [[mapping-service-sessions | signaling-sessions | fallback-notification] statistics]

구문 설명

fallback-notification	(선택 사항) 폴백 알림 통계의 카운터를 지웁니다.
mapping-service-sessions	(선택 사항) mapping-service-session 통계의 카운터를 지웁니다.
signaling-sessions	(선택 사항) signaling-session 통계의 카운터를 지웁니다.
statistics	(선택 사항) Cisco Intercompany Media Engine 프록시에 대해 어떤 카운터를 지울지 구성하는 키워드.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

예

다음 예에서는 signaling-sessions 통계를 표시하는 데 사용되는 카운터를 지웁니다.

```
ciscoasa# clear configure signaling-sessions statistics
```

관련 명령

명령	설명
clear configure uc-ime	ASA의 Cisco Intercompany Media Engine 프록시에 대해 실행 중인 컨피그레이션을 지웁니다.
show running-config uc-ime	Cisco Intercompany Media Engine 프록시의 실행 중인 컨피그레이션을 표시합니다.
show uc-ime	폴백 알림, 매핑 서비스 세션, 시그널링 세션에 대한 통계 또는 세부 정보를 표시합니다.
uc-imc	ASA에 Cisco Intercompany Media Engine 프록시를 만듭니다.

clear url-block block statistics

블록 버퍼 사용량 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear url-block block statistics** 명령을 사용합니다.

clear url-block block statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear url-block block statistics 명령은 블록 버퍼 사용량 카운터를 지웁니다. 현재 보유 패킷 수(전역) 카운터는 제외합니다.

예

다음 예에서는 URL 블록 통계를 지우고 지워진 이후의 카운터 상태를 표시합니다.

```
ciscoasa# clear url-block block statistics
ciscoasa# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
-----------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

관련 명령

명령	설명
filter url	URL 필터링 서버로 트래픽을 전달합니다.
show url-block	URL 캐시에 대한 정보를 표시합니다. 이는 N2H2 또는 Websense 필터링 서버의 응답을 기다리는 동안 URL을 버퍼링하는 데 사용됩니다.
url-block	웹 서버 응답에 사용되는 URL 버퍼를 관리합니다.
url-cache	N2H2 또는 Websense 서버의 응답을 보류한 상태에서 URL 캐싱을 활성화하고 캐시의 크기를 설정합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

clear url-cache statistics

컨피그레이션에서 **url-cache** 명령문을 제거하려면 특별 권한 EXEC 모드에서 **clear url-cache** 명령을 사용합니다.

clear url-cache statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear url-cache 명령은 컨피그레이션에서 URL 캐시 통계를 제거합니다.

URL 캐시를 사용할 때 Websense 프로토콜 버전 1에 대한 Websense 어카운팅 로그는 업데이트하지 않습니다. Websense 프로토콜 버전 1을 사용하는 경우 Websense 실행으로 로그가 누락되게 합니다. 그러면 Websense 어카운팅 정보를 볼 수 있습니다. 보안 요구 사항에 부합하는 사용량 프로필을 얻은 다음 **url-cache** 명령을 입력하여 처리량을 늘립니다. **url-cache** 명령을 사용하는 동안 Websense 프로토콜 버전 4 및 N2H2 URL 필터링을 위한 어카운팅 로그가 업데이트됩니다.

예

다음 예에서는 URL 캐시 통계를 지웁니다.

```
ciscoasa# clear url-cache statistics
```

관련 명령

명령	설명
filter url	URL 필터링 서버로 트래픽을 전달합니다.
show url-cache statistics	URL 캐시에 대한 정보를 표시합니다. 이는 N2H2 또는 Websense 필터링 서버의 응답을 기다리는 동안 URL을 버퍼링하는 데 사용됩니다.
url-block	필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답에 사용할 URL 버퍼를 관리합니다.
url-cache	N2H2 또는 Websense 서버의 응답을 보류한 상태에서 URL 캐싱을 활성화하고 캐시의 크기를 설정합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

clear url-server

URL 필터링 서버 통계를 지우려면 특별 권한 EXEC 모드에서 **clear url-server** 명령을 사용합니다.

clear url-server statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear url-server 명령은 컨피그레이션에서 URL 필터링 서버 통계를 지웁니다.

예

다음 예에서는 URL 서버 통계를 지웁니다.

```
ciscoasa# clear url-server statistics
```

관련 명령

명령	설명
filter url	URL 필터링 서버로 트래픽을 전달합니다.
show url-server	URL 캐시에 대한 정보를 표시합니다. 이는 N2H2 또는 Websense 필터링 서버의 응답을 기다리는 동안 URL을 버퍼링하는 데 사용됩니다.
url-block	필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답에 사용할 URL 버퍼를 관리합니다.
url-cache	N2H2 또는 Websense 서버의 응답을 보류한 상태에서 URL 캐싱을 활성화하고 캐시의 크기를 설정합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

clear user-identity active-user-database

지정된 사용자의 상태를 ID 방화벽에서 로그아웃된 것으로 설정하려면 특별 권한 EXEC 모드에서 **clear user-identity active-user-database** 명령을 사용합니다.

clear user-identity active-user-database [user [*domain_nickname***\]***use_rname***] | user-group [***domain_nickname***\\]***user_group_name***]**

구문 설명

domain_nickname\\user_group_name	통계를 지울 사용자 그룹을 지정합니다. *group_name*은 [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.] 등 어떤 문자도 가능합니다. *domain_NetBIOS_name\group_name*이 공백을 포함할 경우 도메인 이름과 사용자 이름을 따옴표로 묶어야 합니다.
domain_nickname\use_rname	통계를 지울 사용자를 지정합니다. *user_name*은 [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.] 등 어떤 문자도 가능합니다. *domain_NetBIOS_name\user_name*이 공백을 포함할 경우 도메인 이름과 사용자 이름을 따옴표로 묶어야 합니다.
user	사용자에 대한 통계를 지우려면 지정합니다.
user-group	사용자 그룹에 대한 통계를 지우려면 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 지정된 사용자, 지정된 사용자 그룹의 모든 사용자 또는 모든 사용자의 상태를 로그아웃됨으로 설정합니다.

user-group 키워드를 지정할 경우 지정된 사용자 그룹에 속한 모든 사용자의 상태가 로그아웃됨으로 설정됩니다. *domain_nickname* 인수를 **user-group** 키워드와 함께 지정하지 않을 경우 기본 도메인에서 *user_group_name* 그룹의 사용자가 로그아웃됨 상태가 됩니다.

user 키워드를 지정하면 이 사용자의 상태가 로그아웃됨으로 설정됩니다. *domain_nickname* 인수를 **user** 키워드와 함께 지정하지 않을 경우 기본 도메인에서 *user_name* 사용자가 로그아웃됨 상태가 됩니다.

user와 **user-group** 키워드 모두 지정하지 않으면 모든 사용자가 로그아웃됨 상태로 설정됩니다.

예

다음 예에서는 SAMPLE 도메인의 users1 사용자 그룹에 속한 모든 사용자의 상태를 로그아웃됨으로 설정합니다.

```
ciscoasa# clear user-identity active-user-database user-group SAMPLE\users1
```

관련 명령

명령	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.
show user-identity user active	ID 방화벽에 대한 활성 사용자를 표시합니다.

clear user-identity ad-agent statistics

ID 방화벽에 대한 AD 에이전트 통계를 지우려면 특별 권한 EXEC 모드에서 **clear user-identity ad-agent statistics** 명령을 사용합니다.

clear user-identity ad-agent statistics

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

ASA에서는 기본 및 보조 AD 에이전트에 대한 다음 정보를 유지합니다.

- AD 에이전트의 상태
- 도메인의 상태
- AD 에이전트의 통계

AD 에이전트의 통계 데이터를 지우려면 **clear user-identity ad-agent statistics** 명령을 사용합니다.

예

다음 예에서는 ID 방화벽에 대한 AD 에이전트 통계를 지웁니다.

```
ciscoasa# clear user-identity ad-agent statistics
ciscoasa# show user-identity ad-agent statistics

    Primary AD Agent                Total  Last Activity
    -------------------------  ----------  ------------------------
    Input packets:                      0  N/A
    Output packets:                     0  N/A
    Send updates:                       0  N/A
    Recv updates:                       0  N/A
    Keepalive failed:                   0  N/A
    Send update failed:                 0  N/A
    Query failed:                       0  N/A

    Secondary AD Agent              Total  Last Activity
```

```
-------------------------  ----------  ------------------------
Input packets:                      0  N/A
Output packets:                     0  N/A
Send updates:                       0  N/A
Recv updates:                       0  N/A
Keepalive failed:                   0  N/A
Send update failed:                 0  N/A
Query failed:                       0  N/A
```

관련 명령

명령	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.
show user-identity ad-agent [**statistics**]	ID 방화벽의 AD 에이전트에 대한 통계 정보를 표시합니다.

clear user-identity statistics

ID 방화벽에 대한 통계를 표시하는 데 사용되는 카운터를 지우려면 특별 권한 EXEC 모드에서 **clear user-identity statistics** 명령을 사용합니다.

clear user-identity statistics [user [*domain_nickname***\\]***use_rname***] | user-group [***domain_nickname***\\]***user_group_name***]**

구문 설명

*domain_nickname**user_group_name*	통계를 지울 사용자 그룹을 지정합니다. *group_name*은 [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.] 등 어떤 문자도 가능합니다. *domain_NetBIOS_name**group_name*이 공백을 포함할 경우 도메인 이름과 사용자 이름을 따옴표로 묶어야 합니다.
*domain_nickname**use_rname*	통계를 지울 사용자를 지정합니다. *user_name*은 [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.] 등 어떤 문자도 가능합니다. *domain_NetBIOS_name**user_name*이 공백을 포함할 경우 도메인 이름과 사용자 이름을 따옴표로 묶어야 합니다.
user	사용자에 대한 통계를 지우려면 지정합니다.
user-group	사용자 그룹에 대한 통계를 지우려면 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

*domain_nickname*이 *user_group_name*보다 먼저 지정되지 않으면 ASA는 기본 도메인의 *user_group_name* 그룹에 대한 ID 방화벽 통계를 제거합니다.

*domain_nickname*이 *user_name*보다 먼저 지정되지 않으면 ASA는 기본 도메인의 *user_name* 사용자에 대한 ID 방화벽 통계를 제거합니다.

예

다음 예에서는 어떤 사용자 그룹의 통계를 표시하는 데 사용되는 카운터를 지웁니다.

```
ciscoasa# clear user-identity statistics user-group SAMPLE\users1
```

관련 명령

명령	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.
show user-identity statistics	ID 방화벽에 대해 어떤 사용자 또는 사용자 그룹의 통계를 표시합니다.

clear user-identity user-not-found

ID 방화벽을 위한 ASA 로컬 user-not-found 데이터베이스를 지우려면 특별 권한 EXEC 모드에서 **clear user-identity user-not-found** 명령을 사용합니다.

clear user-identity user-not-found

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

ASA는 Microsoft Active Directory에 없는 IP 주소로 구성된 로컬 user-not-found 데이터베이스를 유지합니다. ASA는 데이터베이스의 전체 목록이 아니라 user-not-found 목록의 마지막 1024개 패킷(동일한 소스 IP 주소에서 보낸 연속적인 패킷은 1개의 패킷으로 간주함)만 보존합니다.

ASA에서 로컬 데이터베이스를 지우려면 **clear user-identity user-not-found** 명령을 사용합니다.

팁 Microsoft Active Directory에 없는 사용자의 IP 주소를 표시하려면 **show user-identity user-not-found** 명령을 사용합니다.

예

다음 예에서는 ID 방화벽에 대한 로컬 user-not-found 데이터베이스를 지웁니다.

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
ciscoasa# clear user-identity user-not-found
```

관련 명령

명령	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.
show user-identity user-not-found	ASA user-not-found 데이터베이스에 없는 Active Directory 사용자의 IP 주소를 표시합니다.

clear user-identity user no-policy-activated

ASA의 로컬 레코드에서 ID 방화벽에 대해 활성화되지 않은 사용자를 지우려면 특별 권한 EXEC 모드에서 **clear user-identity user no-policy-activated** 명령을 사용합니다.

clear user-identity user no-policy-activated

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

clear user-identity user no-policy-activated는 어떤 보안 정책에 의해서도 활성화되지 않은 사용자의 로컬 레코드를 지우는 데 사용합니다. 즉 이 사용자는 활성화된 사용자 그룹의 일부가 아니거나 액세스 목록 또는 서비스 정책 컨피그레이션에서 참조되지 않습니다.

clear user-identity user no-policy-activated 명령은 활성 상태이지만 활성화되지 않은 사용자의 IT 주소도 지웁니다.

ID 방화벽에 대해 사용자 그룹을 만들면 이는 활성화되어야 합니다. 즉 그룹이 가져오기 사용자 그룹(액세스 목록 또는 서비스 정책 컨피그레이션에서 사용자 그룹으로 정의됨)이거나 로컬 사용자 그룹(객체 그룹 사용자에 정의됨)이어야 합니다.

예

다음 예에서는 활성화되지 않은 사용자에 대해 ASA에서 로컬 레코드를 지웁니다.

```
ciscoasa# clear user-identity user no-policy-activated
```

관련 명령

명령	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.
show user-identity group	ID 방화벽에 대해 활성화된 사용자 그룹의 목록을 표시합니다.

clear vpn-sessiondb statistics

모든 통계 또는 특정 세션이나 프로토콜을 포함하여 VPN 세션에 대한 정보를 지우려면 특별 권한 EXEC 모드에서 **clear vpn-sessiondb statistics** 명령을 사용합니다.

clear vpn-sessiondb {all | anyconnect | email-proxy | global | index *index_number* **| ipaddress** *IPaddr* **| l2l | name** *username* **| protocol** *protocol* **| ra-ikev1-ipsec | tunnel-group** *name* **| vpn-lb | webvpn}**

구문 설명

all	모든 세션의 통계를 지웁니다.
anyconnect	AnyConnect VPN 클라이언트 세션에 대한 통계를 지웁니다.
email-proxy	이메일 프록시 세션에 대한 통계를 지웁니다.
global	전역 세션 데이터에 대한 통계를 지웁니다.
index *indexnumber*	색인 번호를 기준으로 단일 세션의 통계를 지웁니다. **show vpn-sessiondb detail** 명령의 출력은 세션별로 색인 번호를 표시합니다.
ipaddress *IPaddr*	지정하는 IP 주소의 세션에 대한 통계를 지웁니다.
l2l	VPN LAN-to-LAN 세션에 대한 통계를 지웁니다.
protocol *protocol*	다음 프로토콜에 대한 통계를 지웁니다. • ikev1—IKEv1 프로토콜을 사용하는 세션. • ikev2—IKEv2 프로토콜을 사용하는 세션. • ipsec—IKEv1 또는 IKEv2를 사용하는 IPsec 세션. • ipseclan2lan—IPsec LAN-to-LAN 세션. • ipseclan2lanovernatt—IPsec LAN-to-LAN over NAT-T 세션. • ipsecovernatt—IPsec over NAT-T 세션. • ipsecovertcp—IPsec over TCP 세션. • ipsecoverudp—IPsec over UDP 세션. • l2tpOverIpSec—L2TP over IPsec 세션. • l2tpOverIpsecOverNatT—L2TP over IPsec over NAT-T 세션. • ospfv3—OSPFv3 over IPsec 세션. • webvpn—클라이언트리스 SSL VPN 세션. • imap4s—IMAP4 세션. • pop3s—POP3 세션. • smtps—SMTP 세션. • anyconnectParent—AnyConnect 클라이언트 세션. 세션에 사용되는 프로토콜과 상관없습니다(AnyConnect IPsec IKEv2 및 SSL 세션 종료). • ssltunnel—SSL VPN 세션. SSL을 사용하는 AnyConnect 세션과 클라이언트리스 SSL VPN 세션이 포함됩니다. • dtlstunnel—DTLS가 활성화된 AnyConnect 클라이언트 세션.

ra-ikev1-ipsec	IPsec IKEv1 및 L2TP 세션에 대한 통계를 지웁니다.
tunnel-group *groupname*	지정하는 터널 그룹(연결 프로필)의 세션에 대한 통계를 지웁니다.
vpn-lb	VPN 로드 밸런싱 관리 세션에 대한 통계를 지웁니다.
webvpn	클라이언트리스 SSL VPN 세션에 대한 통계를 지웁니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.

clear wccp

WCCP 정보를 재설정하려면 특별 권한 EXEC 모드에서 **clear wccp** 명령을 사용합니다.

clear wccp [**web-cache** | *service_number*]

구문 설명

web-cache	웹 캐시 서비스를 지정합니다.
service-number	서비스 정의가 캐시에 의해 결정됨을 나타내는 동적 서비스 식별자. 동적 서비스 번호의 범위는 0~255입니다. 최대 허용 개수는 256이며, 여기에는 **web-cache** 키워드로 지정되는 웹 캐시 서비스가 포함됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 웹 캐시 서비스에 대해 WCCP 정보를 재설정하는 방법을 보여줍니다.

```
ciscoasa# clear wccp web-cache
```

관련 명령

명령	설명
show wccp	WCCP 컨피그레이션을 표시합니다.
wccp redirect	WCCP 리디렉션에 대한 지원을 활성화합니다.

clear webvpn sso-server statistics

WebVPN SSO(Single Sign-On) (SSO) 서버의 통계를 재설정하려면 특별 권한 EXEC 모드에서 **clear webvpn sso-server statistics** 명령을 사용합니다.

clear webvpn sso-server statistics *servername*

구문 설명

servername	재설정할 SSO 서버의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 "대기 중 요청" 통계를 재설정하지 않습니다.

예

다음 예에서는 crypto accelerator 통계를 표시합니다.

```
ciscoasa # clear webvpn sso-server statistics
ciscoasa #
```

관련 명령

명령	설명
clear crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 지웁니다.
clear crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 지웁니다.
show crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 표시합니다.
show crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 표시합니다.

clear xlate

현재 동적 변환 및 연결 정보를 지우려면 특별 권한 EXEC 모드에서 **clear xlate** 명령을 사용합니다.

clear xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]]
[**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**state** *state*]

구문 설명

global *ip1*[**-***ip2*]	(선택 사항) 전역 IP 주소 또는 주소 범위를 기준으로 활성 변환을 지웁니다.
gport *port1*[*-port2*]	(선택 사항) 전역 포트 또는 포트 범위를 기준으로 활성 변환을 지웁니다.
interface *if_name*	(선택 사항) 인터페이스를 기준으로 활성 변환을 표시합니다.
local *ip1*[**-***ip2*]	(선택 사항) 로컬 IP 주소 또는 주소 범위를 기준으로 활성 변환을 지웁니다.
lport *port1*[*-port2*]	(선택 사항) 로컬 포트 또는 포트 범위를 기준으로 활성 변환을 지웁니다.
netmask *mask*	(선택 사항) 전역 또는 로컬 IP 주소를 검증할 네트워크 마스크를 지정합니다.
state *state*	(선택 사항) 상태를 기준으로 활성 변환을 지웁니다. 다음 상태 중 하나 이상을 입력할 수 있습니다. • **static—고정** 변환을 지정합니다. • **portmap**—PAT 전역 변환을 지정합니다. • **norandomseq—norondomseq** 설정으로 **nat** 또는 **static** 변환을 지정합니다. • **identity—nat 0** ID 주소 변환을 지정합니다. 둘 이상의 상태를 지정할 경우 공백으로 구분합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

clear xlate 명령은 변환 슬롯의 내용을 지웁니다("xlate"가 translation slot을 의미함). 변환 슬롯은 키 교환이 끝나더라도 유지될 수 있습니다. 컨피그레이션에서 **global** 또는 **nat** 명령을 추가, 변경하거나 제거한 다음에는 반드시 **clear xlate** 명령을 사용합니다.

xlate는 NAT 또는 PAT 세션을 설명합니다. 이 세션은 **show xlate** 명령과 **detail** 옵션으로 볼 수 있습니다. xlate는 고정(static) 유형과 동적(dynamic) 유형이 있습니다.

고정 xlate는 영구적 xlate로서 **static** 명령으로 생성합니다. **clear xlate** 명령은 고정 엔트리의 호스트에 대해서는 지우지 않습니다. 고정 xlate를 제거하려면 컨피그레이션에서 **static** 명령을 제거해야 합니다. **clear xlate** 명령은 고정 변환 규칙을 제거하지 않습니다. 컨피그레이션에서 static 명령을 제거할 경우 이 고정 규칙을 사용하는 기존 연결은 계속 트래픽을 전달할 수 있습니다. 이러한 연결을 비활성화하려면 **clear local-host** 또는 **clear conn** 명령을 사용합니다.

동적 xlate는 트래픽 생성 과정에서 필요에 따라 (**nat** 또는 **global** 명령을 통해) 생성되는 xlate입니다. **clear xlate** 명령은 동적 xlate와 그 연결을 제거합니다. **clear local-host** 또는 **clear conn** 명령을 사용하여 xlate와 관련 연결을 지울 수도 있습니다. 컨피그레이션에서 **nat** 또는 **global** 명령을 제거할 경우 동적 xlate와 관련 연결은 계속 활성 상태일 수 있습니다. 이러한 연결을 제거하려면 **clear xlate** 명령을 사용합니다.

예

다음 예에서는 현재 변환 및 연결 슬롯 정보를 지우는 방법을 보여줍니다.

```
ciscoasa# clear xlate global
```

관련 명령

명령	설명
clear local-host	로컬 호스트 네트워크 정보를 지웁니다.
clear uauth	캐싱된 사용자 인증 및 권한 부여 정보를 지웁니다.
show conn	모든 활성 연결을 표시합니다.
show local-host	로컬 호스트 네트워크 정보를 표시합니다.
show xlate	현재 변환 정보를 표시합니다.

8 장

client-access-rule ~crl enforcenextupdate 명령

client-access-rule

IPsec 방식으로 ASA를 거쳐 연결할 수 있는 원격 액세스 클라이언트 유형 및 버전을 제한하는 규칙을 구성하려면 그룹정책 컨피그레이션 모드에서 **client-access-rule** 명령을 사용합니다. 규칙을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

client-access-rule *priority* {**permit** | **deny**} **type** *type* **version** *version* | **none**

no client-access-rule *priority* [{**permit** | **deny**} **type** *type* **version** *version*]

구문 설명

deny	특정 유형 및/또는 버전의 디바이스에 대해 연결을 거부합니다.
none	어떤 클라이언트 액세스 규칙도 허용하지 않습니다. **client-access-rule**을 null 값으로 설정하여 어떤 제한도 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 값을 상속할 수 없게 합니다.
permit	특정 유형 및/또는 버전의 디바이스에 대해 연결을 허용합니다.
priority	규칙의 우선 순위를 결정합니다. 가장 작은 정수의 규칙이 가장 우선 순위가 높습니다. 따라서 클라이언트 유형 및/똔느 버전과 매칭하는, 가장 작은 정수의 규칙이 적용됩니다. 더 낮은 우선 순위의 규칙과 상충할 경우 ASA는 이를 무시합니다.
type *type*	자유 형식 문자열로 디바이스 유형을 나타냅니다(예: VPN 3002). 문자열은 **show vpn-sessiondb remote** 명령의 출력과 정확하게 일치하는 형태여야 합니다. 단, * 문자를 와일드카드로 사용할 수 있습니다.
version *version*	자유 형식 문자열로 디바이스 버전을 나타냅니다(예: 7.0). 문자열은 **show vpn-sessiondb remote** 명령의 출력과 정확하게 일치하는 형태여야 합니다. 단, * 문자를 와일드카드로 사용할 수 있습니다.

기본값

기본적으로 액세스 규칙이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

모든 규칙을 삭제하려면 **no client-access-rule command**에 *priority* 인수만 사용합니다. 그러면 **client-access-rule none** 명령으로 생성된 null 규칙을 포함하여 구성된 모든 규칙이 삭제됩니다.

클라이언트 액세스 규칙이 없으면 사용자는 기본 그룹 정책에 있는 모든 규칙을 상속합니다. 사용자가 클라이언트 액세스 규칙을 상속할 수 없게 하려면 **client-access-rule none** 명령을 사용합니다. 그러면 모든 클라이언트 유형 및 버전이 연결할 수 있습니다.

다음 지침에 따라 규칙을 만듭니다.

- 어떤 규칙도 정의하지 않을 경우 ASA는 모든 연결 유형을 허용합니다.
- 어떤 클라이언트와 매칭하는 규칙이 없으면 ASA는 연결을 거부합니다. 즉 거부 규칙을 정의할 경우 하나 이상의 허용 규칙도 정의해야 하며, 그렇지 않으면 ASA는 모든 연결을 거부합니다.
- 소프트웨어 및 하드웨어 클라이언트 모두 유형 및 버전이 **show vpn-sessiondb remote** 명령의 출력과 정확히 일치하는 형태여야 합니다.
- * 문자는 와일드카드입니다. 각 규칙에서 여러 번 사용할 수 있습니다. 예를 들어, **client-access-rule 3 deny type * version 3.*** *에 의해* 만들어지는 우선 순위 3 클라이언트 액세스 규칙은 릴리스 버전 3.x 소프트웨어에서 실행 중인 모든 클라이언트 유형을 거부합니다.
- 그룹 정책당 최대 25개의 규칙을 만들 수 있습니다.
- 전체 규칙 세트가 255자를 초과할 수 없습니다.
- 클라이언트 유형 및/또는 버전을 보내지 않는 클라이언트에 대해서는 n/a를 사용할 수 있습니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책을 위해 클라이언트 액세스 규칙을 만드는 방법을 보여줍니다. 이 규칙은 소프트웨어 버전 4.1을 실행하는 VPN 클라이언트를 허용하지만, 모든 VPN 3002 하드웨어 클라이언트를 거부합니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-access-rule 1 d t VPN3002 v *
ciscoasa(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-bypass-proxy

ASA에서 IPv6 트래픽만 예상하고 있을 때 IPv4 트래픽을 다루는 방법 또는 IPv4 트래픽만 예상하고 있을 때 IPv6 트래픽을 다루는 방법을 구성하려면 그룹 정책 컨피그레이션 모드에서 **client-bypass-proxy** 명령을 사용합니다. 클라이언트 바이패스 프로토콜 설정을 지우려면 이 명령의 **no** 형식을 사용합니다.

client-bypass-protocol {enable | disable}

no client-bypass-protocol {enable | disable}

구문 설명

enable	클라이언트 바이패스 프로토콜이 활성화될 경우 ASA에서 IP 주소 유형을 지정하지 않은 IP 트래픽은 클라이언트에서 일반 텍스트로 전송됩니다.
disable	클라이언트 바이패스 프로토콜이 비활성화될 경우 ASA가 IP 주소 유형을 지정하지 않은 IPv6 트래픽은 삭제됩니다.

기본값

클라이언트 바이패스 프로토콜은 DfltGrpPolicy에서 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

클라이언트 바이패스 프로토콜 기능을 사용하면 ASA에서 IPv6 트래픽만 예상하고 있을 때 IPv4 트래픽을 다루는 방법 또는 IPv4 트래픽만 예상하고 있을 때 IPv6 트래픽을 다루는 방법을 구성할 수 있습니다.

AnyConnect 클라이언트가 ASA와의 VPN 연결을 수행할 때 ASA는 IPv4, IPv6 주소를 또는 IPv4 및 IPv6 주소 모두 지정할 수 있습니다. ASA가 AnyConnect 연결에 IPv4 주소만 또는 IPv6 주소만 지정할 경우, ASA에서 IP 주소를 지정하지 않은 네트워크 트래픽을 삭제하거나 이 트래픽이 ASA를 바이패스하여 암호화되지 않은 "일반 텍스트" 형태로 클라이언트에서 전송되는 것을 허용하게끔 클라이언트 바이패스 프로토콜을 구성할 수 있습니다.

예를 들어, ASA에서 AnyConnect 연결에 IPv4 주소만 지정하고 엔드포인트가 이중 스택이라고 가정합니다. 엔드포인트가 IPv6 주소에 연결하려고 할 때 클라이언트 바이패스 프로토콜이 비활성화되었다면 IPv6 트래픽은 삭제됩니다. 그러나 클라이언트 바이패스 프로토콜이 활성화된 경우 IPv6 트래픽은 일반 텍스트로 클라이언트에서 전송됩니다.

예

다음 예에서는 클라이언트 바이패스 프로토콜을 활성화합니다.

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

다음 예에서는 클라이언트 바이패스 프로토콜을 비활성화합니다.

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

다음 예에서는 클라이언트 바이패스 프로토콜 설정을 지웁니다.

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

client(ctl-provider)

인증서 신뢰 목록 제공자에게 연결할 수 있는 클라이언트를 지정하거나 클라이언트 인증을 위한 사용자 이름 및 비밀번호를 지정하려면 ctl 공급자 컨피그레이션 모드에서 **client** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

client [[interface *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

no client [[interface *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

구문 설명

encrypted	비밀번호에 대한 암호화를 지정합니다.
interface *if_name*	연결이 허용되는 인터페이스를 지정합니다.
ipv4_addr	클라이언트의 IP 주소를 지정합니다.
password *password*	클라이언트 인증을 위한 비밀번호를 지정합니다.
username *user_name*	클라이언트 인증을 위한 사용자 이름를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ctl 제공자 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

CTL 제공자와 연결할 수 있는 클라이언트를 지정하고 클라이언트 인증을 위한 사용자 이름 및 비밀번호를 설정하려면 ctl 제공자 컨피그레이션 모드에서 **client** 명령을 사용합니다. 둘 이상의 명령을 실행하여 여러 클라이언트를 정의할 수 있습니다. 사용자 이름 및 비밀번호는 CallManager 클러스터의 CCM 관리자 사용자 이름 및 비밀번호와 일치해야 합니다.

예

다음 예에서는 CTL 제공자 인스턴스를 생성하는 방법을 보여줍니다.

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

관련 명령

명령	설명
ctl	CTL 클라이언트의 CTL 파일을 구문 분석하고 신뢰 지점을 설치합니다.
ctl-provider	ctl-provider 컨피그레이션 모드에서 CTL 제공자 인스턴스를 구성합니다.
export	클라이언트에 내보낼 인증서를 지정합니다.
service	CTL 제공자가 수신할 포트를 지정합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

client(tls-proxy)

신뢰 지점, 키 쌍, 암호 그룹을 구성하려면 프록시 컨피그레이션 모드에서 **client** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

client [cipher-suite *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]]

no client [cipher-suite *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]

구문 설명

cipher-suite *cipher_suite*	암호 그룹을 지정합니다. des-sha1, 3des-sha1, aes128-sha1, aes256-sha1 또는 null-sha1 등을 선택할 수 있습니다.
issuer *ca_tp_name*	클라이언트 동적 인증서를 발급할 로컬 CA 신뢰 지점을 지정합니다.
keypair *key_label*	클라이언트 동적 인증서에서 사용할 RSA 키 쌍을 지정합니다.
ldc	로컬 동적 인증서 발급자 또는 키 쌍을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tls 프록시 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

tls 프록시 컨피그레이션에서 **client** 명령을 사용하면 TLS 프록시의 TLS 클라이언트 역할로서 ASA에 대한 TLS 핸드셰이크 매개변수를 제어할 수 있습니다. 여기에는 암호 그룹을 구성하거나 로컬 동적 인증서 발급자 또는 키 쌍을 설정하는 것이 포함됩니다. 클라이언트 동적 인증서를 발급하는 로컬 CA는 **crypto ca trustpoint** 명령을 통해 정의되며, 신뢰 지점에서 **proxy-ldc-issuer** 명령이 구성되어 있어야 합니다. 그렇지 않으면 기본 로컬 CA 서버(LOCAL-CA-SERVER)가 사용됩니다.

키 쌍의 값은 **crypto key generate** 명령으로 생성되었어야 합니다.

클라이언트 프록시의 경우(프록시가 서버에 대한 TLS 클라이언트의 역할을 함) 사용자 정의 암호 그룹이 기본 암호 그룹 또는 **ssl encryption** 명령에 의해 정의된 것을 대체합니다. 두 TLS 세션 간에 다양한 암호를 구현하기 위해 이 명령을 사용할 수 있습니다. AES 암호는 CallManager 서버와 함께 사용해야 합니다.

예

다음 예에서는 TLS 프록시 인스턴스를 생성하는 방법을 보여줍니다.

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client ldc issuer ldc_server
ciscoasa(config-tlsp)# client ldc keypair phone_common
```

관련 명령

명령	설명
ctl-provider	CTL 제공자 인스턴스를 정의하고 ctl 제공자 컨피그레이션 모드를 시작합니다.
server trust-point	TLS 핸드셰이크 과정에서 제시할 프록시 신뢰 지점 인증서를 지정합니다.
show tls-proxy	TLS 프록시를 표시합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션 수를 설정합니다.

client-firewall

IKE 터널 협상 과정에서 ASA가 VPN 클라이언트에 푸시하는 개인 방화벽 정책을 설정하려면 그룹 정책 컨피그레이션 모드에서 **client-firewall** 명령을 사용합니다. 방화벽 규칙을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

client-firewall none

no client-firewall {opt | req} custom vendor-id *num* **product-id** *num* **policy {AYT | CPP acl-in** *acl* **acl-out** *acl***} [description** *string***]**

client-firewall {opt | req} zonelabs-integrity

참고 방화벽 유형이 **zonelabs-integrity**라면 인수를 포함하지 않습니다. Zone Labs Integrity Server에서 정책을 결정합니다.

client-firewall {opt | req} zonelabs-zonealarm policy {AYT | CPP acl-in *acl* **acl-out** *acl***}**

client-firewall {opt | req} zonelabs-zonealarmorpro policy {AYT | CPP acl-in *acl* **acl-out** *acl***}**

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in *acl* **acl-out** *acl***}**

client-firewall {opt | req} cisco-integrated acl-in *acl* **acl-out** *acl***}**

client-firewall {opt | req} sygate-personal

client-firewall {opt | req} sygate-personal-pro

client-firewall {opt | req} sygate-personal-agent

client-firewall {opt | req} networkice-blackice

client-firewall {opt | req} cisco-security-agent

구문 설명

acl-in *acl*	클라이언트가 인바운드 트래픽에 사용하는 정책을 제공합니다.
acl-out *acl*	클라이언트가 아웃바운드 트래픽에 사용하는 정책을 제공합니다.
AYT	클라이언트 PC 방화벽 애플리케이션이 방화벽 정책을 제어하도록 지정합니다. ASA는 방화벽이 실행 중인지 확인합니다. "Are You There?"라고 묻고 응답이 없으면 ASA는 터널을 해제합니다.
cisco-integrated	Cisco 통합 방화벽 유형을 지정합니다.
cisco-security-agent	Cisco Intrusion Prevention Security Agent 방화벽 유형을 지정합니다.
CPP	Policy Pushed를 VPN 클라이언트 방화벽 정책의 소스로 지정합니다.
custom	Custom 방화벽 유형을 지정합니다.
description *string*	방화벽을 설명합니다.
networkice-blackice	Network ICE Black ICE 방화벽 유형을 지정합니다.
none	클라이언트 방화벽 정책이 없음을 나타냅니다. null 값으로 방화벽 정책을 설정하여 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 방화벽 정책을 상속할 수 없게 합니다.

opt	선택적 방화벽 유형을 지정합니다.
product-id	방화벽 제품을 나타냅니다.
req	필수 방화벽 유형을 지정합니다.
sygate-personal	Sygate Personal 방화벽 유형을 지정합니다.
sygate-personal-pro	Sygate Personal Pro 방화벽 유형을 지정합니다.
sygate-security-agent	Sygate Security Agent 방화벽 유형을 지정합니다.
vendor-id	방화벽 공급업체를 나타냅니다.
zonelabs-integrity	Zone Labs Integrity Server 방화벽 유형을 지정합니다.
zonelabs-zonealarm	Zone Labs Zone Alarm 방화벽 유형을 지정합니다.
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm 또는 Pro 방화벽 유형을 지정합니다.
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro 방화벽 유형을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	**zonelabs-integrity** 방화벽 유형을 추가했습니다.

사용 지침

이 명령의 단일 인스턴스만 구성할 수 있습니다.

모든 방화벽 정책을 삭제하려면 **no client-firewall** 명령을 인수 없이 사용합니다. 이 명령은 **client-firewall none** 명령으로 생성되는 null 정책을 비롯하여 구성된 모든 방화벽 정책을 삭제합니다.

방화벽 정책이 없을 경우 사용자는 기본 또는 다른 그룹 정책에 있는 무엇이든 상속합니다. 사용자가 그러한 방화벽 정책을 상속할 수 없게 하려면 **client-firewall none** 명령을 사용합니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 Cisco Intrusion Prevention Security Agent를 필요로 하는 클라이언트 방화벽 정책을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-firewall req cisco-security-agent
```

client trust-point

CUPS(Cisco Unified Presence Server)에 대한 TLS 프록시를 구성할 때 TLS 핸드셰이크 과정에서 제시할 프록시 신뢰 지점 인증서를 지정하려면 tls 프록시 컨피그레이션 모드에서 **client trust-point** 명령을 사용합니다. 프록시 신뢰 지점 인증서를 제거하려면 이 명령의 **no** 형식을 사용합니다.

client trust-point *proxy_trustpoint*

no client trust-point [*proxy_trustpoint***]**

구문 설명

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

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tls 프록시 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

client trust-point 명령은 ASA에서 TLS 클라이언트의 역할을 할 때 ASA가 TLS 핸드셰이크에 사용하는 신뢰 지점 및 해당 인증서를 지정합니다. 인증서는 ASA(ID 인증서)에서 소유해야 합니다.

자체 서명 인증서, 인증 기관에 등록된 인증서 또는 가져온 자격 증명의 인증서가 가능합니다. **client trust-point** 명령이 전역 **ssl trust-point** 명령에 우선합니다.

예

다음 예에서는 TLS 서버와의 TLS 핸드셰이크에서 신뢰 지점 "ent_y_proxy" 사용을 지정하기 위해 **client trust-point** 명령을 사용하는 것을 보여줍니다. 이 핸드셰이크는 엔티티 Y에서 시작하여 TLS 서버가 상주하는 엔티티 X로 갈 것입니다. ASA는 엔티티 Y를 위해 TLS 프록시의 역할을 합니다.

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

사용 지침

여러 신뢰 지점이 동일한 CA 인증서와 연결되었을 때 그중 하나만 특정 클라이언트 유형에 대해 구성될 수 있습니다. 그러나 이 신뢰 지점 중 하나는 한 클라이언트 유형에, 다른 신뢰 지점은 또 다른 클라이언트 유형에 구성하는 것이 가능합니다.

이미 어떤 클라이언트 유형으로 구성된 CA 인증서에 어떤 신뢰 지점이 연결될 경우 새 신뢰 지점은 동일한 클라이언트 유형 설정으로 구성될 수 없습니다. 이 명령의 **no** 형식은 설정을 지워 어떤 클라이언트 유효성 검사에서도 신뢰 지점을 사용할 수 없게 합니다.

원격 액세스 VPN에서는 구축 요구 사항에 따라 SSL(Secure Sockets Layer) VPN, IPsec(IP Security) 또는 둘 다 사용하여 임의의 네트워크 애플리케이션 또는 리소스에 대한 액세스를 허용할 수 있습니다.

예

다음 예에서는 신뢰 지점 central에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작하고 이를 SSL 신뢰 지점으로 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# client-types ssl
ciscoasa(config-ca-trustpoint)#
```

다음 예에서는 신뢰 지점 checkin1에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작하고 이를 IPsec 신뢰 지점으로 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# client-types ipsec
ciscoasa(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.
id-usage	신뢰 지점의 등록된 ID를 어떻게 사용할 수 있는지 지정합니다.
ssl trust-point	인터페이스에 대한 SSL 인증서를 나타내는 인증서 신뢰 지점을 지정합니다.

client-update

모든 터널 그룹에서 또는 특정 터널 그룹에서 모든 활성 원격 VPN 소프트웨어/하드웨어 클라이언트 및 자동 업데이트 클라이언트로 구성된 ASA에 대해 클라이언트 업데이트를 실행하려면 특별 권한 EXEC 모드에서 **client-update** 명령을 사용합니다.

VPN 소프트웨어/하드웨어 클라이언트 및 자동 업데이트 클라이언트로 구성된 ASA까지 포함하여 전역 레벨에서 클라이언트 업데이트 매개변수를 구성하거나 변경하려면 글로벌 컨피그레이션 모드에서 **client-update** 명령을 사용합니다.

VPN 소프트웨어 및 하드웨어 클라이언트에 대해 클라이언트 업데이트 터널 그룹 IPsec 특성을 구성하고 변경하려면 tunnel-group ipsec-attributes 컨피그레이션 모드에서 **client-update** 명령을 사용합니다.

클라이언트 업데이트를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

글로벌 컨피그레이션 모드 명령:

client-update {enable | component {asdm | image} | device-id *dev_string* **|**
family *family_name* **| type** *type***} url** *url-string* **rev-nums** *rev-nums***}**

no client-update {enable | component {asdm | image} | device-id *dev_string* **|**
family *family_name* **| type** *type***} url** *url-string* **rev-nums** *rev-nums***}**

Tunnel-group ipsec-attributes 컨피그레이션 모드 명령:

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

특별 권한 EXEC 모드 명령:

client-update {all | *tunnel-group***}**

no client-update *tunnel-group*

구문 설명

all	(특별 권한 EXEC 모드에서만 사용 가능) 모든 터널 그룹의 모든 활성 원격 클라이언트에 작업을 적용합니다. **all** 키워드는 이 명령의 **no** 형식과 함께 사용할 수 없습니다.
component {**asdm** | **image**}	자동 업데이트 클라이언트로 구성된 ASA를 위한 소프트웨어 구성 요소.
device-id *dev_string*	자동 업데이트 클라이언트가 고유한 문자열로 스스로를 식별하도록 구성된 경우 클라이언트가 사용하는 것과 동일한 문자열을 지정합니다. 최대 길이는 63자입니다.
enable	(글로벌 컨피그레이션 모드에서만 사용 가능) 원격 클라이언트 소프트웨어 업데이트를 활성화합니다.
family *family_name*	자동 업데이트 클라이언트가 디바이스 제품군으로 스스로를 식별하도록 구성된 경우 클라이언트에서 사용하는 것과 동일한 디바이스 제품군을 지정합니다. 최대 길이가 7자인 asa, pix 또는 text 문자열일 수 있습니다.

rev-nums *rev-nums*	(특별 권한 EXEC 모드에서는 사용할 수 없음) 이 클라이언트의 소프트웨어 또는 펌웨어 이미지를 지정합니다. Windows, WIN9X, WinNT, VPN3002 클라이언트의 경우 최대 4개를 임의의 순서로 입력하고 쉼표로 구분합니다. ASA의 경우 하나만 허용됩니다. 문자열의 최대 길이는 127자입니다.
tunnel-group	(특별 권한 EXEC 모드에서만 사용 가능) 원격 클라이언트 업데이트에 적합한 터널 그룹의 이름을 지정합니다.
type *type*	(특별 권한 EXEC 모드에서는 사용할 수 없음) 클라이언트 업데이트에 대해 알릴 원격 PC의 운영 체제 또는 ASA(자동 업데이트 클라이언트로 구성된 경우)의 유형을 지정합니다. 목록은 다음과 같습니다. • asa5505: Cisco 5505 Adaptive Security Appliance • asa5510: Cisco 5510 Adaptive Security Appliance • asa5520: Cisco 5520 Adaptive Security Appliance • asa5540: Cisco 5540 Adaptive Security Appliance • linux: Linux 클라이언트 • mac: MAC OS X 클라이언트 • pix-515: Cisco PIX 515 Firewall • pix-515e: Cisco PIX 515E Firewall • pix-525: Cisco PIX 525 Firewall • pix-535: Cisco PIX 535 Firewall • Windows: 모든 Windows 기반 플랫폼 • WIN9X: Windows 95, Windows 98, Windows ME 플랫폼 • WinNT: Windows NT 4.0, Windows 2000, Windows XP 플랫폼 • vpn3002: VPN 3002 하드웨어 클라이언트 • 최대 15자의 텍스트 문자열
url *url-string*	(특별 권한 EXEC 모드에서 사용할 수 없음) 소프트웨어/펌웨어 이미지의 URL을 지정합니다. 이 URL은 해당 클라이언트에 적합한 파일을 가리켜야 합니다. 문자열의 최대 길이는 255자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
Tunnel-group ipsec-attributes 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	tunnel-group ipsec-attributes 컨피그레이션 모드를 추가했습니다.
7.2(1)	자동 업데이트 서버로 구성된 ASA를 지원하기 위해 **component**, **device-id**, **family** 키워드와 그 인수를 추가했습니다.

사용 지침

tunnel-group ipsec-attributes 컨피그레이션 모드에서 IPsec remote-access tunnel-group 유형에만 이 특성을 적용할 수 있습니다.

client-update 명령을 사용하여 업데이트를 활성화하고, 업데이트가 적용되는 클라이언트의 유형 및 수정 버전 번호를 지정하며, 업데이트를 가져올 URL 또는 IP 주소를 제공하고, Windows 클라이언트의 경우 선택적으로 사용자에게 VPN 클라이언트 버전을 업데이트하도록 알릴 수 있습니다. 클라이언트에서 수정 버전 번호 목록에 있는 소프트웨어 버전을 이미 실행하고 있을 경우 소프트웨어를 업데이트할 필요 없습니다. 클라이언트에서 목록의 소프트웨어 버전을 실행하고 있지 않을 경우 업데이트해야 합니다.

Windows 클라이언트에서는 사용자가 업데이트를 수행하기 위한 메커니즘을 제공할 수 있습니다. VPN 3002 하드웨어 클라이언트 사용자의 경우 알림 없이 자동으로 업데이트가 수행됩니다. 클라이언트 유형이 또 다른 ASA일 경우 이 ASA는 자동 업데이트 서버의 역할을 합니다.

참고 모든 Windows 클라이언트 및 자동 업데이트 클라이언트에서 프로토콜 "http://" 또는 "https://"를 URL의 접두사로 사용해야 합니다. VPN 3002 하드웨어 클라이언트의 경우 프로토콜 "tftp://"를 대신 지정해야 합니다.

또는 Windows 클라이언트 및 VPN 3002 하드웨어 클라이언트의 경우 특정 유형의 모든 클라이언트가 아니라 개별 터널 그룹에 대해서만 클라이언트 업데이트를 구성할 수 있습니다.

참고 URL의 끝에 애플리케이션 이름을 넣어 브라우저에서 자동으로 애플리케이션을 시작하게 할 수 있습니다(예: https://support/updates/vpnclient.exe).

클라이언트 업데이트를 활성화한 다음 특정 IPsec 원격 액세스 터널 그룹에 대한 클라이언트 업데이트 매개변수의 집합을 정의할 수 있습니다. 이를 위해 tunnel-group ipsec-attributes 모드에서 터널 그룹 이름과 그 유형 그리고 업데이트된 이미지를 가져올 URL 또는 IP 주소를 지정합니다. 또한 수정 버전 번호를 지정해야 합니다. 사용자 클라이언트 수정 버전 번호가 지정된 수정 버전 번호 중 하나와 일치할 경우, 모든 Windows 클라이언트에 대해 클라이언트 업데이트를 실행하는 등의 방법으로 클라이언트를 업데이트할 필요 없습니다.

오래된 Windows 클라이언트를 사용하는 활성 사용자에게 VPN 클라이언트의 업데이트가 필요하다는 알림을 보낼 수도 있습니다. 이러한 사용자에게 표시되는 대화 상자를 통해 브라우저를 시작하고 URL에 지정된 사이트에서 업데이트된 소프트웨어를 다운로드할 수 있습니다. 이 메시지에서 유일하게 구성 가능한 부분이 URL입니다. 활성 상태가 아닌 사용자는 다음에 로그인할 때 알림 메시지를 받습니다. 모든 터널 그룹의 모든 활성 클라이언트에 이 알림을 보내거나 특정 터널 그룹의 클라이언트에 보낼 수 있습니다.

사용자 클라이언트 수정 버전 번호가 지정된 수정 버전 번호 중 하나와 일치할 경우 클라이언트를 업데이트할 필요 없으며 사용자는 어떤 알림 메시지도 받지 않습니다. VPN 3002 클라이언트는 사용자 작업 없이 업데이트되며, 사용자는 어떤 알림 메시지도 받지 않습니다.

참고 클라이언트 업데이트 유형을 **windows**로 지정했는데(모든 Windows 기반 플랫폼 지정) 나중에 동일한 엔티티에 대해 **win9x** 또는 **winnt** 클라이언트 업데이트 유형을 입력하고 싶다면 먼저 이 명령의 **no** 형식을 사용하여 windows 클라이언트 유형을 제거한 다음 새로 **client-update** 명령을 사용하여 새 클라이언트 유형을 지정해야 합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 모든 터널 그룹의 모든 활성 원격 클라이언트에 대해 클라이언트 업데이트를 활성화합니다.

```
ciscoasa(config)# client-update enable
ciscoasa#
```

다음 예에서는 Windows(Win9x, WinNT)에만 적용합니다. 글로벌 컨피그레이션 모드에서 모든 Windows 기반 클라이언트에 대해 클라이언트 업데이트 매개변수를 구성합니다. 여기에는 수정 버전 번호(4.7)와 업데이트를 가져올 URL(https://support/updates)이 포함됩니다.

```
ciscoasa(config)# client-update type windows url https://support/updates/ rev-nums 4.7
ciscoasa(config)#
```

다음 예에서는 VPN 3002 하드웨어 클라이언트에만 적용합니다. tunnel-group ipsec-attributes 컨피그레이션 모드에서 IPsec 원격 액세스 터널 그룹 "salesgrp"에 대해 클라이언트 업데이트 매개변수를 구성합니다. 수정 버전 번호(4.7)를 지정하고 IP 주소가 192.168.1.1인 사이트에서 업데이트된 소프트웨어를 가져오기 위해 TFTP 프로토콜을 사용합니다.

```
ciscoasa(config)# tunnel-group salesgrp type ipsec-ra
ciscoasa(config)# tunnel-group salesgrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
ciscoasa(config-tunnel-ipsec)#
```

다음 예에서는 자동 업데이트 클라이언트로 구성된 Cisco 5520 ASA인 클라이언트에 대해 클라이언트 업데이트를 실행하는 방법을 보여줍니다.

```
ciscoasa(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

특별 권한 EXEC 모드에서 입력한 다음 예에서는 "remotegrp"라는 터널 그룹에 속하고 클라이언트 소프트웨어의 업데이트가 필요한, 연결된 모든 원격 클라이언트에 클라이언트 업데이트 알림을 보냅니다. 다른 그룹의 클라이언트는 업데이트 알림을 받지 않습니다.

```
ciscoasa# client-update remotegrp
ciscoasa#
```

특별 권한 EXEC 모드에서 입력한 다음 예에서는 모든 터널 그룹의 모든 활성 사용자에게 알립니다.

```
ciscoasa# client-update all
ciscoasa#
```

관련 명령

명령	설명
clear configure client-update	클라이언트 업데이트 컨피그레이션 전체를 지웁니다.
show running-config client-update	현재 클라이언트 업데이트 컨피그레이션을 표시합니다.
tunnel-group ipsec-attributes	이 그룹에 대한 tunnel-group ipsec-attributes를 구성합니다.

clock set

ASA의 시계를 수동으로 설정하려면 특별 권한 EXEC 모드에서 **clock set** 명령을 사용합니다.

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

구문 설명

day	일을 1~31의 범위에서 설정합니다. 표준 날짜 형식에 따라 일과 월을 **april 1** 또는 **1 april**과 같이 입력할 수 있습니다.
hh:*mm*:*ss*	시간, 분, 초를 24시간 표시로 설정합니다. 예를 들어, 오후 8시 54분은 **20:54:00**으로 설정합니다.
month	월을 설정합니다. 표준 날짜 형식에 따라 일과 월을 **april 1** 또는 **1 april**과 같이 입력할 수 있습니다.
year	연도를 4자리로 설정합니다(예: **2004**). 연도 범위는 1993~2035입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

어떤 **clock** 컨피그레이션 명령도 입력하지 않은 경우 **clock set** 명령의 기본 표준 시간대는 UTC입니다. **clock set** 명령을 입력한 후 **clock timezone** 명령을 사용하여 표준 시간대를 변경하면 자동으로 새 표준 시간대에 맞게 시간이 조정됩니다. **clock timezone** 명령으로 표준 시간대를 설정한 후에 **clock set** 명령을 입력할 경우 UTC가 아닌 새 표준 시간대에 적합한 시간으로 입력합니다. 또한 **clock set** 명령 다음에 **clock summer-time** 명령을 입력할 경우 일광 절약 시간에 따라 시간이 조정됩니다. **clock set** 명령을 **clock summer-time** 명령 다음에 입력할 경우 일광 절약 시간에 맞는 시간을 입력합니다.

이 명령은 하드웨어 칩의 시간을 설정하며, 컨피그레이션 파일에 시간을 저장하지 않습니다. 이 시간은 재부팅해도 유지됩니다. 다른 **clock** 명령과 달리 이 명령은 특별 권한 EXEC 명령입니다. 시계를 재설정하려면 **clock set** 명령으로 새 시간을 설정해야 합니다.

예

다음 예에서는 표준 시간대를 MST로, 일광 절약 시간을 미국의 기본 기간으로, MDT 현재 시간을 2004년 7월 27일 오후 1:15으로 설정합니다.

```
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa(config)# exit
ciscoasa# clock set 13:15:0 jul 27 2004
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

다음 예에서는 UTC 표준 시간대에서 2004년 7월 27일 8:15로 시계를 설정한 다음 표준 시간대를 MST로, 일광 절약 시간을 미국의 기본 기간으로 설정합니다. 종료 시간(MDT 1:15)은 앞의 예와 동일합니다.

```
ciscoasa# clock set 20:15:0 jul 27 2004
ciscoasa# configure terminal
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

관련 명령

명령	설명
clock summer-time	일광 절약 시간을 표시하기 위해 날짜 범위를 설정합니다.
clock timezone	표준 시간대를 설정합니다.
show clock	현재 시간을 표시합니다.

clock summer-time

ASA 시간 표시에서 일광 절약 시간을 위한 날짜 범위를 설정하려면 글로벌 컨피그레이션 모드에서 **clock summer-time** 명령을 사용합니다. 일광 절약 시간 날짜를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

no clock summer-time [*zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]]

clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

no clock summer-time [*zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]]

구문 설명

date	일광 절약 시간의 시작일과 종료일을 특정 연도의 특정 날짜로 지정합니다. 이 키워드를 사용할 경우 매년 날짜를 재설정해야 합니다.
day	일을 1~31의 범위에서 설정합니다. 표준 날짜 형식에 따라 일과 월을 **April 1** 또는 **1 April**과 같이 입력할 수 있습니다.
hh:mm	시간과 분을 24시간 표시로 설정합니다.
month	월을 문자열로 설정합니다. **date** 명령에서는 표준 날짜 형식에 따라 일과 월을 **April 1** 또는 **1 April**과 같이 입력할 수 있습니다.
offset	(선택 사항) 일광 절약 시간의 시간을 변경하기 위해 분 수를 설정합니다. 기본값은 60분입니다.
recurring	일광 절약 시간의 시작일과 종료일을 어떤 연도의 특정 날짜가 아닌 해당 월의 요일 및 시각 형식으로 지정합니다. 이 키워드를 사용하면 매년 변경할 필요 없는 반복 날짜 범위를 설정할 수 있습니다. 어떤 날짜도 지정하지 않을 경우 ASA는 미국의 기본 날짜 범위를 사용합니다. 즉 3월 두 번째 일요일 2:00 a.m.부터 11월 첫 번째 일요일 2:00 a.m.까지입니다.
week	(선택 사항) 해당 월의 주를 1~4의 정수 혹은 **first** 또는 **last**로 지정합니다. 예를 들어, 해당 일이 불완전한 5번째 주에 속할 경우 **last**로 지정합니다.
weekday	(선택 사항) 요일을 **Monday**, **Tuesday**, **Wednesday** 등으로 지정합니다.
year	연도를 4자리로 설정합니다(예: **2004**). 연도 범위는 1993~2035입니다.
zone	표준 시간대를 문자열로 지정합니다. 예를 들어, **PDT**는 태평양 일광 절약 시간입니다. ASA에서 이 명령으로 설정된 날짜 범위에 따라 일광 절약 시간을 표시할 경우 표준 시간대는 여기서 설정한 값으로 바뀝니다. 기본 표준 시간대를 UTC가 아닌 값으로 설정하려면 **clock timezone** 명령을 참조하십시오.

기본값

기본 차감은 60분입니다.

기본 반복 날짜 범위는 3월 두 번째 일요일 2:00 a.m.부터 11월 첫 번째 일요일 2:00 a.m.까지입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	기본 반복 날짜 범위를 3월 두 번째 일요일 2:00 a.m.부터 11월 첫 번째 일요일 2:00 a.m.까지로 변경했습니다.

사용 지침

남반구의 경우 ASA에서는 시작 월이 종료 월보다 늦은 달이 되는 것을 허용합니다(예: 10월부터 3월까지).

예

다음 예에서는 호주의 일광 절약 시간을 설정합니다.

```
ciscoasa(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

일부 국가에서는 특정 날짜에 일광 절약 시간을 시작합니다. 다음 예에서는 일광 절약 시간이 2008년 4월 1일 3 a.m.에 시작하여 2008년 10월 1일 4 a.m.에 끝나도록 구성됩니다.

```
ciscoasa(config)# clock summer-time UTC date 1 April 2008 3:00 1 October 2008 4:00
```

관련 명령

명령	설명
clock set	ASA의 시계를 수동으로 설정합니다.
clock timezone	표준 시간대를 설정합니다.
ntp server	NTP 서버를 나타냅니다.
show clock	현재 시간을 표시합니다.

clock timezone

ASA 시계의 표준 시간대를 설정하려면 글로벌 컨피그레이션 모드에서 **clock timezone** 명령을 사용합니다. 표준 시간대를 다시 기본값인 UTC로 설정하려면 이 명령의 **no** 형식을 사용합니다.

clock timezone *zone* **[-]***hours* **[***minutes***]**

no clock timezone [*zone* **[-]***hours* **[***minutes***]]**

구문 설명

[-]*hours*	UTC에서 차감할 시간 수를 설정합니다. 예를 들어, PST는 -8시간입니다.
minutes	(선택 사항) UTC에서 차감할 분 수를 설정합니다.
zone	표준 시간대를 문자열로 지정합니다. 예를 들어, PST는 태평양 표준시입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

일광 절약 시간을 설정하려면 **clock summer-time** 명령을 참조하십시오.

clock set 명령 또는 NTP 서버에서 가져온 시간이 UTC 시간을 설정합니다. 이 명령을 사용하여 UTC에 대한 차감으로 표준 시간대를 설정해야 합니다.

예

다음 예에서는 표준 시간대를 태평양 표준시로 설정합니다. 이는 UTC에서 8시간을 차감합니다.

```
ciscoasa(config)# clock timezone PST -8
```

관련 명령

명령	설명
clock set	ASA의 시계를 수동으로 설정합니다.
clock summer-time	일광 절약 시간을 표시하기 위해 날짜 범위를 설정합니다.
ntp server	NTP 서버를 나타냅니다.
show clock	현재 시간을 표시합니다.

cluster-ctl-file

플래시 메모리에 저장된 기존 CTL 파일로부터 이미 생성한 신뢰 지점을 사용하려면 ctl 파일 컨피그레이션 모드에서 **cluster-ctl-file** 명령을 사용합니다. 새 CTL 파일을 만들기 위해 CTL 파일 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

cluster-ctl-file *filename_path*

no cluster-ctl-file *filename_path*

구문 설명

filename_path	디스크 또는 플래시 메모리에 저장된 CTL 파일의 경로 및 파일 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ctl 파일 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

이 명령을 구성하면 전화 프록시는 플래시 메모리에 저장된 CTL 파일을 구문 분석하고 이 CTL 파일로부터 신뢰 지점을 설치한 다음 플래시의 파일을 사용하여 새 CTL 파일을 생성합니다.

예

다음 예에서는 플래시 메모리에 저장된 CTL 파일로부터 신뢰 지점을 설치하기 위해 이 파일을 구문 분석합니다.

```
ciscoasa(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

관련 명령

명령	설명
ctl-file (global)	전화 프록시 구성을 위해 생성할 CTL 파일 또는 플래시 메모리에 있는, 구문 분석할 CTL 파일을 지정합니다.
ctl-file (phone-proxy)	전화 프록시 컨피그레이션에 사용할 CTL 파일을 지정합니다.
phone-proxy	전화 프록시 인스턴스를 구성합니다.

cluster encryption

가상 로드 밸런싱 클러스터에서 교환되는 메시지의 암호화를 활성화하려면 vpn 로드 밸런싱 컨피그레이션 모드에서 **cluster encryption** 명령을 사용합니다. 암호화를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cluster encryption

no cluster encryption

참고 VPN 로드 밸런싱에는 활성 3DES/AES 라이센스가 필요합니다. ASA는 로드 밸런싱을 활성화하기 전에 이 암호화 라이센스가 있는지 확인합니다. 활성 상태의 3DES 또는 AES 라이센스를 찾지 못하면 ASA는 로드 밸런싱을 활성화하지 못하게 하며, 라이센스에서 허용하지 않는 한 로드 밸런싱 시스템에 의한 3DES 내부 컨피그레이션을 차단합니다.

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

암호화는 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Vpn 로드 밸런싱 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 가상 로드 밸런싱 클러스터에서 교환되는 메시지에 대해 암호화를 활성화하거나 비활성화합니다.

cluster encryption 명령을 구성하려면 먼저 **vpn load-balancing** 명령을 사용하여 vpn 로드 밸런싱 컨피그레이션 모드를 시작한 상태여야 합니다. 또한 클러스터 암호화를 활성화하기 전에 **cluster key** 명령을 사용하여 클러스터 공유 비밀 키를 구성해야 합니다.

참고 암호화를 사용할 때 먼저 **isakmp enable** *inside* 명령을 구성해야 하는데, 여기서 *inside*는 로드 밸런싱 내부 인터페이스를 가리킵니다. ISAKMP가 로드 밸런싱 내부 인터페이스에서 활성화되지 않을 경우 클러스터 암호화를 구성하려 할 때 오류 메시지가 나타납니다.

예

다음은 VPN 로드 밸런싱 명령 시퀀스의 예로서 가상 로드 밸런싱 클러스터에 대한 암호화를 활성화하는 **cluster encryption** 명령을 포함합니다.

```
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)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
cluster key	클러스터에 대한 공유 비밀 키를 지정합니다.
vpn load-balancing	vpn 로드 밸런싱 컨피그레이션 모드를 시작합니다.

cluster exec

클러스터의 모든 유닛에서 또는 특정 멤버에서 명령을 실행하려면 특별 권한 EXEC 모드에서 **cluster exec** 명령을 사용합니다.

cluster exec [unit *unit_name***]** *command*

구문 설명

unit *unit_name*	(선택 사항) 특정 유닛에서 명령을 수행합니다. 멤버 이름을 보려면 **cluster exec unit ?** 을 입력하거나(현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info** 명령을 입력합니다.
command	실행하려는 명령을 지정합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

모든 멤버에 **show** 명령을 보내면 모든 출력이 수집되고 해당 내용이 현재 유닛의 콘솔에 표시됩니다. **capture** 및 **copy** 같은 다른 명령의 경우 클러스터 전체 실행을 활용할 수도 있습니다.

예

클러스터에 있는 모든 유닛의 동일한 캡처 파일을 TFTP 서버에 동시에 복사하려면 다음 명령을 마스터 유닛에 입력합니다.

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 대상 캡처 파일의 이름 뒤에는 유닛 이름이 자동으로 연결되며 capture1_asa1.pcap, capture1_asa2.pcap 같은 형식이 됩니다. 이 예에서 asa1 및 asa2는 클러스터 유닛 이름 입니다.

cluster exec show port-channel 요약 명령에 대한 다음 샘플 출력에는 클러스터의 각 멤버에 대한 EtherChannel 정보가 나와 있습니다.

```
ciscoasa# cluster exec show port-channel summary
primary(LOCAL):*********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
```

```
------+-------------+-----------+-------------------------------------------------
1         Po1             LACP      Yes  Gi0/0(P)
2         Po2             LACP      Yes  Gi0/1(P)
 secondary:************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-------------------------------------------------
1         Po1             LACP      Yes   Gi0/0(P)
2         Po2             LACP      Yes   Gi0/1(P)
```

관련 명령

명령	설명
cluster group	클러스터 그룹 컨피그레이션 모드를 시작합니다.
show cluster info	클러스터 정보를 표시합니다.

cluster group

클러스터 부트스트랩 매개변수 및 기타 클러스터 설정을 구성하려면 글로벌 컨피그레이션 모드에서 **cluster group** 명령을 사용합니다. 클러스터 컨피그레이션을 지우려면 이 명령의 **no** 형식을 사용합니다.

cluster group *name*

no cluster group *name*

구문 설명

name	클러스터 이름을 1자 ~ 38자의 ASCII 문자열로 지정합니다. 유닛당 클러스터 그룹은 하나만 구성할 수 있습니다. 클러스터의 모든 멤버는 동일한 이름을 사용해야 합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

클러스터의 각 유닛은 클러스터에 참가하려면 부트스트랩 컨피그레이션이 필요합니다. 일반적으로 클러스터에 참가하기 위해 구성하는 첫 번째 유닛이 마스터 유닛이 됩니다. 클러스터링이 활성화되고 선택 기간이 지나면 클러스터에서 마스터 유닛을 선택합니다. 맨 처음 클러스터에 유닛이 하나밖에 없을 경우, 해당 유닛이 마스터 유닛이 됩니다. 클러스터에 추가되는 후속 유닛은 슬레이브 유닛이 됩니다.

클러스터링을 구성하기 전에 **cluster interface-mode** 명령을 사용하여 클러스터 인터페이스 모드를 설정해야 합니다.

클러스터링을 활성화하거나 비활성화하려면 콘솔 포트 또는 ASDM을 사용해야 합니다. 텔넷이나 SSH는 사용할 수 없습니다.

예

다음 예에서는 관리 인터페이스를 구성하고, 클러스터 제어 링크에 대한 디바이스-로컬 EtherChannel을 구성하며, 상태 검사를 (일시적으로) 비활성화한 다음 "unit1"라는 이름의 ASA에 대해 클러스터링을 활성화합니다. 이 유닛은 클러스터에 가장 처음 추가되었으므로 마스터 유닛이 됩니다.

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    no health-check
    enable noconfirm
```

다음 예에는 슬레이브 유닛인 unit2에 대한 컨피그레이션이 포함됩니다.

```
interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    no health-check
    enable as-slave
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용하면 ASA에서는 cLACP를 통해 네이버 스위치와 EtherChannel을 협상합니다.
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	클러스터 상태 검사 기능을 활성화합니다. 여기에는 유닛 상태 모니터링 및 인터페이스 상태 모니터링이 포함됩니다.
key	클러스터 제어 링크의 제어 트래픽에 대해 인증 키를 설정합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스를 위한 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택에서 이 유닛의 우선 순위를 설정합니다.

cluster ip address

가상 로드 밸런싱 클러스터의 IP 주소를 설정하려면 vpn 로드 밸런싱 컨피그레이션 모드에서 **cluster ip address** 명령을 사용합니다. IP 주소 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

구문 설명

ip-address	가상 로드 밸런싱 클러스터에 지정할 IP 주소.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Vpn 로드 밸런싱 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

먼저 **vpn load-balancing** 명령을 사용하여 vpn 로드 밸런싱 컨피그레이션 모드를 시작하고 가상 클러스터 IP 주소가 참조하는 인터페이스를 구성해야 합니다.

클러스터 IP 주소는 가상 클러스터를 구성하고 있는 인터페이스와 동일한 서브넷에 있어야 합니다.

이 명령의 **no** 형식에서는 선택 사항인 *ip-address* 값을 지정할 경우 기존 클러스터 IP 주소와 일치해야 **no cluster ip address** 명령을 완료할 수 있습니다.

예

다음 예에서 보여주는 VPN 로드 밸런싱 명령 시퀀스는 가상 로드 밸런싱 클러스터의 IP 주소를 209.165.202.224로 설정하는 **cluster ip address** 명령을 포함합니다.

```
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
interface	디바이스의 인터페이스를 설정합니다.
nameif	인터페이스에 이름을 지정합니다.
vpn load-balancing	vpn 로드 밸런싱 컨피그레이션 모드를 시작합니다.

cluster key

가상 로드 밸런싱 클러스터에서 IPsec 사이트 대 사이트 터널 교환을 위한 공유 암호를 설정하려면 vpn 로드 밸런싱 컨피그레이션 모드에서 **cluster key** 명령을 사용합니다. 이 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

cluster key *shared-secret*

no cluster key [*shared-secret*]

구문 설명

shared-secret	VPN 로드 밸런싱 클러스터를 위한 공유 암호를 정의하는 3자~17자의 문자열. 이 문자열에는 공백을 제외한 특수 문자를 사용할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Vpn 로드 밸런싱 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

먼저 **vpn load-balancing** 명령을 사용하여 vpn 로드 밸런싱 컨피그레이션 모드를 시작해야 합니다. **cluster key** 명령에 정의된 공유 암호도 클러스터 암호화에 사용됩니다.

또한 클러스터 암호화를 활성화하기 전에 **cluster key** 명령을 사용하여 공유 암호를 구성해야 합니다.

이 명령의 **no cluster key** 형식에서 *shared-secret*의 값을 지정할 경우 공유 암호 값이 기존 컨피그레이션과 일치해야 합니다.

예

다음 예에서 보여주는 VPN 로드 밸런싱 명령 시퀀스는 가상 로드 밸런싱 클러스터의 공유 암호를 123456789로 설정하는 **cluster key** 명령을 포함합니다.

```
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)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
vpn load-balancing	vpn 로드 밸런싱 컨피그레이션 모드를 시작합니다.

cluster master unit

새 유닛을 ASA 클러스터의 마스터 유닛으로 설정하려면 특별 권한 EXEC 모드에서 **cluster master unit** 명령을 사용합니다.

cluster master unit *unit_name*

주의 마스터 유닛을 변경하는 가장 좋은 방법은 마스터 유닛의 클러스터링을 비활성화한 후(**no cluster enable** 명령 참조) 새 마스터가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 마스터가 될 정확한 유닛을 지정해야 할 경우 **cluster master unit** 명령을 사용합니다. 그러나 중앙 집중식 기능의 경우 이 명령을 통해 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

구문 설명

unit_name	새 마스터 유닛이 될 로컬 유닛 이름을 지정합니다. 멤버 이름을 보려면 **cluster master unit ?** 을 입력하거나(현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info** 명령을 입력합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

기본 클러스터 IP 주소에 다시 연결해야 합니다.

예

다음 예에서는 asa2를 마스터 유닛으로 설정합니다.

```
ciscoasa# cluster master unit asa2
```

관련 명령

명령	설명
cluster exec	모든 클러스터 멤버에 명령을 보냅니다.
cluster group	클러스터를 구성합니다.
cluster remove unit	클러스터에서 유닛을 제거합니다.

cluster remove unit

ASA 클러스터에서 유닛을 제거하려면 특별 권한 EXEC 모드에서 cluster remove unit 명령을 사용합니다.

cluster remove unit *unit_name*

구문 설명

unit_name	클러스터에서 제거할 로컬 유닛 이름을 지정합니다. 멤버 이름을 보려면 **cluster remove unit ?**을 입력하거나 **show cluster info** 명령을 입력합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

부트스트랩 컨피그레이션과 마스터 유닛에서 동기화한 마지막 컨피그레이션도 그대로 유지되므로 나중에 컨피그레이션을 잃지 않고 다시 유닛을 추가할 수 있습니다. 슬레이브 유닛에 이 명령을 입력하여 마스터 유닛을 제거할 경우 새 마스터 유닛이 선택됩니다.

예

다음 예에서는 유닛 이름을 확인한 다음 클러스터에서 asa2를 제거합니다.

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

관련 명령

명령	설명
cluster exec	모든 클러스터 멤버에 명령을 보냅니다.
cluster group	클러스터를 구성합니다.
cluster master unit	새 유닛을 ASA 클러스터의 마스터 유닛으로 설정합니다.

cluster-interface

클러스터 제어 링크 물리적 인터페이스 및 IP 주소를 지정하려면 클러스터 그룹 컨피그레이션 모드에서 **cluster-interface** 명령을 사용합니다. 클러스터 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

cluster-interface *interface_id* **ip** *ip_address mask*

no cluster-interface [*interface_id* **ip** *ip_address mask***]**

구문 설명

interface_id	물리적 인터페이스, EtherChannel 또는 이중 인터페이스를 지정합니다. 하위 인터페이스 및 관리 인터페이스는 허용되지 않습니다. 이 인터페이스에는 **nameif**가 구성될 수 없습니다. IPS 모듈이 포함된 ASA 5585-X의 경우, 클러스터 제어 링크에 IPS 모듈 인터페이스를 사용할 수 없습니다.
ip *ip_address mask*	IP 주소의 IPv4 주소를 지정합니다. 이 인터페이스에는 IPv6가 지원되지 않습니다. 각 유닛의 IP 주소는 동일한 네트워크상에 있되 서로 다르게 지정하십시오.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

클러스터에 참가하기 전에 클러스터 제어 링크 인터페이스를 활성화해야 합니다.

인터페이스가 충분한 경우 여러 개의 클러스터 제어 링크 인터페이스를 하나의 EtherChannel로 통합하는 편이 좋습니다. EtherChannel은 ASA에 대해 로컬이며 Spanned EtherChannel이 아닙니다. 클러스터 제어 링크에는 10기가비트 이더넷 인터페이스를 사용하는 것이 좋습니다. EtherChannel 멤버 인터페이스에 On 모드를 사용하여 클러스터 제어 링크의 불필요한 트래픽을 줄이는 것이 좋습니다. 클러스터 제어 링크는 분리된 안정적인 네트워크이므로 LACP 트래픽의 오버헤드가 필요 없습니다.

클러스터 제어 링크 인터페이스 컨피그레이션은 마스터 유닛에서 슬레이브 유닛으로 복제되지 않지만, 각 유닛에는 동일한 컨피그레이션을 사용해야 합니다. 이 컨피그레이션은 복제되지 않으므로, 각 유닛에 클러스터 제어 링크 인터페이스를 별도로 구성해야 합니다.

클러스터 제어 링크에 대한 자세한 내용은 컨피그레이션 가이드를 참조하십시오.

예

다음 예에서는 TenGigabitEthernet 0/6 및 TenGigabitEthernet 0/7에 대해 EtherChannel, Port-channel 2를 생성한 다음 이 포트 채널을 클러스터 제어 링크로 지정합니다. 채널 그룹에 인터페이스를 지정할 때 포트 채널 인터페이스가 자동으로 생성됩니다.

```
interface tengigabitethernet 0/6
    channel-group 2 mode on
    no shutdown

interface tengigabitethernet 0/7
    channel-group 2 mode on
    no shutdown

cluster group cluster1
    cluster-interface port-channel2 ip 10.1.1.1 255.255.255.0
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용하면 ASA에서는 cLACP를 통해 네이버 스위치와 EtherChannel을 협상합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드를 시작합니다.
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	클러스터 상태 검사 기능을 활성화합니다. 여기에는 유닛 상태 모니터링 및 인터페이스 상태 모니터링이 포함됩니다.
key	클러스터 제어 링크의 제어 트래픽에 대해 인증 키를 설정합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스를 위한 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택에서 이 유닛의 우선 순위를 설정합니다.

cluster-mode

클러스터의 보안 모드를 지정하려면 전화 프록시 컨피그레이션 모드에서 **cluster-mode** 명령을 사용합니다. 클러스터의 보안 모드를 기본 모드로 설정하려면 이 명령의 **no** 형식을 사용합니다.

cluster-mode [mixed | nonsecure]

no cluster-mode [mixed | nonsecure]

구문 설명

mixed	전화 프록시 기능을 구성할 때 클러스터 모드가 혼합 모드가 되도록 지정합니다.
nonsecure	전화 프록시 기능을 구성할 때 클러스터 모드가 비보안 모드가 되도록 지정합니다.

기본값

기본 클러스터 모드는 비보안입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
전화 프록시 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

전화 프록시가 혼합 모드 클러스터(보안 모드와 비보안 모드가 모두 있음)에서 실행되도록 구성할 경우, 일부 전화가 인증 모드 또는 암호화 모드로 구성된다면 LDC 발급자도 구성해야 합니다.

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

예

다음 예에서는 전화 프록시의 보안 모드를 혼합으로 설정합니다. 즉 IP 전화기가 보안 및 비보안 모드에서 작동합니다.

```
ciscoasa(config-phone-proxy)# cluster-mode mixed
```

관련 명령

명령	설명
phone-proxy	전화 프록시 인스턴스를 구성합니다.
tls-proxy	TLS 프록시 인스턴스를 구성합니다.

cluster port

가상 로드 밸런싱 클러스터의 UDP 포트를 설정하려면 vpn 로드 밸런싱 컨피그레이션 모드에서 **cluster port** 명령을 사용합니다. 포트 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

cluster port *port*

no cluster port [*port*]

구문 설명

port	가상 로드 밸런싱 클러스터에 지정할 UDP 포트

기본값

기본 클러스터 포트는 9023입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Vpn 로드 밸런싱 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

먼저 **vpn load-balancing** 명령을 사용하여 vpn 로드 밸런싱 컨피그레이션 모드를 시작해야 합니다.

어떤 유효한 UDP 포트 번호도 지정할 수 있습니다. 범위는 1~65535입니다.

이 명령의 **no cluster port** 형식에서 *port*의 값을 지정할 경우 지정된 포트 번호가 구성된 기존 포트 번호와 일치해야 합니다.

예

다음 예에서는 가상 로드 밸런싱 클러스터의 UDP 포트를 9023으로 설정합니다.

```
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)# cluster port 9023
ciscoasa(config-load-balancing)# participate
```

관련 명령

명령	설명
vpn load-balancing	vpn 로드 밸런싱 컨피그레이션 모드를 시작합니다.

command-alias

명령에 대한 별칭을 생성하려면 글로벌 컨피그레이션 모드에서 **command-alias** 명령을 사용합니다. 별칭을 제거하려면 이 명령의 **no** 형식을 사용합니다.

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

구문 설명

command_alias	기존 명령의 새 이름을 지정합니다.
mode	명령 별칭을 생성할 명령 모드를 지정합니다. 이를테면 **exec**(사용자 및 특별 권한 EXEC 모드), **configure** 또는 **interface**로 지정합니다.
original_command	명령 별칭을 생성하려는 기존 명령 또는 키워드를 포함한 명령을 지정합니다.

기본값

기본적으로 다음 사용자 EXEC 모드 별칭이 구성되어 있습니다.

- **h**는 **help**
- **lo**는 **logout**
- **p**는 **ping**
- **s**는 **show**

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

명령 별칭을 입력하면 원래의 명령이 호출됩니다. 이를테면 긴 명령에 대한 바로가기를 제공하기 위해 명령 별칭을 만들 수 있습니다.

어떤 명령의 첫 부분에 대해 별칭을 만들고 추가 키워드와 인수는 평소처럼 입력할 수 있습니다.

CLI 도움말을 사용할 때 명령 별칭은 별표(*)로 나타내며 다음 형식으로 표시합니다.

```
*command-alias=original-command
```

예를 들어, **lo** 명령 별칭은 다음과 같이 "lo"로 시작하는 다른 특별 권한 EXEC 모드 명령과 나란히 표시됩니다.

```
ciscoasa# lo?
*lo=logout login  logout
```

동일한 별칭을 각기 다른 모드에서 사용할 수 있습니다. 예를 들어, 다음과 같이 특별 권한 모드와 컨피그레이션 모드에서 "happy"를 사용하여 서로 다른 명령의 별칭을 만들 수 있습니다.

```
ciscoasa(config)# happy?

configure mode commands/options:
*happy="username employee1 password test"

exec mode commands/options:
*happy=enable
```

명령만 나열하고 별칭을 생략하려면 입력 라인을 공백으로 시작합니다. 또한 명령 별칭을 피하려면 명령을 입력하기 전에 공백을 넣습니다. 다음 예에서는 "happy"라는 이름의 별칭이 표시되지 않습니다. **happy?** 앞에 공백이 있기 때문입니다. 명령을 입력합니다.

```
ciscoasa(config)# alias exec test enable
ciscoasa(config)# exit
ciscoasa#   happy?
ERROR: % Unrecognized command
```

명령과 마찬가지로 명령 별칭에 이어 인수와 키워드를 표시하기 위해 CLI 도움말을 사용할 수 있습니다.

명령 별칭을 완전하게 입력해야 합니다. 축약된 별칭은 허용되지 않습니다. 다음 예에서는 파서가 **hap** 명령을 "happy"라는 별칭을 나타내는 것으로 인식하지 않습니다.

```
ciscoasa# hap
% Ambiguous command: "hap"
```

예

다음 예에서는 "save"라는 이름의 명령 별칭을 **copy running-config startup-config** 명령에 대해 만드는 방법을 보여줍니다.

```
ciscoasa(config)# command-alias exec save copy running-config startup-config
ciscoasa(config)# exit
ciscoasa# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
ciscoasa#
```

관련 명령

명령	설명
clear configure command-alias	기본적으로 제공되지 않는 모든 명령 별칭을 지웁니다.
show running-config command-alias	기본적으로 제공되지 않지만 구성된 모든 명령 별칭을 표시합니다.

command-queue

응답을 기다리는 동안 대기열에서 포함할 수 있는 MGCP 명령의 최대 개수를 지정하려면 mgcp 맵 컨피그레이션 모드에서 **command-queue** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

command-queue *limit*

no command-queue *limit*

구문 설명

limit	대기열에 넣을 명령의 최대 개수를 1~2147483647의 범위에서 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

MGCP 명령 대기열의 기본값은 200입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Mgcp 맵 컨피그레이션	•	•	•	•	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

대기열에서 응답을 기다릴 수 있는 MGCP 명령의 최대 개수를 지정하려면 **command-queue** 명령을 사용합니다. 허용되는 값의 범위는 1~4294967295입니다. 기본값은 200입니다. 한도에 도달한 상태에서 새 명령이 도착하면 대기열에 가장 오래 있었던 명령이 제거됩니다.

예

다음 예에서는 MGCP 명령 대기열을 명령 150개로 제한합니다.

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)#command-queue 150
```

관련 명령

명령	설명
debug mgcp	MGCP를 위한 디버깅 정보의 표시를 활성화합니다.
mgcp-map	MGCP 맵을 정의하고 MGCP 맵 컨피그레이션 모드를 활성화합니다.
show mgcp	MGCP 컨피그레이션 및 세션 정보를 표시합니다.
timeout	유휴 타이머를 구성합니다. 이 시간이 경과하면 MGCP 미디어 또는 MGCP PAT xlate 연결이 닫힙니다.

community-list

BGP(Border Gateway Protocol) 커뮤니티 목록을 만들거나 구성하고 그에 대한 액세스를 제어하려면 글로벌 컨피그레이션 모드에서 **community-list** 명령을 사용합니다. 커뮤니티 목록을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

표준 커뮤니티 목록

community-list {*standard* | **standard** *list-name*} {**deny** | **permit**} [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**]

no community-list {*standard* | **standard** *list-name*}

확장 커뮤니티 목록

community-list {*expanded* | **expanded** *list-name*} {**deny** | **permit**} *regexp*

no community-list {*expanded* | **expanded** *list-name*}

구문 설명

standard	1~99의 숫자를 사용하여 표준 커뮤니티 목록을 만들어 하나 이상의 허용 또는 거부 커뮤니티 그룹을 식별합니다.
standard *list-name*	명명된 표준 커뮤니티 목록을 구성합니다.
permit	매칭하는 조건에 대한 액세스를 허용합니다.
deny	매칭하는 조건에 대한 액세스를 거부합니다.
community-number	(선택 사항) 커뮤니티를 1~4294967200의 32비트 번호로 지정합니다. 단일 커뮤니티를 입력하거나 공백으로 구분된 여러 커뮤니티를 입력할 수 있습니다.
AA:NN	(선택 사항) 4바이트의 새로운 커뮤니티 형식으로 입력되는 자율 시스템 번호 및 네트워크 번호. 이 값은 콜론으로 구분된 2개의 2바이트 숫자로 구성됩니다. 각 2바이트 숫자에 대해 1~65535의 숫자를 입력할 수 있습니다. 단일 커뮤니티를 입력하거나 공백으로 구분된 여러 커뮤니티를 입력할 수 있습니다.
internet	(선택 사항) 인터넷 커뮤니티를 지정합니다. 이 커뮤니티 경로는 모든 피어(내부 및 외부)에게 알려집니다.
no-export	(선택 사항) no-export 커뮤니티를 지정합니다. 이 커뮤니티 경로는 같은 자율 시스템 안에 있는 피어 또는 연합 내에 다른 하위 자율 시스템으로만 알려집니다. 이 경로는 외부 피어에 알려지지 않습니다.
local-AS	(선택 사항) local-as 커뮤니티를 지정합니다. 커뮤니티의 경로는 로컬 자율 시스템에 속한 피어 또는 어떤 연합의 한 하위 자율 시스템에 속한 피어에게만 알려집니다. 이 경로는 외부 피어 또는 연합 내 다른 자율 시스템에는 알려지지 않습니다.
no-advertise	(선택 사항) no-advertise 커뮤니티를 지정합니다. 이 커뮤니티 경로는 모든 피어(내부 또는 외부)에게 알려지지 않습니다.
Expanded	100~500의 숫자로 확장 커뮤니티 목록 번호를 구성하여 하나 이상의 허용 또는 거부 커뮤니티 그룹을 식별합니다.
expanded *list-name*	명명된 확장 커뮤니티 목록을 구성합니다.
regexp	입력 문자열과의 매칭을 위해 패턴을 지정하는 데 사용되는 정규식을 구성합니다. **참고** 정규 표현식은 확장 커뮤니티 목록에서만 사용할 수 있습니다 .

기본값

BGP 커뮤니티 교환은 기본적으로 활성화되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

community-list 명령은 BGP 커뮤니티 필터링을 구성하는 데 사용합니다. BGP 커뮤니티 값은 32비트 숫자(기존 형식) 또는 4바이트 숫자(새 형식)로 구성됩니다. 새 커뮤니티 형식은 글로벌 컨피그레이션 모드에서 **bgp-community new-format** 명령을 입력하여 활성화합니다. 새 커뮤니티 형식은 4바이트 값으로 구성됩니다.

처음 2바이트는 자율 시스템 번호를, 나머지 2바이트는 사용자 정의 네트워크 번호를 나타냅니다. 명명된 커뮤니티 목록과 번호가 지정된 커뮤니티 목록도 지원됩니다. BGP 피어 간의 BGP 커뮤니티 특성 교환은 지정된 네이버에 대해 **neighbor send-community** 명령이 구성될 때 활성화됩니다. BGP 커뮤니티 특성은 RFC 1997 및 RFC 1998에서 정의됩니다.

BGP 커뮤니티 교환은 기본적으로 활성화되지 않습니다. 네이버별로 **neighbor send-community** 명령을 사용하여 활성화합니다. 이 명령 또는 **set community** 명령으로 다른 커뮤니티 값이 구성되지 않는 한 인터넷 커뮤니티는 기본적으로 모든 경로 또는 접두사에 적용됩니다.

지정된 커뮤니티 세트와 매칭하는 허용 값이 구성되었으면 커뮤니티 목록은 기본적으로 다른 모든 커뮤니티 값에 대해 암시적 거부가 됩니다.

표준 커뮤니티 목록

표준 커뮤니티 목록은 잘 알려진 커뮤니티 및 특정 커뮤니티 번호를 구성하는 데 사용합니다. 표준 커뮤니티 목록에 최대 16개의 커뮤니티를 구성할 수 있습니다. 16개를 초과하여 구성하려고 하면 한도를 초과하는 커뮤니티는 처리되지 않으며 실행 중인 컨피그레이션 파일에 저장되지 않습니다.

확장 커뮤니티 목록

확장 커뮤니티 목록은 정규식을 사용하여 커뮤니티를 필터링하는 데 사용합니다. 정규식을 사용하여 커뮤니티 특성과 매칭할 패턴을 구성합니다. * 또는 + 문자를 사용하여 매칭할 경우 가장 긴 구성소를 가장 먼저 매칭합니다. 중첩 구성소는 바깥쪽에서 안쪽으로 이동하며 매칭합니다. 연결 구성소는 왼쪽부터 매칭합니다. 정규식에서 한 입력 문자열의 서로 다른 파트와 매칭할 경우 가장 앞에 오는 것을 먼저 매칭합니다. 정규식 구성에 대한 자세한 내용은 *Cisco IOS Terminal Services 컨피그레이션 가이드*의 "정규식" 부록을 참조하십시오.

커뮤니티 목록 처리

동일한 커뮤니티 목록 문에 여러 값이 구성될 경우 논리 AND 조건이 생성됩니다. 모든 커뮤니티 값이 매칭해야 AND 조건을 만족합니다. 각기 다른 커뮤니티 목록 문에 여러 값이 구성될 경우 논리 OR 조건이 생성됩니다. 조건과 매칭하는 첫 번째 목록이 처리됩니다.

예

다음 예에서는 자율 시스템 번호 50000에 속한 네트워크 10으로부터의 경로를 허용하는 표준 커뮤니티 목록을 구성합니다.

```
ciscoasa(config)#  community-list 1 permit 50000:10
```

다음 예에서는 동일한 자율 시스템의 피어 또는 동일한 연합에 속한 하위 자율 시스템 피어로부터의 경로만 허용하는 표준 커뮤니티 목록을 구성합니다.

```
ciscoasa(config)#  community-list 1 permit no-export
```

다음 예에서는 자율 시스템 65534에 속한 네트워크 40 및 자율 시스템 65412에 속한 네트워크 60에서 나온 커뮤니티를 전달하는 경로를 거부하도록 표준 커뮤니티 목록을 구성합니다. 이 예에서는 논리 AND 조건을 보여줍니다. 모든 커뮤니티 값이 매칭해야 목록이 처리될 수 있습니다.

```
ciscoasa(config)#  community-list 2 deny 65534:40 65412:60
```

다음 예에서는 로컬 자율 시스템에 속한 모든 경로를 허용하거나 자율 시스템 40000에 속한 네트워크 20으로부터의 경로를 허용하도록 명명된 표준 커뮤니티 목록을 구성합니다. 이 예에서는 논리 OR 조건을 보여주는데, 첫 번째 매칭이 처리됩니다.

```
ciscoasa(config)#  community-list standard RED permit local-AS
ciscoasa(config)#  community-list standard RED permit 40000:20
```

다음 예에서는 임의의 비공개 자율 시스템에서 나온 커뮤니티를 전달하는 경로를 거부하도록 확장 커뮤니티 목록을 구성합니다.

```
ciscoasa(config)#  community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
```

다음 예에서는 자율 시스템 50000에 속한 네트워크 1~99로부터의 경로를 거부하도록 명명된 확장 커뮤니티 목록을 구성합합니다.

```
ciscoasa(config)#  community-list expanded BLUE deny 50000:[0-9][0-9]_
```

관련 명령

명령	설명
bgp-community-new format	AA:NN 형식(자율 시스템:커뮤니티 번호/4바이트 번호)으로 커뮤니티를 표시하도록 BGP를 구성합니다.
neighbor send-community	커뮤니티 특성이 BGP 네이버로 전송되도록 지정합니다.
set community	BGP 커뮤니티 특성을 설정합니다.

compatible rfc1583

RFC 1583에 따라 요약 경로 비용을 계산하는 데 사용되는 방법을 복원하려면 라우터 컨피그레이션 모드에서 **compatible rfc1583** 명령을 사용합니다. RFC 1583 호환성을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

compatible rfc1583

no compatible rfc1583

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령의 **no** 형식만 컨피그레이션에 나타납니다.

예

다음 예에서는 RFC 1583 호환 경로 요약 비용 계산을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config-router)# no compatible rfc1583
ciscoasa(config-router)#
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

compression

SVC 연결 및 WebVPN 연결에 대한 압축을 활성화하려면 글로벌 컨피그레이션 모드에서 **compression** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

compression {**all** | **svc** | **http-comp**}

no compression {**all** | **svc** | **http-comp**}

구문 설명

all	사용 가능한 모든 압축 기술을 활성화하도록 지정합니다.
http-comp	WebVPN 연결에 대한 압축을 지정합니다.
svc	SVC 연결에 대한 압축을 지정합니다.

기본값

기본값은 *all*입니다. 사용 가능한 모든 압축 기술이 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

SVC 연결에서는 글로벌 컨피그레이션 모드에서 구성된 **compression** 명령이 그룹 정책 webvpn 및 사용자 이름 webvpn 컨피그레이션 모드에서 구성된 **svc compression** 명령을 재정의합니다.

예를 들어, 그룹 정책 webvpn 컨피그레이션 모드에서 어떤 그룹에 대해 **svc compression** 명령을 입력한 다음 글로벌 컨피그레이션 모드에서 **no compression** 명령을 입력하면 해당 그룹에 대해 구성했던 **svc compression** 명령 설정을 재정의하게 됩니다.

이와 달리 글로벌 컨피그레이션 모드에서 **compression** 명령으로 압축을 다시 활성화할 경우 모든 그룹 설정이 적용되며 이 설정이 최종적으로 압축 동작을 결정합니다.

no compression 명령으로 압축을 비활성화할 경우 새 연결만 영향을 받습니다. 활성 상태의 연결은 영향을 받지 않습니다.

예

다음 예에서는 SVC 연결에 대해 압축을 활성화합니다.

```
hostname(config)# compression svc
```

다음 예에서는 SVC 및 WebVPN 연결에 대해 압축을 비활성화합니다.

```
hostname(config)# no compression svc http-comp
```

관련 명령

명령	설명
show webvpn svc	SVC 설치에 대한 정보를 표시합니다.
svc	특정 그룹 또는 사용자에 대해 SVC를 활성화하거나 요구합니다.
svc compression	특정 그룹 또는 사용자에 대해 SVC 연결을 통한 HTTP 데이터 압축을 활성화합니다.

config-register

다음에 ASA를 다시 로드할 때 사용될 컨피그레이션 레지스터 값을 설정하려면 글로벌 컨피그레이션 모드에서 **config-register** 명령을 사용합니다. 이 값을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

config-register *hex_value*

no config-register

구문 설명

hex_value	컨피그레이션 레지스터 값을 0x0~0xFFFFFFFF 범위의 16진수 값으로 설정합니다. 이 숫자는 32비트를 나타내며, 각 16진수 문자가 4비트를 나타냅니다. 각 비트가 서로 다른 특성을 제어합니다. 그러나 비트 32부터 20까지는 나중에 사용하기 위해 예약되어 있으므로 사용자가 설정할 수 없고 현재 ASA에서도 사용하지 않습니다. 따라서 이 비트를 나타내는 3개 문자는 항상 0으로 설정되므로 무시해도 좋습니다. 관련 비트는 5개의 16진수 문자로 표시합니다. 즉 0x*nnnnn*입니다. 앞에 오는 0을 포함할 필요 없습니다. 뒤에 오는 0은 포함해야 합니다. 예를 들어, 0x2001은 0x02001과 같지만 0x10000에서는 모든 0을 표시해야 합니다. 관련 비트에 사용 가능한 값에 대한 자세한 내용은 표 8-1을 참조하십시오.

기본값

기본값은 0x1이며, 이는 로컬 이미지 및 시작 컨피그레이션에서 부팅합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 ASA 5500 시리즈에서만 지원됩니다. 이 컨피그레이션 레지스터 값에 따라 부팅할 이미지 및 기타 부팅 매개변수가 결정됩니다.

5개 문자는 오른쪽부터 왼쪽의 순서로 0~4의 숫자가 지정되는데, 이는 16진수 및 2진수의 표준입니다. 문자별로 1개의 값을 선택할 수 있으며 적절히 혼합 가능합니다. 예를 들어, 문자 3번에서 0 또는 2를 선택할 수 있습니다. 어떤 값은 다른 값과 충돌할 경우 우선적으로 적용됩니다. 이를테면 ASA가 TFTP 서버와 로컬 이미지 모두에서 부팅하게 하는 0x2011을 설정하면 ASA는 TFTP 서버에서 부팅합니다. 이 값을 사용하면 TFTP 부팅이 실패할 경우 ASA는 직접 ROMMON으로 부팅해야 합니다. 따라서 기본 이미지에서 부팅하도록 지정하는 작업은 무시됩니다.

값이 0이면 달리 명시되지 않는 한 어떤 작업도 수행되지 않습니다.

표 8-1에서는 각 16진수 문자와 연결된 작업을 나열합니다. 문자별로 1개의 값을 선택합니다.

표 8-1 컨피그레이션 레지스터 값

접두사	16진수 문자 번호 4, 3, 2, 1, 0				
0x	0	0	0[1]	0[2]	0
	1 시작 과정에서 10초 ROMMON 카운트다운을 비활성화합니다. 일반적으로 카운트다운 과정에서 Escape를 눌러 ROMMON으로 들어갈 수 있습니다.	2 ASA가 TFTP 서버에서 부팅하도록 설정할 경우 이 부팅이 실패하면 직접 ROMMON으로 부팅합니다.		1 ROMMON 부팅 매개변수에 지정된 대로 TFTP 서버 이미지에서 부팅합니다. 이는 **boot system tftp** 명령이 있을 경우 그 기능과 동일합니다. 이 값은 문자 1에 대해 설정된 값보다 우선합니다.	1 첫 번째 **boot system** *local_flash* 명령에 의해 지정된 이미지를 부팅합니다. 그 이미지가 로드되지 않을 경우 ASA는 부팅에 성공할 때까지 후속 **boot system** 명령에서 지정하는 각 이미지로 부팅을 시도합니다.
					2, 4, 6, 8 특정 **boot system** *local_flash* 명령에 의해 지정된 이미지를 부팅합니다. 값 3은 첫 번째 **boot system** 명령에서 지정된 이미지를, 값 5는 두 번째 이미지를 부팅하는 식입니다. 이미지 부팅에 성공하지 못할 경우 ASA는 다른 **boot system** 명령 이미지에 폴백하지 않습니다. 이것이 값 1을 사용할 때와 값 3을 사용할 때의 차이점입니다. 그러나 ASA에는 부팅 실패 시 내부 플래시 메모리의 루트 디렉토리에 있는 임의의 이미지에서 부팅하도록 시도하는 안전 장치가 있습니다. 이 안전 장치가 작동하지 않게 하려면 이미지를 루트가 아닌 디렉토리에 저장합니다.
				4[3] 시작 컨피그레이션을 무시하고 기본 컨피그레이션을 로드합니다.	3, 5, 7, 9 ROMMON에서 인수 없이 **boot** 명령을 입력할 경우 ASA는 특정 **boot system** *local_flash* 명령에 의해 지정된 이미지를 부팅합니다. 값 3은 첫 번째 **boot system** 명령에서 지정된 이미지를, 값 5는 두 번째 이미지를 부팅하는 식입니다. 이 값은 자동으로 이미지를 부팅하지 않습니다.
				5 뒤의 두 작업을 모두 수행합니다.	

1. 나중에 사용하도록 예약되었습니다.
2. 문자 번호 0과 1이 이미지에서 자동으로 부팅하도록 설정되지 않을 경우 ASA는 직접 ROMMON으로 부팅합니다.
3. **service password-recovery** 명령을 사용하여 비밀번호 복구를 비활성화할 경우 시작 컨피그레이션을 무시하도록 컨피그레이션 레지스터를 설정할 수 없습니다.

컨피그레이션 레지스터 값이 스탠바이 유닛에 복제되지 않지만, 활성 유닛에서 컨피그레이션 레지스터를 설정할 때 다음 경고 메시지가 표시됩니다.

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

ROMMON에서 **confreg** 명령을 사용하여 컨피그레이션 레지스터 값을 설정할 수도 있습니다.

예

다음 예에서는 기본 이미지에서 부팅하도록 컨피그레이션 레지스터를 설정합니다.

```
ciscoasa(config)# config-register 0x1
```

관련 명령

명령	설명
boot	부팅 이미지 및 시작 컨피그레이션을 설정합니다.
service password-recovery	비밀번호 복구를 활성화하거나 비활성화합니다.

configure factory-default

컨피그레이션을 공장 기본 설정으로 복원하려면 글로벌 컨피그레이션 모드에서 **configure factory-default** 명령을 사용합니다.

configure factory-default [*ip_address* [*mask*]]

구문 설명

ip_address	기본 주소 192.168.1.1을 사용하지 않고 관리 인터페이스 또 내부 인터페이스의 IP 주소를 설정합니다. 해당 모델에 어떤 인터페이스가 구성되었가에 대한 자세한 내용은 "사용 지침" 섹션을 참조하십시오.
mask	인터페이스의 서브넷 마스크를 설정합니다. 마스크를 설정하지 않을 경우 ASA는 IP 주소 클래스에 적합한 마스크를 사용합니다.

기본값

기본 IP 주소와 마스크는 각각 192.168.1.1과 255.255.255.0입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	ASA 5505의 공장 기본 컨피그레이션을 추가했습니다.

사용 지침

공장 기본 컨피그레이션은 Cisco에서 신규 ASA에 적용하는 컨피그레이션입니다. 이 명령은 PIX 525 및 PIX 535 ASA를 제외한 모든 플랫폼에서 지원됩니다.

PIX 515/515E 및 ASA 5510 이상의 ASA라면 공장 기본 컨피그레이션이 자동으로 관리 인터페이스를 구성합니다. 따라서 ASDM를 사용하여 여기에 연결한 다음 컨피그레이션을 완료할 수 있습니다. ASA 5505에서는 공장 기본 컨피그레이션이 인터페이스와 NAT를 자동으로 변환하므로 ASA는 해당 네트워크에서 즉시 사용할 수 있는 상태가 됩니다.

이 명령은 라우팅 방화벽 모드에서만 사용할 수 있습니다. 투명 모드는 인터페이스에 대한 IP 주소를 지원하지 않으며, 인터페이스 IP 주소 설정은 이 명령이 수행하는 작업 중 하나입니다. 또한 이 명령은 단일 컨텍스트 모드에서만 사용할 수 있습니다. 컨피그레이션이 지워진 ASA는 이 명령을 통해 자동으로 구성할 정의된 컨텍스트가 없습니다.

이 명령은 현재 실행 중인 컨피그레이션을 지우고 여러 명령을 구성합니다.

configure factory-default 명령에서 IP 주소를 설정할 경우 **http** 명령은 사용자가 지정하는 서브넷을 사용합니다. 이와 마찬가지로 **dhcpd address** 명령어 범위는 사용자가 지정하는 서브넷 내의 주소로 구성됩니다.

공장 기본 컨피그레이션을 복원한 다음 **write memory** 명령을 사용하여 내부 플래시 메모리에 저장합니다. **write memory** 명령을 사용하면 현재 실행 중인 컨피그레이션이 시작 컨피그레이션의 기본 위치에 저장되며, 이는 이전에 **boot config** 명령을 구성하여 다른 위치를 설정한 경우에도 마찬가지입니다. 해당 컨피그레이션이 지워지면 이 경로도 지워집니다.

참고 이 명령어를 사용하면 **boot system** 명령과 함께 나머지 컨피그레이션도 지워집니다. **boot system** 명령을 사용하면 외부 플래시 메모리 카드의 이미지를 비롯한 특정 이미지에서 부팅할 수 있습니다. 공장 기본 컨피그레이션을 복원한 후 다음번에 ASA를 다시 로드할 경우, 내부 플래시 메모리의 첫 번째 이미지에서 부팅합니다. 내부 플래시 메모리에 이미지가 없을 경우 ASA는 부팅하지 않습니다.

전체 컨피그레이션에 유용한 추가 설정을 구성하려면 **setup** 명령을 참조하십시오.

ASA 5505 컨피그레이션

ASA 5505에 대한 공장 기본 컨피그레이션은 다음 항목을 구성합니다.

- 이더넷 0/1~0/7 스위치 포트를 포함하는 내부 VLAN 1 인터페이스. **configure factory-default** 명령에서 IP 주소를 설정하지 않은 경우 VLAN 1 IP 주소와 마스크는 192.168.1.1과 255.255.255.0입니다.
- 이더넷 0/0 스위치 포트를 포함하는 외부 VLAN 2 인터페이스. VLAN 2는 DHCP를 사용하여 IP 주소를 얻습니다.
- 기본 경로도 DHCP에서 파생됩니다.
- 인터페이스 PAT를 사용하여 외부에 액세스할 때 모든 내부 IP 주소가 변환됩니다.
- 기본적으로 내부 사용자는 액세스 목록을 사용하여 외부에 액세스할 수 있으며 외부 사용자는 내부에 액세스할 수 없습니다.
- DHCP 서버가 ASA에서 활성화됩니다. 즉 VLAN 1 인터페이스와 연결하는 PC는 192.168.1.2~192.168.1.254 범위의 주소를 받습니다.
- HTTP 서버는 ASDM에 대해 활성화되며 사용자는 192.168.1.0 네트워크에서 액세스할 수 있습니다.

컨피그레이션은 다음 명령으로 구성됩니다.

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
```

```
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 이상의 컨피그레이션

ASA 5510 이상에 대한 공장 기본 컨피그레이션은 다음 항목을 구성합니다.

- 관리 0/0 인터페이스. **configure factory-default** 명령에서 IP 주소를 설정하지 않은 경우 IP 주소와 마스크는 192.168.1.1과 255.255.255.0입니다.
- DHCP 서버가 ASA에서 활성화됩니다. 즉 인터페이스와 연결하는 PC는 192.168.1.2~192.168.1.254 범위의 주소를 받습니다.
- HTTP 서버는 ASDM에 대해 활성화되며 사용자는 192.168.1.0 네트워크에서 액세스할 수 있습니다.

컨피그레이션은 다음 명령으로 구성됩니다.

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E Security Appliance 컨피그레이션

PIX 515/515E 보안 어플라이언스의 공장 기본 컨피그레이션에서는 다음 항목을 구성합니다.

- 내부 Ethernet1 인터페이스. **configure factory-default** 명령에서 IP 주소를 설정하지 않은 경우 IP 주소와 마스크는 192.168.1.1과 255.255.255.0입니다.
- DHCP 서버가 PIX 보안 어플라이언스에서 활성화됩니다. 즉 인터페이스와 연결하는 PC는 192.168.1.2~192.168.1.254 범위의 주소를 받습니다.
- HTTP 서버는 ASDM에 대해 활성화되며 사용자는 192.168.1.0 네트워크에서 액세스할 수 있습니다.

컨피그레이션은 다음 명령으로 구성됩니다.

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

예

다음 예에서는 공장 기본 컨피그레이션으로 재설정하고 인터페이스에 IP 주소 10.1.1.1을 지정한 다음 새 컨피그레이션을 시작 컨피그레이션으로 저장합니다.

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
ciscoasa(config)#
ciscoasa(config)# copy running-config startup-config
```

관련 명령

명령	설명
boot system	부팅할 소프트웨어 이미지를 설정합니다.
clear configure	실행 중인 컨텍스트를 지웁니다.
copy running-config startup-config	실행 중인 컨피그레이션을 시작 컨피그레이션에 복사합니다.
setup	ASA에 대한 기본 설정을 구성하라는 프롬프트를 표시합니다.
show running-config	실행 중인 컨피그레이션을 표시합니다.

configure http

HTTP(S) 서버에서 얻은 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합하려면 글로벌 컨피그레이션 모드에서 **configure http** 명령을 사용합니다.

configure http[s]://[*user***[:***password***]@]***server***[:***port***]/[***path***/]***filename***

구문 설명

:password	(선택 사항) HTTP(S) 인증의 경우 비밀번호를 지정합니다.
:*port*	(선택 사항) 포트를 지정합니다. HTTP는 기본값이 80입니다. HTTPS는 기본값이 443입니다.
@	(선택 사항) 이름 또는 비밀번호를 입력할 경우 서버 IP 주소의 앞에 @ 기호를 넣습니다.
filename	컨피그레이션 파일 이름을 지정합니다.
http[**s**]	HTTP 또는 HTTPS를 지정합니다.
path	(선택 사항) 파일 이름에 경로를 지정합니다.
server	서버 IP 주소 또는 이름을 지정합니다. IPv6 서버 주소의 경우 포트를 지정할 경우 IP 주소를 괄호로 묶어야 합니다. 그러면 IP 주소의 콜론이 포트 번호 앞의 콜론으로 혼동될 우려가 없습니다. 예를 들어, 다음 주소와 포트를 입력합니다. `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	(선택 사항) HTTP(S) 인증의 경우 사용자 이름을 지정합니다.

기본값

HTTP는 기본 포트가 80입니다. HTTPS는 기본 포트가 443입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 IPv4 및 IPv6 주소를 지원합니다. 병합은 새 컨피그레이션의 모든 명령을 실행 중인 컨피그레이션에 추가하고 충돌하는 명령이 있으면 새 버전으로 재정의합니다. 예를 들어, 어떤 명령에서 여러 인스턴스를 허용할 경우 새 명령이 실행 중인 컨피그레이션의 기존 명령에 추가됩니다. 어떤 명령에서 인스턴스를 하나만 허용할 경우 새 명령은 실행 중인 컨피그레이션에서 명령을 재정의합니다. 병합에서는 실행 중인 컨피그레이션에 있지만 새 컨피그레이션에서 설정되지 않은 명령을 절대 제거하지 않습니다.

이 명령은 **copy http running-config** 명령과 동일합니다. 다중 컨텍스트 모드에서는 시스템 실행 영역에서만 명령을 사용할 수 있으므로, **configure http** 명령은 컨텍스트 내에서 사용할 수 있는 대안입니다.

예

다음 예에서는 HTTPS 서버의 컨피그레이션 데이터를 실행 중인 컨피그레이션으로 복사합니다.

```
ciscoasa(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

관련 명령

명령	설명
clear configure	실행 중인 컨텍스트를 지웁니다.
configure memory	시작 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다.
configure net	지정된 TFTP URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합합니다.
configure factory-default	CLI에 입력하는 명령을 실행 중인 컨피그레이션에 추가합니다.
show running-config	실행 중인 컨피그레이션을 표시합니다.

configure memory

시작 컨피그레이션을 실행 중인 컨피그레이션과 병합하려면 글로벌 컨피그레이션 모드에서 **configure memory** 명령을 사용합니다.

configure memory

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

병합은 새 컨피그레이션의 모든 명령을 실행 중인 컨피그레이션에 추가하고 충돌하는 명령이 있으면 새 버전으로 재정의합니다. 예를 들어, 어떤 명령에서 여러 인스턴스를 허용할 경우 새 명령이 실행 중인 컨피그레이션의 기존 명령에 추가됩니다. 어떤 명령에서 인스턴스를 하나만 허용할 경우 새 명령은 실행 중인 컨피그레이션에서 명령을 재정의합니다. 병합에서는 실행 중인 컨피그레이션에 있지만 새 컨피그레이션에서 설정되지 않은 명령을 절대 제거하지 않습니다.

컨피그레이션 병합을 원치 않을 경우 실행 중인 컨피그레이션을 지울 수 있습니다. 그러면 ASA를 통한 모든 커뮤니케이션이 중지됩니다. 그런 다음 **configure memory** 명령을 입력하여 새 컨피그레이션을 로드합니다.

이 명령은 **copy startup-config running-config** 명령과 동일합니다.

다중 컨텍스트 모드에서는 컨텍스트 시작 컨피그레이션이 **config-url** 명령에 의해 지정되는 위치에 있습니다.

예

다음 예에서는 시작 컨피그레이션을 실행 중인 컨피그레이션에 복사합니다.

```
ciscoasa(config)# configure memory
```

관련 명령

명령	설명
clear configure	실행 중인 컨텍스트를 지웁니다.
configure http	지정된 HTTP(S) URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합합니다.
configure net	지정된 TFTP URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합합니다.
configure factory-default	CLI에 입력하는 명령을 실행 중인 컨피그레이션에 추가합니다.
show running-config	실행 중인 컨피그레이션을 표시합니다.

configure net

TFTP 서버에서 얻은 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합하려면 글로벌 컨피그레이션 모드에서 **configure net** 명령을 사용합니다.

configure net [*server***:[***filename***] | :***filename***]**

구문 설명

:*filename*	경로와 파일 이름을 지정합니다. 이미 **tftp-server** 명령으로 파일 이름을 설정한 경우 이 인수는 선택 사항입니다. 이 명령에서 파일 이름을, 또한 **tftp-server** 명령에서 이름을 지정할 경우 ASA는 **tftp-server** 명령의 파일 이름을 디렉토리처럼 간주하고 **configure net** 명령의 파일 이름을 이 디렉토리의 파일로 추가합니다. **tftp-server** 명령의 값을 재정의하려면 경로와 파일 이름의 앞에 슬래시를 입력합니다. 슬래시는 경로가 tftpboot 디렉토리와 상관없는 절대 경로임을 나타냅니다. 이 파일을 위해 생성되는 URL은 파일 이름 경로의 앞에 이중 슬래시(//)가 있습니다. 원하는 파일이 tftpboot 디렉토리에 있을 경우 tftpboot 디렉토리의 경로를 파일 이름 경로에 포함할 수 있습니다. **tftp-server** 명령을 사용하여 TFTP 서버 주소를 지정한 경우 콜론(:) 다음에 파일 이름만 입력할 수 있습니다.
*server***:**	TFTP 서버 IP 주소 또는 이름을 설정합니다. 이 주소는 **tftp-server** 명령에서 설정한 주소가 있다면 이를 재정의합니다. IPv6 서버 주소의 경우, IP 주소의 콜론이 파일 이름의 앞에 오는 콜론으로 혼동되지 않도록 IP 주소를 괄호로 묶어야 합니다. 이를테면 다음 주소를 입력합니다. [fe80::2e0:b6ff:fe01:3b7a] 기본 게이트웨이 인터페이스는 최상위 보안 인터페이스입니다. 그러나 **tftp-server** 명령을 사용하여 다른 인터페이스 이름을 설정할 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 IPv4 및 IPv6 주소를 지원합니다. 병합은 새 컨피그레이션의 모든 명령을 실행 중인 컨피그레이션에 추가하고 충돌하는 명령이 있으면 새 버전으로 재정의합니다. 예를 들어, 어떤 명령에서 여러 인스턴스를 허용할 경우 새 명령이 실행 중인 컨피그레이션의 기존 명령에 추가됩니다. 어떤 명령에서 인스턴스를 하나만 허용할 경우 새 명령은 실행 중인 컨피그레이션에서 명령을 재정의합니다. 병합에서는 실행 중인 컨피그레이션에 있지만 새 컨피그레이션에서 설정되지 않은 명령을 절대 제거하지 않습니다.

이 명령은 **copy tftp running-config** 명령과 동일합니다. 다중 컨텍스트 모드에서는 시스템 실행 영역에서만 명령을 사용할 수 있으므로, **configure net** 명령은 컨텍스트 내에서 사용할 수 있는 대안입니다.

예

다음 예에서는 **tftp-server** 명령에서 서버 및 파일 이름을 설정한 다음 **configure net** 명령을 사용하여 서버를 재정의합니다. 동일한 파일 이름이 사용됩니다.

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:
```

다음 예에서는 서버 및 파일 이름을 재정의합니다. 파일 이름의 기본 경로는 /tftpboot/configs/config1입니다. 경로의 /tftpboot/ 파트는 파일 이름의 앞에 슬래시(/)가 오지 않을 때 기본적으로 포함됩니다. 이 경로를 재정의하려 하고 파일이 tftpboot에 있으므로 tftpboot 경로를 **configure net** 명령에 포함합니다.

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

다음 예에서는 **tftp-server** 명령에서 서버만 설정합니다. **configure net** 명령은 파일 이름만 지정합니다.

```
ciscoasa(config)# tftp-server inside 10.1.1.1
ciscoasa(config)# configure net :configs/config1
```

관련 명령

명령	설명
configure http	지정된 HTTP(S) URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합합니다.
configure memory	시작 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다.
show running-config	실행 중인 컨피그레이션을 표시합니다.
tftp-server	다른 명령에 사용할 기본 TFTP 서버 및 경로를 설정합니다.
write net	실행 중인 컨피그레이션을 TFTP 서버에 복사합니다.

configure terminal

실행 중인 컨피그레이션을 명령줄에서 구성하려면 특별 권한 EXEC 모드에서 **configure terminal** 명령을 사용합니다.

configure terminal

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 글로벌 컨피그레이션 모드를 시작하며, 여기에서 컨피그레이션을 변경할 명령을 입력할 수 있습니다.

예

다음 예에서는 글로벌 컨피그레이션 모드를 시작합니다.

```
ciscoasa# configure terminal
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure	실행 중인 컨텍스트를 지웁니다.
configure http	지정된 HTTP(S) URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합합니다.
configure memory	시작 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다.
configure net	지정된 TFTP URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합합니다.
show running-config	실행 중인 컨피그레이션을 표시합니다.

config-url

시스템에서 컨텍스트 컨피그레이션을 다운로드하는 URL을 식별하려면 컨텍스트 컨피그레이션 모드에서 **config-url** 명령을 사용합니다.

config-url *url*

구문 설명

url 컨텍스트 컨피그레이션 URL을 설정합니다. 모든 원격 URL은 관리 컨텍스트에서 액세스 가능해야 합니다. 다음 URL 구문을 참조하십시오.

- **disk0:/**[*path*/]*filename*

  ASA 5500 시리즈에서는 이 URL이 내부 플래시 메모리를 가리킵니다. **flash** 명령을 **disk0** 명령 대신 사용할 수 있습니다. 별칭입니다.
- **disk1:/**[*path*/]*filename*

  ASA 5500 시리즈에서는 이 URL이 외부 플래시 메모리 카드를 가리킵니다.
- **flash:/**[*path*/]*filename*

  이 URL이 내부 플래시 메모리를 가리킵니다.
- **ftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]

  type은 다음 키워드 중 하나가 될 수 있습니다.
  - **ap**—ASCII 패시브 모드
  - **an**—ASCII 일반 모드
  - **ip**—(기본값) 2진 패시브 모드
  - **in**—2진 일반 모드
- **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*
- **tftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*]

  서버 address 경로를 재정의하려면 인터페이스 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

컨텍스트 URL을 추가하면 시스템은 즉시 컨텍스트를 로드하여 실행되게 합니다.

참고 **allocate-interface** 명령을 **config-url** 명령보다 먼저 입력합니다. ASA는 컨텍스트 컨피그레이션을 로드하기 전에 컨텍스트에 인터페이스를 지정해야 합니다. 컨텍스트 컨피그레이션은 인터페이스를 참조하는 명령(**interface**, **nat**, **global**)을 포함할 수 있습니다. **config-url** 명령을 먼저 입력하면 ASA는 즉시 컨텍스트 컨피그레이션을 로드합니다. 컨텍스트에 인터페이스를 참조하는 명령이 있을 경우 그 명령은 실패합니다.

파일 이름에서 확장자가 필요하지는 않지만 ".cfg"를 사용하는 것이 좋습니다.

관리 컨텍스트 파일이 내부 플래시 메모리에 저장되어야 합니다.

HTTP 또는 HTTPS 서버에서 컨텍스트 컨피그레이션을 다운로드할 경우 **copy running-config startup-config** 명령을 사용하여 이 서버에 변경 사항을 다시 저장할 수 없습니다. 그러나 **copy tftp** 명령으로 실행 중인 컨피그레이션을 TFTP 서버에 복사할 수 있습니다.

서버가 사용할 수 없는 상태이거나 파일이 존재하지 않아 시스템에서 컨텍스트 컨피그레이션 파일을 검색할 수 없을 경우, 빈 컨텍스트가 만들어지며 이는 명령줄 인터페이스를 사용하여 즉시 구성할 수 있습니다.

URL을 변경하려면 새 URL과 함께 **config-url** 명령을 다시 입력합니다.

ASA에서는 새 컨피그레이션을 현재 실행 중인 컨피그레이션과 병합합니다. 동일한 URL을 다시 입력하면 역시 저장된 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다. 병합은 새 컨피그레이션의 새로운 명령을 실행 중인 컨피그레이션에 추가합니다. 컨피그레이션이 동일할 경우 어떤 변경도 없습니다. 명령이 충돌하거나 명령이 컨텍스트 실행에 영향을 줄 경 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다. 실행 중인 컨피그레이션이 비어 있을 경우(예: 서버가 사용할 수 없는 상태이고 컨피그레이션이 다운로드된 적이 없는 경우) 새로운 컨피그레이션이 사용됩니다. 컨피그레이션의 병합을 원치 않는다면 실행 중인 컨피그레이션을 지운 다음(해당 컨텍스트를 통한 모든 통신이 중지됨) 새 URL에서 컨피그레이션을 다시 로드하면 됩니다.

예

다음 예에서는 관리 컨텍스트를 "administrator"로 설정하고 내부 플래시 메모리에 "administrator"라는 컨텍스트를 만든 다음 FT 서버에서 2개의 컨텍스트를 추가합니다.

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url flash:/admin.cfg

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)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

관련 명령

명령	설명
allocate-interface	컨텍스트에 인터페이스를 할당합니다.
context	시스템 컨피그레이션에서 보안 컨텍스트를 만들고 컨텍스트 컨피그레이션 모드를 시작합니다.
show context	컨텍스트의 목록(시스템 실행 영역) 또는 현재 컨텍스트에 대한 정보를 표시합니다.

conn-rebalance

클러스터의 멤버 간에 연결 리밸런싱을 활성화하려면 클러스터 그룹 컨피그레이션 모드에서 **conn-rebalance** 명령을 사용합니다. 연결 리밸런싱을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

conn-rebalance [frequency *seconds***]**

no conn-rebalance [frequency *seconds***]**

구문 설명

frequency *seconds*	(선택 사항) 로드 정보가 교환되는 빈도를 1초~360초의 범위에서 지정합니다. 기본값은 5초입니다.

명령 기본값

연결 리밸런싱은 기본적으로 비활성화되어 있습니다.

활성화된 경우 기본 빈도는 5초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

업스트림 또는 다운스트림 라우터의 로드 밸런싱 기능을 사용하는 도중 흐름이 균일하게 분산되지 않을 경우, 오버로드된 유닛에서 새 흐름을 다른 유닛에 리디렉션하도록 구성할 수 있습니다. 기존 흐름은 다른 유닛으로 이동되지 않습니다. 활성화할 경우 ASA에서는 로드 정보를 주기적으로 교환하며, 로드가 과중한 디바이스에서 적은 디바이스로 새 연결을 오프로드합니다.

이 명령은 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.

예

다음 예에서는 연결 리밸런싱 빈도를 60초로 설정합니다.

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용하면 ASA에서는 cLACP를 통해 네이버 스위치와 EtherChannel을 협상합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드를 시작합니다.
cluster-interface	클러스터 제어 링크 인터페이스를 지정합니다.
cluster interface-mode	클러스터 인터페이스 모드를 설정합니다.
console-replicate	슬레이브 유닛에서 마스터 유닛으로의 콘솔 복제를 활성화합니다.
enable (cluster group)	클러스터링을 활성화합니다.
health-check	클러스터 상태 검사 기능을 활성화합니다. 여기에는 유닛 상태 모니터링 및 인터페이스 상태 모니터링이 포함됩니다.
key	클러스터 제어 링크의 제어 트래픽에 대해 인증 키를 설정합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스를 위한 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택에서 이 유닛의 우선 순위를 설정합니다.

console timeout

인증된 시리얼 콘솔 세션에 대해 무활동 시간 초과를 설정하여(**aaa authentication serial console**) 이 시간 경과 시 사용자가 로그아웃되게 하거나 인증된 활성화 세션(**aaa authentication enable console**)에서 시간 초과 경과 시 사용자가 특별 권한 EXEC 모드를 종료하고 사용자 EXEC 모드로 돌아가게 하려면 글로벌 컨피그레이션 모드에서 **console timeout** 명령을 사용합니다. 인증된 시리얼 콘솔 세션에 대해 무활동 시간 초과를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

console timeout [*number*]

no console timeout [*number*]

구문 설명

number	콘솔 세션이 끝난 이후의 유휴 시간(0분~60분)을 지정합니다. 0은 콘솔이 시간 초과되지 않음을 의미합니다.

기본값

기본 시간 초과는 0입니다. 즉 콘솔 세션에 시간 초과가 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

console timeout 명령은 인증된 시리얼 또는 활성화 연결에만 적용됩니다. 이 명령은 텔넷, SSH 또는 HTTP 시간 초과를 변경하지 않습니다. 이 액세스 방식은 각자의 시간 초과 값을 유지합니다. 이 명령은 인증되지 않은 콘솔 연결에는 적용되지 않습니다.

no console timeout 명령은 콘솔 시간 초과 값을 기본 시간 초과인 0으로 재설정합니다. 그러면 콘솔은 시간 초과되지 않습니다.

예

다음 예에서는 콘솔 시간 초과를 15분으로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# console timeout 15
```

관련 명령

명령	설명
clear configure console	기본 콘솔 연결 설정을 복원합니다.
clear configure timeout	컨피그레이션에서 기본 유휴 기간을 복원합니다.
show running-config console timeout	ASA와의 콘솔 연결에 대한 유휴 타이머를 표시합니다.

console-replicate

ASA 클러스터의 슬레이브 유닛에서 마스터 유닛으로 콘솔 복제를 활성화하려면 클러스터 그룹 컨피그레이션 모드에서 **console-replicate** 명령을 사용합니다. 콘솔 복제를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

console-replicate

no console-replicate

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

콘솔 복제는 기본적으로 비활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서는 중요한 특정 이벤트 발생 시 일부 메시지를 콘솔에 직접 출력합니다. 콘솔 복제를 활성화할 경우, 슬레이브 유닛에서는 콘솔 메시지를 마스터 유닛에 전송하므로 클러스터의 콘솔 포트 하나만 모니터링하면 됩니다.

이 명령은 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.

예

다음 예에서는 콘솔 복제를 활성화합니다.

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# console-replicate
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용하면 ASA에서는 cLACP를 통해 네이버 스위치와 EtherChannel을 협상합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드를 시작합니다.
cluster-interface	클러스터 제어 링크 인터페이스를 지정합니다.
cluster interface-mode	클러스터 인터페이스 모드를 설정합니다.
conn-rebalance	연결 리밸런싱을 활성화합니다.
enable (cluster group)	클러스터링을 활성화합니다.
health-check	클러스터 상태 검사 기능을 활성화합니다. 여기에는 유닛 상태 모니터링 및 인터페이스 상태 모니터링이 포함됩니다.
key	클러스터 제어 링크의 제어 트래픽에 대해 인증 키를 설정합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스를 위한 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택에서 이 유닛의 우선 순위를 설정합니다.

content-length

HTTP 메시지 바디 길이를 기준으로 HTTP 트래픽을 제한하려면, http-map 컨피그레이션 모드에서 **content-length** 명령을 사용합니다. 이 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

content-length { min *bytes* **[max** *bytes***] | max** *bytes***] } action {allow | reset | drop} [log]**

content-length { min *bytes* **[max** *bytes***] | max** *bytes***] } action {allow | reset | drop} [log]**

구문 설명

action	이 검사에서 메세지 실패 시의 작업을 지정합니다.
allow	메시지를 허용합니다.
bytes	바이트 수를 지정합니다. 허용 범위는 **최소** 옵션 1 ~ 65535이고, **최대** 옵션 1 ~ 50000000입니다.
drop	연결을 닫습니다.\
log	(선택 사항) syslog를 생성합니다.
max	(선택 사항) 허용된 최대 콘텐츠 길이를 지정합니다.
min	허용된 최소 콘텐츠 길이를 지정합니다.
reset	클라이언트와 서버에 TCP 리셋 메시지를 보냅니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Http-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

content-length 활성화한 후에는 구성된 범위 내에서 ASA만이 메시지를 허용하며 그렇지 않은 경우 지정된 조치를 취합니다. ASA가 TCP 연결을 리셋하고 syslog 입력을 생성하게 하려면 **action** 키워드를 사용합니다.

예

HTTP 트래픽을 100바이트 이상이지만 2000바이트는 초과하지 않는 메시지로 제한합니다. 메시지가 이 범위를 벗어나는 경우, ASA가 TCP 연결을 리셋하고 syslog 입력을 생성합니다.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# content-length min 100 max 2000 action reset log
ciscoasa(config-http-map)# exit
```

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
http-map	HTTP 맵을 고급 HTTP 검사 구성용으로 정의합니다.
debug appfw	고급 HTTP 검사와 연관된 트래픽에 관한 자세한 정보를 표시합니다.
inspect http	애플리케이션 검사에 사용하도록 특정 HTTP 맵을 적용합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.

context

시스템 컨피그레이션과 컨텍스트 입력 컨피그레이션 모드에서 보안 컨텍스트를 생성하려면, 글로벌 컨피그레이션 모드에서 context 명령을 사용합니다. 규칙을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

context *name*

no context *name* **[noconfirm]**

구문 설명

name	최대 32자의 문자열로 이름을 설정합니다. 이 이름은 대/소문자를 구분합니다. 즉 "customerA"와 "CustomerA"는 2개의 컨텍스트입니다. 문자, 숫자 또는 하이픈을 사용할 수 있으나 하이픈으로 이름을 시작하거나 끝내서는 안 됩니다. "System"과 "Null"(대문자 및 소문자 모두 해당)은 예약된 이름이므로 사용할 수 없습니다.
noconfirm	(선택 사항) 확인 프롬프트 없이 컨텍스트를 제거합니다. 이 옵션은 자동화된 스크립트에 유용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

컨텍스트 컨피그레이션 모드에서, 컨텍스트에서 사용할 수 있는 컨피그레이션 파일 URL과 인터페이스를 식별할 수 있습니다. 관리 컨텍스트가 없는 경우에는(예를 들어, 컨피그레이션을 지우는 경우), 추가하는 첫 번째 컨텍스트가 관리 컨텍스트여야만 합니다. 관리 컨텍스트를 추가하려면, **admin-context** 명령을 참조하십시오. 관리 컨텍스트를 지정한 후에는, **context** 명령을 입력하여 관리 컨텍스트를 구성할 수 있습니다.

시스템 컨피그레이션 수정을 통해서만 컨텍스트를 제거할 수 있습니다. 이 명령의 **no** 양식을 사용해서는 현재 관리 컨텍스트를 제거할 수 없으며, **clear configure context** 명령을 사용하여 모든 컨텍스트를 제거하는 경우에만 현재 관리 컨텍스트를 제거할 수 있습니다.

예

다음 예에서는 관리 컨텍스트를 "administrator"로 설정하고 내부 플래시 메모리에 "administrator"라는 컨텍스트를 만든 다음 FT 서버에서 2개의 컨텍스트를 추가합니다.

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url flash:/admin.cfg

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)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

관련 명령

명령	설명
allocate-interface	컨텍스트에 인터페이스를 할당합니다.
changeto	컨텍스트와 시스템 실행 영역 간에 변경합니다.
config-url	컨텍스트 컨피그레이션 위치를 지정합니다.
join-failover-group	장애 조치 그룹에 컨텍스트를 지정합니다.
show context	컨텍스트 정보를 표시합니다.

copy

ASA 플래시 메모리에서 또는 메모리로 파일을 복사하려면 특권 실행 모드에서 **copy** 명령을 사용합니다.

copy [/noconfirm] [/pcap] [/noverify] {*url* **| running-config | startup-config}**
{running-config | startup-config | *url***}**

구문 설명

/noconfirm	(선택 사항) 확인 프롬프트 없이 파일을 복사합니다.
/pcap	(선택 사항) **capture** 명령의 원시 패킷 캡처 덤프를 지정합니다.
/noverify	(선택 사항) 개발 키 서명 이미지 복사 시 서명 확인을 생략하려면 사용합니다.
running-config	시스템 메모리에 저장된 실행 컨피그레이션을 지정합니다.
startup-config	플래시 메모리에 저장된 시작 컨피그레이션을 지정합니다. 단일 모드 또는 다중 컨텍스트 모드의 시스템용 시작 컨피그레이션은 플래시 메모리 내 숨겨진 파일로 있습니다. 컨텍스트 내에서 시작 컨피그레이션 위치는 **config-url** 명령에 의해 지정됩니다. 예를 들어, **config-url** 명령에 대해 HTTP 서버를 지정한 다음 **copy startup-config running-config** 명령을 입력하는 경우 ASA는 관리 컨텍스트 인터페이스를 사용하여 HTTP 서버에서 시작 컨피그레이션을 복사합니다.

url 로컬 및 원격 위치 간에 복사할 소스 또는 목적지 파일을 지정합니다. (한 원격 서버에서 또다른 원격 서버로 복사할 수 없습니다.) 컨텍스트에서 컨텍스트 인터페이스를 사용하여 TFTP 또는 FTP 서버로 실행 또는 시작 컨피그레이션을 복사할 수는 있지만, 서버에서 실행 또는 시작 컨피그레이션으로 복사할 수는 없습니다. 다른 옵션은 **startup-config** 키워드를 참조하십시오. TFTP 서버에서 실행 컨텍스트 컨피그레이션으로 다운로드하려면 **configure net** 명령을 사용합니다. 이 명령에서는 다음 URL 구문을 사용합니다.

- **cache:/**[[*path*/]*filename*]—파일 시스템의 캐시 메모리를 가리킵니다.
- **capture:/**[[*context_name*/]*buffer_name*]—캡처 버퍼의 출력을 가리킵니다.
- **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*]—**flash** 및 **disk0**이 내부 플래시 메모리를 가리킵니다. 두 옵션 중 하나를 사용할 수 있습니다.
- **disk1:/**[[*path*/]*filename*]—외부 메모리를 가리킵니다.
- **smb:/**[[*path*/]*filename*]—UNIX 서버 로컬 파일 시스템을 가리킵니다. 데이터와 교환 정보를 다른 시스템과 함께 패키지로 제공하려면 LAN 매니저 및 유사 네트워크 시스템의 서버 메시지 블록 파일-시스템 프로토콜을 사용합니다.
- **ftp://**[[*user*[**:***password*]**@**]*server*[*:port*]/[*path*/]*filename*[**;type=***xx*]]—**type**은 **ap**(ASCII 패시브 모드), **an**(ASCII 일반 모드), **ip**(기본값—바이너리 패시브 모드), **in**(바이너리 일반 모드)와 같은 키워드 중 하나일 수 있습니다.
- **http**[**s**]**://**[[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*]
- **scp://**[[*user*[**:***password*]**@**]*server*[**/***path*]**/***filename*[**;int=***interface_name*]]—**;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다.
- **system:/**[[*path*/]*filename*]—시스템 메모리를 나타냅니다.
- **tftp://**[[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*[**;int=***interface_name*]]

  경로이름에는 공백을 포함할 수 없습니다. 경로이름에 공백이 있는 경우, **copy tftp** 명령 대신에 **tftp-server** 명령에서 경로를 설정합니다. **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 TFTP 서버에 연결합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
특별 권한 EXEC	• 예	• 예	• 예	• 예[1]	• 예

1. 컨텍스트 내에서는 실행-컨피그레이션 또는 시작 컨피그레이션을 외부 URL로 복사만 할 수 있습니다.

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	DNS 이름 지원이 추가되었습니다.
8.0(2)	**smb** 옵션이 추가되었습니다.
9.1(5)	**scp** 옵션이 추가되었습니다.
9.3(2)	**noverify** 옵션이 추가되었습니다.

사용 지침

- 어떤 컨피그레이션을 실행 중인 컨피그레이션에 복사하면 두 컨피그레이션을 병합하는 것입니다. 병합은 새 컨피그레이션의 새로운 명령을 실행 중인 컨피그레이션에 추가합니다. 컨피그레이션이 동일할 경우 어떤 변경도 없습니다. 명령이 충돌하거나 명령이 컨텍스트 실행에 영향을 줄 경 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다.
  RSA 키를 NVRAM에 저장할 수 없는 경우, 다음 오류 메시지가 표시됩니다.

  ```
  ERROR: NV RAM does not have enough space to save keypair keypair name
  ```

- 클러스터 전체 캡처를 수행한 후에는, 마스터 유닛에서 다음 명령을 입력하여 동일한 캡처 파일을 클러스터의 모든 유닛으로부터 TFTP 서버로 동시에 복사할 수 있습니다.

  ```
  hostname (config-cluster)# cluster exec copy /pcap capture: cap_name
  tftp://location/path/filename.pcap
  ```

  유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일 이름에는 유닛 이름이 자동으로 추가됩니다(예: filename_A.pcap, filename_B.pcap 등). 여기서 A와 B는 클러스터 유닛 이름입니다.

참고 파일 이름의 끝에 유닛 이름을 추가하면 다른 목적지 이름이 생성됩니다.

예

다음 예에서는 디스크에서 시스템 실행 영역의 TFTP 서버로 파일을 복사하는 방법을 보여줍니다.

```
ciscoasa(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

다음 예에서는 디스크의 한 위치에서 다른 위치로 파일을 복사하는 방법을 보여줍니다. 목적지 파일의 이름은 소스 파일의 이름이거나 또는 다른 이름일 수 있습니다.

```
ciscoasa(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

다음 예에서는 TFTP 서버에서 내부 플래시 메모리로 ASDM 파일을 복사하는 방법을 보여줍니다.

```
ciscoasa(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

다음 예에서는 컨텍스트의 실행 중인 컨피그레이션을 TFTP 서버에 복사하는 방법을 보여줍니다.

```
ciscoasa(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

copy 명령은 앞 예의 다음 버전에서 보여주는 것처럼 IP 주소뿐 아니라 DNS 이름도 지원합니다.

```
ciscoasa(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

다음 예에서는 전체 경로를 지정하지 않고 **copy capture** 명령을 입력할 때 제공되는 프롬프트를 보여줍니다.

```
ciscoasa(config)# copy capture:abc tftp
Address or name of remote host [209.165.200.224]?
Source file name [username/cdisk]?
copying capture to tftp://209.165.200.224/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

전체 경로를 다음과 같이 지정할 수 있습니다.

```
ciscoasa(config)# copy capture:abc tftp:209.165.200.224/tftpboot/abc.cap
```

TFTP 서버가 이미 구성된 경우 그 위치 또는 파일 이름은 다음과 같이 미지정 상태일 수 있습니다.

```
ciscoasa(config)# tftp-server outside 209.165.200.224 tftp/cdisk
ciscoasa(config)# copy capture:abc tftp:/tftp/abc.cap
```

다음 예에서는 개발 키가 서명된 이미지를 검증 없이 복사하는 방법을 보여줍니다.

```
ciscoasa(config)# copy /noverify lfbff.SSA exa_lfbff.SSA

Source filename [lfbff.SSA]?

Destination filename [exa_lfbff.SSA]?

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

관련 명령

명령	설명
configure net	TFTP 서버의 파일을 실행 중인 컨피그레이션으로 복사합니다.
copy capture	TFTP 서버에 캡처 파일을 복사합니다.
tftp-server	기본 TFTP 서버를 설정합니다.
write memory	실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.
write net	실행 중인 컨피그레이션을 TFTP 서버에 복사합니다.

cpu hog granular-detection

짧은 시간에 실시간 과다 사용 탐지를 제공하고 CPU 과다 사용 임계값을 설정하려면 특별 권한 EXEC 모드에서 **cpu hog granular-detection** 명령을 사용합니다.

cpu hog granular-detection [count *number***] [threshold** *value***]**

구문 설명

count *number*	코드 실행 중단 횟수를 나타냅니다. 유효한 값은 1~10000000입니다. 권장되는 기본값은 1000입니다.
threshold *value*	범위는 1~100입니다. 설정되지 않으면 기본값이 사용됩니다. 이는 플랫폼에 따라 달라집니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

cpu hog granular-detection 명령은 현재 코드 실행을 10밀리초마다 중단시키며, 총 중단 횟수가 계수입니다. 중단 시 CPU 과다 사용 여부를 확인합니다. 해당될 경우 로그에 기록합니다. 이 명령은 데이터 경로에서 CPU 과다 사용 탐지의 세분화를 낮춥니다.

각 스케줄러 기반의 과다 사용은 최대 5개의 중단 기반 과다 사용 엔트리와 연결됩니다. 각 엔트리는 최대 3개의 추적을 포함할 수 있습니다. 중단 기반의 과다 사용은 덮어쓸 수 없습니다. 공간이 없을 경우 새 것을 삭제합니다. 스케줄러 기반의 과다 사용은 LRU 정책에 따라 계속 재사용됩니다. 그러면 중단 기반의 과다 사용이 지워집니다.

참고 작은 UDP 패킷으로 ASA 5585-X의 성능에 영향을 미칠 수 있습니다.

예

다음 예에서는 CPU 과다 사용 탐지를 트리거하는 방법을 보여줍니다.

```
ciscoasa# cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer under heavy
traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

관련 명령

명령	설명
show process cpu-hog	CPU를 과다 사용하고 있는 프로세스를 표시합니다.
clear process cpu-hog	CPU를 과다 사용하고 있는 프로세스를 지웁니다.

cpu profile activate

CPU 프로파일링을 시작하려면 특별 권한 EXEC 모드에서 **cpu profile activate** 명령을 사용합니다.

cpu profile activate *n-samples* **[sample-process** *process-name***] [trigger cpu-usage** *cpu %* **[***process-name***]]**

구문 설명

n-samples	*n*개의 샘플을 저장할 메모리를 할당합니다. 유효한 값의 범위는 1~100,000입니다.
sample-process *process-name*	특정 프로세스만 샘플링합니다.
trigger cpu-usage *cpu %*	전역 5초 CPU 백분율이 더 큰 값인 한 프로파일러가 시작할 수 없게 하고 CPU 백분율이 이 값보다 낮아지면 프로파일러를 중단합니다.
trigger cpu-usage *cpu % process-name*	프로세스 5초 CPU 백분율을 트리거로 사용합니다.

기본값

*n-samples*의 기본값은 1000입니다.

*cpu %*의 기본값은 0입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.1(2)	**sample-process** *process-name*, **trigger cpu-usage** *cpu % ,* **trigger cpu-usage** *cpu % process-name* 옵션을 추가했습니다. 출력 형식을 업데이트했습니다.

사용 지침

CPU 프로파일러는 어떤 프로세스에서 더 많은 CPU를 사용하고 있는지 확인하는 데 활용할 수 있습니다. CPU 프로파일링에서는 타이머 인터럽트가 실행되었을 때 CPU에서 실행 중이던 프로세스의 주소를 캡처합니다. 이 프로파일링은 CPU 부하에 관계없이 10밀리초마다 수행됩니다. 예를 들어, 5,000개의 샘플을 수집하면 프로파일링이 완료되는 데 정확히 50초가 걸립니다. CPU 프로파일러에서 사용하는 CPU 시간의 양이 상대적으로 적을 경우 샘플 수집에 더 많은 시간이 걸립니다. CPU 프로필 레코드는 별도의 버퍼에서 샘플링됩니다.

show cpu profile 명령과 **cpu profile activate** 명령을 함께 사용하여 수집 가능한 정보 및 TAC에서 CPU 문제 해결에 사용할 수 있는 정보를 표시합니다. **show cpu profile dump** 명령 출력은 16진수 형식입니다.

CPU 프로파일러에서 시작 조건을 기다리는 중이라면 **show cpu profile** 명령은 다음 출력을 표시합니다.

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

예

다음 예에서는 프로파일러를 활성화하고 1,000개의 샘플을 저장하도록 지시합니다.

```
hostname# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

다음 예에서는 프로파일링의 상태(진행 중 및 완료됨)를 표시합니다.

```
hostname# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.

hostname# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
---------------------------
…
---------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

관련 명령

명령	설명
show cpu profile	CPU 프로파일링 진행 상황을 표시합니다.
show cpu profile dump	미완료 또는 완료 프로파일링 결과를 표시합니다.

coredump enable

코어덤프 기능을 활성화하려면 **coredump enable** 명령을 입력합니다. 이 명령을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

coredump enable [filesystem [disk0: | disk1: | flash:] [size [default | size_in_MB]]

[no] coredump enable [filesystem [disk0: | disk1: | flash:] [size [default | size_in_MB]]

구문 설명

default	ASA에서 기본값을 계산하므로 사용하도록 제안된 값이 기본값임을 나타냅니다.
filesystem disk0: | disk1: | flash:	코어덤프 파일을 저장할 디스크를 지정합니다.
size	ASA 플래시에 있는 코어덤프 파일 시스템 이미지에 할당된 총 크기를 정의합니다. 코어덤프를 구성할 때 사용 가능한 공간이 충분하지 않으면 오류 메시지가 나타납니다. **size** 옵션을 일종의 컨테이너로 간주할 수 있습니다. 즉 생성되는 코어덤프는 결코 이 크기를 초과하여 디스크 공간을 사용할 수 없습니다.
size_in_MB	ASA에서 기본값을 재정의하고 (공간이 있을 경우) 지정된 값(MB)을 코어덤프 파일 시스템에 할당할 것임을 나타냅니다.

기본값

기본적으로 코어덤프는 활성화되어 있지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

이 기능을 활성화하면 문제 해결과 관련하여 중요한 정보를 제공합니다. 이 기능을 비활성화하면 모든 구성 요소에 대해 시스템 충돌 시 코어덤프 파일이 생성되지 않습니다. 또한 이 기능을 비활성화하더라도 이전의 코어덤프 파일 시스템 이미지 및/또는 코어덤프 파일 시스템 이미지 내용이 삭제되지 않습니다. 코어덤프를 활성화할 때 코어덤프 파일 시스템의 생성을 허용하라는 프롬프트가 나타납니다. 이는 확인 프롬프트로서 생성될 코어덤프 파일 시스템의 크기(MB)가 포함됩니다. 코어덤프를 활성화하거나 비활성화한 다음 반드시 컨피그레이션을 저장해야 합니다.

코어덤프가 활성화되면 다음 파일 요소가 생성됩니다. 이 파일 요소를 명시적으로 조작해서는 안 됩니다.

- coredumpfsys – 코어덤프 이미지를 포함하는 디렉토리
- coredumpfsysimage.bin –코어덤프 관리에 사용되는 코어덤프 파일 시스템 이미지
- coredumpinfo – 코어덤프 로그를 포함하는 디렉토리

참고 코어덤프를 비활성화할 경우 충돌 정보 파일 생성에는 영향을 주지 않습니다.

ASA의 애플리케이션이나 시스템 충돌 문제를 해결하기 위해 코어덤프 기능을 활성화하도록 Cisco TAC에서 요청할 수 있습니다.

참고 코어덤프 파일을 아카이브에 보관해야 합니다. 후속 코어덤프가 수행되면서 최신 코어덤프를 수용하기 위해 이전의 코어덤프를 제거할 가능성이 있기 때문입니다. 코어덤프 파일은 구성된 파일 시스템(예: "disk0:/coredumpfsys" 또는 "disk1:/coredumpfsys")에 위치하며 ASA에서 제거될 수 있습니다.

코어덤프를 활성화하려면 다음 단계를 수행합니다.

1. /root 디렉토리에 있어야 합니다. 콘솔에서 디렉토리 위치를 확인하려면 **pwd** 명령을 입력합니다.
2. 필요하다면 **cd disk0:/**, **cd disk1:/**, **cd flash:/** 명령 중 하나를 입력하여 디렉토리를 변경합니다.
3. **coredump enable** 명령을 입력합니다.

ASA에 발생한 충돌을 해결하기 위해 **coredump** 명령을 사용할 때 충돌 후 어떤 코어덤프 파일도 저장되지 않을 수 있습니다. 코어덤프 기능이 활성화되었고 디스크 공간이 사전 할당된 코어덤프 파일 시스템이 생성되었을 때 생길 수 있는 경우입니다. 대개는 많은 양의 RAM을 할당한, 사용량이 많은 ASA에서 몇 주 후 발생한 충돌을 해결하는 과정에서 이러한 조건이 나타납니다.

show coredump 명령의 출력에서 다음과 비슷한 내용이 나타납니다.

```
Coredump Aborted as the complete coredump could not be written to flash
   Filesystem full on 'disk0', current coredump size <size> bytes too big for allocated
   filesystem
```

이러한 문제를 줄이려면 전체 메모리를 수용하고 코어덤프 파일 시스템에 적당한 공간을 할당할 만큼 큰 코어덤프 파일 시스템 카드가 있어야 합니다.

예 다음 예에서 각 느낌표(!)는 기록되는 코어덤프 파일 시스템의 1MB를 나타냅니다.

다음 예에서는 기본값과 **disk0:**을 사용하여 코어덤프 파일 시스템을 만듭니다.

```
hostname(config)# coredump enable
Warning: Enabling coredump on an ASA5505 platform will delay the reload of the system in
the event of software forced reload. The exact time depends on the size of the coredump
generated.
Proceed with coredump filesystem allocation of 60 MB on 'disk0:' (Note this may take a
while) [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

다음 예에서는 **disk1:**에 120MB 코어덤프 파일 시스템을 만들어 파일 시스템 및 크기를 지정하는 방법을 보여줍니다.

```
hostname(config)# coredump enable filesystem disk1: size 120
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceed with coredump filesystem allocation of 120 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

다음 예에서는 코어덤프 파일 시스템의 크기를 120MB에서 100MB로 조정하는 방법을 보여줍니다.

참고 120MB 코어덤프 파일 시스템의 내용은 보존되지 않으므로, 이 작업에 앞서 이전의 코어덤프를 보관해야 합니다.

```
hostname(config)# coredump enable filesystem disk1: size 100
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceeding with resizing to 100 MB results in
deletion of current 120 MB coredump filesystem and
its contents on 'disk1:', proceed ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
```

다음 예에서는 처음에는 **disk0:**에서 그 다음에는 **disk1:**에서 코어덤프를 활성화합니다. **default** 키워드도 사용합니다.

참고 2개의 활성 코어덤프 파일 시스템을 할당하지 않으므로 진행하기 전에 이전의 코어덤프 파일 시스템을 삭제해야 합니다.

```
hostname(config)# coredump enable filesystem disk1: size default
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Coredump is currently configured on 'disk0:', upon successful
configuration on 'disk1:', the coredump filesystem will be
deleted on 'disk0:', proceed ? [confirm]
Proceed with coredump filesystem allocation of 100 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
```

다음 예에서는 코어덤프 파일 시스템을 비활성화하는 방법을 보여줍니다. 그러나 현재 코어덤프 파일 시스템 이미지와 그 내용은 영향을 받지 않습니다.

```
hostname(config)# no coredump enable
```

코어덤프를 다시 활성화하려면 원래 코어덤프 파일 시스템을 구성하기 위해 사용했던 명령을 다시 입력합니다.

다음 예에서는 코어덤프를 비활성화했다가 다시 활성화합니다.

- 기본값 사용:

```
hostname(config)# coredump enable
hostname(config)# no coredump enable
hostname(config)# coredump enable
```

- 명시적 값 사용:

```
hostname(config)# coredump enable filesystem disk1: size 200
hostname(config)# no coredump enable
hostname(config)# coredump enable filesystem disk1: size 200
```

관련 명령

명령	설명
clear configure coredump	시스템에서 코어덤프 파일 시스템과 그 내용을 제거합니다. 코어덤프 로그도 지웁니다.
clear coredump	현재 코어덤프 파일 시스템에 저장된 코어덤프를 모두 제거하고 코어덤프 로그를 지웁니다.
show coredump filesystem	코어덤프 파일 시스템의 파일을 표시하고 얼마나 차지할지 보여줍니다.
show coredump log	코어덤프 로그를 표시합니다.

crashinfo console disable

충돌 정보가 콘솔에 출력되지 않게 하려면 글로벌 컨피그레이션 모드에서 **crashinfo console disable** 명령을 사용합니다.

crashinfo console disable

no crashinfo console disable

구문 설명

disable	충돌 발생 시 콘솔에 출력하지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(4)	이 명령을 도입했습니다.

사용 지침

이 명령을 사용하면 충돌 정보가 콘솔에 출력되지 않게 할 수 있습니다. 충돌 정보에는 디바이스에 연결된 모든 사용자가 보기에는 적합하지 않은 민감한 성격의 정보가 포함될 수도 있습니다. 이 명령을 사용할 뿐 아니라 충돌 정보를 플래시에 기록하여 디바이스 재부팅 후 확인할 수 있게 해야 합니다. 이 명령은 충돌 정보 및 체크힙의 출력에 적용됩니다. 이러한 정보는 플래시에 저장되는데, 문제 해결에 충분한 내용이어야 합니다.

예

다음 예에서는 충돌 정보가 콘솔에 출력되지 않게 하는 방법을 보여줍니다.

```
hostname(config)# crashinfo console disable
```

관련 명령

명령	설명
clear configure fips	NVRAM에 저장된 시스템 또는 모듈 FIPS 컨피그레이션 정보를 지웁니다.
fips enable	시스템 또는 모듈에서 FIPS 규정준수를 적용하기 위한 정책 확인을 활성화하거나 비활성화합니다.
fips self-test poweron	POST를 실행합니다.
show crashinfo console	플래시에 대한 충돌 정보 출력을 읽고 쓰고 구성합니다.
show running-config fips	ASA에서 실행 중인 FIPS 컨피그레이션을 표시합니다.

crashinfo force

강제로 ASA에서 충돌이 일어나게 하려면 특별 권한 EXEC 모드에서 **crashinfo force** 명령을 사용합니다.

crashinfo force [**page-fault** | **watchdog**]

구문 설명

page-fault	(선택 사항) 페이지 폴트 때문에 강제로 ASA가 충돌하게 합니다.
watchdog	(선택 사항) watchdogging 때문에 강제로 ASA가 충돌하게 합니다.

기본값

기본적으로 ASA는 충돌 정보 파일을 플래시 메모리에 저장합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

crashinfo force 명령을 사용하여 충돌 출력 생성을 테스트할 수 있습니다. 충돌 출력에서는 일반 충돌을 **crashinfo force page-fault** 또는 **crashinfo force watchdog** 명령이 원인이 충돌과 구분할 방법이 없습니다. 후자 역시 실제 충돌이기 때문입니다. ASA는 크래시 덤프가 완료되면 다시 로드합니다.

주의 운영 환경에서는 **crashinfo force** 명령을 사용하지 마십시오. **crashinfo force** 명령은 ASA에 충돌을 일으키고 강제적으로 다시 로드하게 합니다.

예

다음 예에서는 **crashinfo force page-fault** 명령을 입력할 때 표시되는 경고를 보여줍니다.

```
ciscoasa# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
   Do you wish to proceed? [confirm]:
```

(키보드에서 Return 또는 Enter 키를 눌러) 캐리지 리턴, "Y" 또는 "y"를 입력하면 ASA가 충돌하고 다시 로드됩니다. 이러한 응답 모두 확인으로 해석됩니다. 그 밖의 모든 문자는 아니요로 해석됩니다. 그리고 ASA는 명령줄 프롬프트로 돌아갑니다.

관련 명령

clear crashinfo	충돌 정보 파일의 내용을 지웁니다.
crashinfo save disable	충돌 정보를 플래시 메모리에 기록할 수 없게 합니다.
crashinfo test	ASA에서 플래시 메모리의 파일에 충돌 정보를 저장하는 기능을 테스트합니다.
show crashinfo	충돌 정보 파일의 내용을 표시합니다.

crashinfo save disable

충돌 정보가 플래시 메모리에 기록되지 않게 하려면 글로벌 컨피그레이션 모드에서 **crashinfo save** 명령을 사용합니다. 충돌 정보가 플래시 메모리에 기록되는 것을 허용하고 기본 동작으로 돌아오려면 이 명령의 **no** 형식을 사용합니다.

crashinfo save disable

no crashinfo save disable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본적으로 ASA는 충돌 정보 파일을 플래시 메모리에 저장합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**crashinfo save enable** 명령을 더 이상 사용하지 않습니다. 그 대신 **no crashinfo save disable** 명령을 사용합니다.

사용 지침

충돌 정보는 플래시 메모리와 콘솔의 순으로 기록됩니다.

참고 시작 과정에서 ASA가 충돌할 경우 충돌 정보 파일이 저장되지 않습니다. ASA가 완전히 초기화되고 실행되어야 플래시 메모리에 충돌 정보를 저장할 수 있습니다.

플래시 메모리에 충돌 정보를 저장하는 것을 다시 활성화하려면 **no crashinfo save disable** 명령을 사용합니다.

예

다음 예에서는 충돌 정보가 플래시 메모리에 기록되는 것을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# crashinfo save disable
```

관련 명령

clear crashinfo	충돌 파일의 내용을 지웁니다.
crashinfo force	강제로 ASA가 충돌하게 합니다.
crashinfo test	ASA에서 플래시 메모리의 파일에 충돌 정보를 저장하는 기능을 테스트합니다.
show crashinfo	충돌 파일의 내용을 표시합니다.

crashinfo test

ASA에서 플래시 메모리의 파일에 충돌 정보를 저장하는 기능을 테스트하려면 특별 권한 EXEC 모드에서 **crashinfo test** 명령을 사용합니다.

crashinfo test

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이전의 충돌 정보 파일이 플래시 메모리에 있을 경우 그 파일을 덮어씁니다.

참고 **crashinfo test** 명령을 입력하더라도 ASA가 충돌하지 않습니다.

예

다음 예에서는 충돌 정보 파일 테스트의 출력을 보여줍니다.

```
ciscoasa# crashinfo test
```

관련 명령

clear crashinfo	충돌 파일의 내용을 삭제합니다.
crashinfo force	강제로 ASA가 충돌하게 합니다.
crashinfo save disable	충돌 정보를 플래시 메모리에 기록할 수 없게 합니다.
show crashinfo	충돌 파일의 내용을 표시합니다.

crl

CRL 컨피그레이션 옵션을 지정하려면 crypto ca trustpoint 컨피그레이션 모드에서 **crl** 명령을 사용합니다.

crl {**required** | **optional** | **nocheck**}

구문 설명

nocheck	ASA에서 CRL 검사를 수행하지 않게 합니다.
optional	필수 CRL을 사용할 수 없는 경우에 ASA는 피어 인증서를 계속 받을 수 있습니다.
required	피어 인증서의 유효성 검사를 위해서는 필수 CRL을 사용할 수 있어야 합니다.

기본값

기본값은 **nocheck**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	이 명령을 더 이상 사용하지 않습니다. 다음 형식의 **revocation-check** 명령이 대체합니다. • **revocation-check crl none**이 **crl optional**을 대체합니다. • **revocation-check crl**이 **crl required**를 대체합니다. • **revocation-check none**이 **crl nocheck**을 대체합니다.

예

다음 예에서는 trustpoint central에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작하고 이 신뢰 지점에서 피어 인증서의 유효성 검사를 위해 CRL이 사용 가능할 것을 요구합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl required
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
clear configure crypto ca trustpoint	모든 신뢰 지점을 제거합니다.
crypto ca trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.
crl configure	crl 컨피그레이션 모드를 시작합니다.
url	CRL 검색을 위한 URL을 지정합니다.

crl cache-time

ASA에서 새로 고치기 전에 신뢰 풀 CRL이 CRL 캐시에 머무를 수 있는 기간(분)을 구성하려면 ca-trustpool 컨피그레이션 모드에서 **crl cache-time** 명령을 사용합니다. 기본값인 60분을 적용하려면 이 명령의 **no** 형식을 사용합니다.

crl cache-time

no crl cache-time

구문 설명

cache-time	값의 범위는 1분~1440분입니다.

기본값

기본값은 **60**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ca-trustpool 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 신뢰 지점 컨피그레이션 모드에서 지원되는 이 명령의 버전과 동일합니다.

예

```
ciscoasa(ca-trustpool)# crl cache-time 30
```

관련 명령

명령	설명
crl enforcenextupdate	NextUpdate CRL 필드를 업데이트하는 방법을 지정합니다.

crl configure

CRL 컨피그레이션 모드를 시작하려면 crypto ca trustpoint 컨피그레이션 모드에서 **crl configure** 명령을 사용합니다.

crl configure

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 trustpoint central에 대해 crl 컨피그레이션 모드를 시작합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)#
```

crl enforcenextupdate

NextUpdate CRL 필드를 처리하는 방법을 지정하려면 ca-trustpool 컨피그레이션 모드에서 **crl enforcenextupdate** 명령을 사용합니다. 활성화된 경우 CRL은 아직 경과하지 않은 NextUpdate 필드를 가져야 합니다. 이 제한을 적용하지 않으려면 이 명령의 **no** 형식을 사용합니다.

crl enforcenextupdate

no crl enforcenextupdate

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본값은 enabled입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ca-trustpool 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

활성화된 경우 CRL은 아직 경과하지 않은 NextUpdate 필드를 가져야 합니다. 이 명령은 신뢰 지점 컨피그레이션 모드에서 지원되는 이 명령의 버전과 동일합니다.

관련 명령

명령	설명
crl cache-time	ASA에서 새로 고치기 전에 CRL이 CRL 캐시에 머무를 수 있는 기간을 구성합니다.

9 장

crypto am-disable ~ crypto ipsec ikev1 transform-set mode transport 명령

crypto am-disable

IPsec IKEv1 인바운드 aggressive 모드 연결을 비활성화하려면 글로벌 컨피그레이션 모드에서 **crypto ikev1 am-disable** 명령을 사용합니다. 인바운드 aggressive 모드 연결을 활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev1 am-disable

no crypto ikev1 am-disable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본값은 enabled입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp am-disable** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp am-disable** 명령으로 **isakmp am-disable** 명령을 대체했습니다**.**
8.4(1)	명령 이름을 **crypto isakmp am-disable**에서 **crypto ikev1 am-disable**로 변경했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 인바운드 aggressive 모드 연결을 비활성화합니다.

```
ciscoasa(config)# crypto ikev1 am-disable
```

관련 명령

명령	설명
clear configure crypto isakmp	ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	활성 컨피그레이션을 표시합니다.

crypto ca authenticate

신뢰 지점과 연결된 CA 인증서를 설치하고 인증하려면 글로벌 컨피그레이션 모드에서 **crypto ca authenticate** 명령을 사용합니다. CA 인증서를 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ca authenticate *trustpoint* **[fingerprint** *hexvalue***] [nointeractive]**

no crypto ca authenticate *trustpoint*

구문 설명

fingerprint	ASA에서 CA 인증서를 인증하는 데 사용하는 영숫자로 된 해시 값입니다. 지문이 제공될 경우 ASA는 CA 인증서의 계산된 지문과 비교하고 두 값이 일치할 때만 인증서를 승인합니다. 지문이 없을 경우 ASA는 계산된 지문을 표시하고 인증서를 승인할지 여부를 묻습니다.
hexvalue	지문의 16진수 값을 나타냅니다.
nointeractive	비대화형 모드를 사용하여 이 신뢰 지점에 대한 CA 인증서를 얻습니다. 디바이스 관리자만 사용합니다. 이러한 경우 지문이 없다면 ASA는 묻지 않고 인증서를 승인합니다.
trustpoint	CA 인증서를 얻을 신뢰 지점을 지정합니다. 이름은 최대 128자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

SCEP 등록을 위해 신뢰 지점이 구성된 경우 CA 인증서는 SCEP에서 다운로드합니다. 그렇지 않으면 ASA에서는 base64 형식 CA 인증서를 터미널에 붙여넣으라는 프롬프트를 표시합니다.

이 명령의 호출은 실행 중인 컨피그레이션의 일부가 되지 않습니다.

예

다음 예에서는 ASA가 CA 인증서를 요청하는 것을 보여줍니다. CA가 인증서를 전송하고 ASA는 관리자에게 CA 인증서 지문을 확인하여 CA의 인증서를 검증하라는 프롬프트를 표시합니다. ASA 관리자는 확인된 올바른 값으로 표시된 지문 값을 검증해야 합니다. ASA에서 표시하는 지문이 올바른 값과 매칭할 경우 유효한 인증서로 승인해야 합니다.

```
ciscoasa(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
ciscoasa(config)#
```

다음 예에서는 터미널 기반 (수동) 등록을 위해 구성된 trustpoint tp9을 보여줍니다. ASA에서는 관리자에게 터미널에 CA 인증서를 붙여넣으라는 프롬프트를 표시합니다. 인증서의 지문을 표시한 다음 ASA는 관리자에게 인증서를 보존할 것임을 확인하는 프롬프트를 표시합니다.

```
ciscoasa(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9Ccmlhbnl5NDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ca enroll	CA와의 등록을 시작합니다.
crypto ca import certificate	수동 등록 요청에 대한 응답으로 CA로부터 받은 인증서를 설치합니다.
crypto ca trustpoint	표시된 신뢰 지점에 대한 crypto ca trustpoint 컨피그레이션 모드를 시작합니다.

crypto ca certificate chain

표시된 신뢰 지점에 대해 인증서 체인 컨피그레이션 모드를 시작하려면 글로벌 컨피그레이션 모드에서 **crypto ca certificate chain** 명령을 사용합니다.

crypto ca certificate chain *trustpoint*

구문 설명

trustpoint	인증서 체인을 구성하기 위한 신뢰 지점을 지정합니다.

기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 신뢰 지점 central에 대해 인증서 체인 컨피그레이션 모드를 시작합니다.

```
ciscoasa(config)# crypto ca certificate chain central
ciscoasa(config-cert-chain)#
```

관련 명령

명령	설명
clear configure crypto ca trustpoint	모든 신뢰 지점을 제거합니다.

crypto ca certificate map

인증서 매핑 규칙의 우선 순위 목록을 유지 관리하려면 글로벌 컨피그레이션 모드에서**crypto ca certificate map** 명령을 사용합니다. 암호화 CA 컨피그레이션 맵 규칙을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ca certificate map {*sequence-number* | *map-name sequence-number*}

no crypto ca certificate map {*sequence-number* | *map-name* [*sequence-number*]}

구문 설명

map-name	certificate-to-group 맵의 이름을 지정합니다.
sequence-number	생성하고 있는 인증서 맵 규칙의 번호를 지정합니다. 범위는 1~65535입니다. 터널 그룹 맵을 만들 때 이 번호를 사용할 수 있는데, 터널 그룹을 인증서 맵 규칙에 매핑합니다.

기본값

*map-name*의 기본값은 DefaultCertificateMap입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	*map-name* 옵션을 추가했습니다.

사용 지침

이 명령을 입력하면 ASA는 ca 인증서 맵 컨피그레이션 모드가 되며, 여기서 인증서의 발급자 및 주체 DN(고유 이름)을 기준으로 규칙을 구성할 수 있습니다. 순차 번호에 따라 매핑 규칙의 순서가 정해집니다. 이러한 규칙의 일반적인 형식은 다음과 같습니다.

- *DN match-criteria match-value*
- *DN*은 *주체 이름* 또는 *발급자 이름*. DN은 ITU-T X.509 표준에서 정의합니다.
- *match-criteria*는 다음 표현식 또는 연산자로 구성됩니다.

attr *tag*	CN(공용 이름)과 같은 특정 DN 특성으로 비교를 제한합니다.
co	포함
eq	같음
nc	포함하지 않음
ne	같지 않음

DN 매칭 표현식은 대/소문자를 구분합니다.

예

다음 예에서는 맵 이름 example-map과 순차 번호 1(rule # 1)로 ca 인증서 맵 모드를 시작하며 주체 이름의 CN 특성이 Example1과 일치해야 한다고 지정합니다.

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name attr cn eq Example1
ciscoasa(ca-certificate-map)#
```

다음 예에서는 맵 이름 example-map과 순차 번호 1로 ca 인증서 맵 모드를 시작하며 주체 이름의 내부 어디서든 cisco라는 값을 포함하도록 지정합니다.

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name co cisco
ciscoasa(ca-certificate-map)#
```

관련 명령

명령	설명
issuer-name	IPsec 피어 인증서의 발급자 DN에 규칙 엔트리를 적용하도록 지정합니다.
subject-name (crypto ca certificate map)	IPsec 피어 인증서의 주체 DN에 규칙 엔트리를 적용하도록 지정합니다.
tunnel-group-map enable	**crypto ca certificate map** 명령으로 생성된 인증서 맵 엔트리를 터널 그룹과 연결합니다.

crypto ca crl request

지정된 신뢰 지점의 컨피그레이션 매개변수를 기반으로 CRL을 요청하려면 crypto ca trustpoint 컨피그레이션 모드에서 **crypto ca crl request** 명령을 사용합니다.

crypto ca crl request *trustpoint*

구문 설명

trustpoint	신뢰 지점을 지정합니다. 최대 128자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령의 호출은 실행 중인 컨피그레이션의 일부가 되지 않습니다.

예

다음 예에서는 central이라는 신뢰 지점을 기반으로 CRL을 요청합니다.

```
ciscoasa(config)# crypto ca crl request central
ciscoasa(config)#
```

관련 명령

명령	설명
crl configure	crl 컨피그레이션 모드를 시작합니다.

crypto ca enroll

CA와의 등록 프로세스를 시작하려면 글로벌 컨피그레이션 모드에서 **crypto ca enroll** 명령을 사용합니다.

crypto ca enroll *trustpoint* [**noconfirm**]

구문 설명

noconfirm	(선택 사항) 모든 프롬프트를 억제합니다. 프롬프트에 표시할 등록 옵션은 신뢰 지점에서 미리 구성되어야 합니다. 이 옵션은 스크립트, ASDM 또는 기타 비대화형 용도에 사용합니다.
trustpoint	등록할 신뢰 지점의 이름을 지정합니다. 최대 128자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

SCEP 등록을 위해 신뢰 지점이 구성된 경우 ASA는 즉시 CLI 프롬프트를 표시하며 상태 메시지가 콘솔에 비동기적으로 나타납니다. 수동 등록을 위해 신뢰 지점이 구성된 경우 ASA는 콘솔에 base64 인코딩 PKCS10 인증서 요청을 기록하며 그 다음에 CLI 프롬프트가 나타납니다.

이 명령은 참조된 신뢰 지점의 구성된 상태에 따라 다양한 대화형 프롬프트를 생성합니다. 이 명령이 성공적으로 실행되려면 신뢰 지점이 올바르게 구성되어 있어야 합니다.

예

다음 예에서는 SCEP 등록을 사용하여 신뢰 지점 tp1과의 ID 인증서 등록을 요청합니다. ASA는 신뢰 지점 컨피그레이션에 저장되지 않은 정보를 요청하는 프롬프트를 표시합니다.

```
ciscoasa(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
```

```
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

ciscoasa(config)#
```

다음 예에서는 CA 인증서의 수동 등록을 보여줍니다.

```
ciscoasa(config)# crypto ca enroll tp1

% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ca authenticate	이 신뢰 지점에 대해 CA 인증서를 얻습니다.
crypto ca import pkcs12	수동 등록 요청에 대한 응답으로 CA로부터 받은 인증서를 설치합니다.
crypto ca trustpoint	표시된 신뢰 지점에 대한 crypto ca trustpoint 컨피그레이션 모드를 시작합니다.

crypto ca export

ASA 신뢰 지점 컨피그레이션을 모든 관련 키 및 인증서와 함께 PKCS12 형식으로 내보내거나 디바이스 ID 인증서를 PEM 형식으로 내보내려면 글로벌 컨피그레이션 모드에서 **crypto ca export** 명령을 사용합니다.

crypto ca export *trustpoint* **identity-certificate**

구문 설명

identity-certificate	명명된 신뢰 지점과 관련된 등록된 인증서를 콘솔에 표시하도록 지정합니다.
trustpoint	인증서를 표시할 신뢰 지점의 이름을 지정합니다. 신뢰 지점의 이름은 최대 128자입니다.

기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0(2)	PEM 형식의 인증서 내보내기를 지원하도록 이 명령을 변경했습니다.

사용 지침

이 명령의 호출은 활성 컨피그레이션의 일부가 되지 않습니다. PEM 또는 PKCS12 데이터가 콘솔에 기록됩니다.

웹 브라우저에서는 개인 키와 해당 공개 키 인증서(비밀번호 기반의 대칭형 키로 보호됨)를 저장하는 데 PKCS12 형식을 사용합니다. ASA는 어떤 신뢰 지점과 관련된 인증서와 키를 base64 인코딩 PKCS12 형식으로 내보냅니다. 이 기능은 ASA 간에 인증서와 키를 이동하는 데 사용할 수 있습니다.

인증서의 PEM 인코딩은 PEM 헤더로 묶인 X.509 인증서의 base64 인코딩입니다 . 이 인코딩은 ASA 간의 텍스트 기반 인증서 전송에 일반적으로 사용되는 방식입니다 . PEM 인코딩은 ASA 가 클라이언트의 역할을 할 때 SSL/TLS 프로토콜 프록시를 통해 *proxy-ldc-issuer* 인증서를 내보내는 데 사용할 수 있습니다 .

예

다음 예에서는 신뢰 지점 222에 대해 PEM 형식의 인증서를 콘솔 화면에 내보냅니다.

```
ciscoasa (config)# crypto ca export 222 identity-certificate
```

```
Exported 222 follows:
-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----
ciscoasa (config)#
```

관련 명령

명령	설명
crypto ca authenticate	이 신뢰 지점에 대해 CA 인증서를 얻습니다.
crypto ca enroll	CA와의 등록을 시작합니다.
crypto ca import	수동 등록 요청에 대한 응답으로 CA로부터 받은 인증서를 설치합니다.
crypto ca trustpoint	표시된 신뢰 지점에 대한 crypto ca trustpoint 컨피그레이션 모드를 시작합니다.

crypto ca import

수동 등록 요청에 대한 응답으로 CA에게서 받은 인증서를 설치하거나 어떤 신뢰 지점을 위한 인증서 및 키 쌍을 PKCS12 데이터를 사용하여 가져오려면 글로벌 컨피그레이션 모드에서 **crypto ca import** 명령을 사용합니다.

crypto ca import *trustpoint* **certificate [nointeractive]**

crypto ca import *trustpoint* **pkcs12** *passphrase* **[nointeractive]**

구문 설명

certificate	ASA에 신뢰 지점이 나타내는 CA로부터 인증서를 가져오도록 지시합니다.
nointeractive	(선택 사항) 비대화형 모드를 사용하여 인증서를 가져옵니다. 그러면 어떤 프롬프트도 표시되지 않습니다. 이 옵션은 스크립트, ASDM 또는 기타 비대화형 용도에 사용합니다.
passphrase	PKCS12 데이터의 해독에 사용한 패스프레이즈를 지정합니다.
pkcs12	ASA에 어떤 신뢰 지점을 위한 인증서와 키 쌍을 PKCS12 형식으로 가져오도록 지시합니다.
trustpoint	가져오기 작업을 연결할 신뢰 지점을 지정합니다. 최대 128자입니다. PKCS12 데이터를 가져오는데 신뢰 지점에서 RSA 키를 사용할 경우 가져온 키 쌍에는 신뢰 지점과 동일한 이름이 부여됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 신뢰 지점 Main의 인증서를 수동으로 가져옵니다.

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
ciscoasa (config)#
```

다음 예에서는 수동으로 신뢰 지점 central에 PKCS12 데이터를 가져옵니다.

```
ciscoasa (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
ciscoasa (config)#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 RSA 키 쌍을 저장하기에 충분한 공간이 NVRAM에 없어 경고 메시지를 생성합니다.

```
ciscoasa(config)# crypto ca import central pkcs12 mod 2048
INFO: The name for the keys will be: central
Keypair generation process begin. Please wait...
NV RAM will not have enough space to save keypair central. Remove any unnecessary keypairs
and save the running config before using this keypair.
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ca export	신뢰 지점 인증서와 키 쌍을 PKCS12 형식으로 내보냅니다.
crypto ca authenticate	신뢰 지점에 대해 CA 인증서를 얻습니다.
crypto ca enroll	CA와의 등록을 시작합니다.
crypto ca trustpoint	표시된 신뢰 지점에 대한 crypto ca trustpoint 컨피그레이션 모드를 시작합니다.

crypto ca server

ASA에서 로컬 CA 서버를 설정하고 관리하려면 글로벌 컨피그레이션 모드에서 **crypto ca server** 명령을 사용합니다. 구성된 로컬 CA 서버를 ASA에서 삭제하려면 이 명령의 **no** 형식을 사용합니다.

crypto ca server

no crypto ca server

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

ASA에서 CA 서버가 활성화되어 있지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

각 ASA에는 로컬 CA가 하나만 가능합니다.

crypto ca server 명령에서 CA 서버를 구성하지만, 서버를 활성화하지는 않습니다. 로컬 CA를 활성화하려면 ca 서버 컨피그레이션 모드에서 **shutdown** 명령의 **no** 형식을 사용합니다.

no shutdown 명령으로 CA 서버를 활성화할 때 자체 서명 인증서를 저장하기 위해 CA와 LOCAL-CA-SERVER라는 신뢰 지점의 RSA 키 쌍을 설정합니다. 새로 생성된 이 자체 서명 인증서는 항상 디지털 서명, CRL 서명, 인증서 서명 키 사용법이 설정되어 있습니다.

주의 **no crypto ca server** 명령은 구성된 로컬 CA 서버, 그 RSA 키 쌍, 관련 신뢰 지점을 로컬 CA 서버의 현재 상태에 관계없이 삭제합니다.

예

다음 예에서는 ca 서버 컨피그레이션 모드를 시작한 다음 이 모드에서 사용 가능한 로컬 CA 서버 명령을 나열합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# ?

CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
                        certificates
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

다음 예에서는 구성되고 활성화된 CA 서버를 ASA에서 삭제하기 위해 ca 서버 컨피그레이션 모드에서 **crypto ca server** 명령의 **no** 형식을 사용합니다.

```
ciscoasa(config-ca-server)# no crypto ca server

Certificate server 'remove server' event has been queued for processing.
ciscoasa(config)#
```

관련 명령

명령	설명
debug crypto ca server	로컬 CA 서버를 구성할 때 디버깅 메시지를 표시합니다.
show crypto ca server	구성된 CA 서버의 상태 및 매개변수를 표시합니다.
show crypto ca server cert-db	로컬 CA 서버 인증서를 표시합니다.

crypto ca server crl issue

CRL(인증서 취소 목록)을 강제로 실행하려면 특별 권한 EXEC 모드에서 **crypto ca server crl issue** 명령을 사용합니다.

crypto ca server crl issue

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

분실한 CRL을 복구할 때 이 명령을 사용합니다. 일반적으로 CRL은 만료 시 기존 CRL을 다시 서명하는 방식으로 자동 재발급됩니다. **crypto ca server crl issue** 명령은 인증서 데이터베이스를 기반으로 CRL을 다시 생성합니다. 인증서 데이터베이스의 내용을 토대로 CRL을 다시 생성하는 데 필요한 경우에만 사용해야 합니다.

예

다음 예에서는 강제로 로컬 CA 서버에서 CRL을 실행하게 합니다.

```
ciscoasa(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
cdp-url	CA 발급 인증서에 포함할 인증서 취소 목록 배포 지점을 지정합니다.
crypto ca server	ca 서버 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다. 그러면 로컬 CA를 구성하고 관리할 수 있습니다.
crypto ca server revoke	로컬 CA 서버가 발급한 인증서를 인증서 데이터베이스 및 CRL에서 폐기된 것으로 표시합니다.
show crypto ca server crl	로컬 CA의 현재 CRL을 표시합니다.

crypto ca server revoke

로컬 CA 서버에서 발급한 인증서를 인증서 데이터베이스 및 CRL에서 폐기됨으로 표시하려면 특별 권한 EXEC 모드에서 **crypto ca server revoke** 명령을 사용합니다.

crypto ca server revoke *cert-serial-no*

구문 설명

cert-serial-no	폐기할 인증서의 일련 번호를 지정합니다. 이는 16진수 형식이어야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ASA에서 로컬 CA가 발급한 특정 인증서를 폐기하려면 해당 ASA에서 **crypto ca server revoke** 명령을 입력합니다. 이 명령에 의해 인증서가 CA 서버의 인증서 데이터베이스 및 CRL에 폐기됨으로 표시되면 폐기가 완료된 것입니다. 인증서 일련 번호를 16진수 형식으로 입력하여 폐기할 인증서를 지정할 수 있습니다.

지정된 인증서가 폐기된 후 CRL은 자동으로 다시 생성됩니다.

예

다음 예에서는 로컬 CA 서버에서 발급했고 일련 번호가 782ea09f인 인증서를 폐기합니다.

```
ciscoasa(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked. A new CRL has been issued.
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server crl issue	강제적으로 CRL을 발행합니다.
crypto ca server unrevoke	로컬 CA 서버에서 발급했고 이미 폐기된 인증서를 폐기 해제합니다.
crypto ca server user-db remove	CA 서버 사용자 데이터베이스에서 사용자를 삭제합니다.
show crypto ca server crl	로컬 CA의 현재 CRL을 표시합니다.
show crypto ca server user-db	CA 서버 사용자 데이터베이스에 포함된 사용자를 표시합니다.

crypto ca server unrevoke

로컬 CA 서버에서 발급했고 이미 폐기된 인증서를 폐기 해제하려면 특별 권한 EXEC 모드에서 **crypto ca server unrevoke** 명령을 사용합니다.

crypto ca server unrevoke *cert-serial-no*

구문 설명

cert-serial-no	폐기 해제할 인증서의 일련 번호를 지정합니다. 이는 16진수 형식이어야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ASA에서 로컬 CA가 발급했고 이미 폐기된 인증서를 폐기 해제하려면 **crypto ca server unrevoke** 명령을 입력합니다. 이 명령이 실행되어 해당 인증서가 인증서 데이터베이스에서 유효한 것으로 표시되고 CRL에서 삭제되면 인증서의 효력이 복원됩니다. 인증서 일련 번호를 16진수 형식으로 입력하여 폐기 해제할 인증서를 지정할 수 있습니다.

지정된 인증서가 폐기 해제된 후 CRL은 자동으로 다시 생성됩니다.

예

다음 예에서는 로컬 CA 서버에서 발급했고 일련 번호가 782ea09f인 인증서를 폐기 해제합니다.

```
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked. A new CRL has been
issued.

ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	ca 서버 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다. 그러면 로컬 CA를 구성하고 관리할 수 있습니다.
crypto ca server crl issue	강제적으로 CRL을 발행합니다.
crypto ca server revoke	로컬 CA 서버가 발급한 인증서를 인증서 데이터베이스 및 CRL에서 폐기된 것으로 표시합니다.
crypto ca server user-db add	CA 서버 사용자 데이터베이스에 사용자를 추가합니다.
show crypto ca server cert-db	로컬 CA 서버 인증서를 표시합니다.
show crypto ca server user-db	CA 서버 사용자 데이터베이스에 포함된 사용자를 표시합니다.

crypto ca server user-db add

CA 서버 사용자 데이터베이스에 새 사용자를 삽입하려면 특별 권한 EXEC 모드에서 **crypto ca server user-db add** 명령을 사용합니다.

crypto ca server user-db add *user* **[dn** *dn***] [email** *e-mail-address***]**

구문 설명

dn *dn*	추가된 사용자에게 발급되는 인증서를 위해 주체 이름 DN을 지정합니다. DN 문자열에 공백이 포함될 경우 큰 따옴표로 그 값을 묶습니다. 쉼표는 DN 특성을 구분하는 용도로만 사용할 수 있습니다(예: OU=Service, O=Company, Inc.").
email *e-mail-address*	새 사용자의 이메일 주소를 지정합니다.
user	등록 권한을 부여할 단일 사용자를 지정합니다. 사용자 이름은 간단한 사용자 이름 또는 이메일 주소일 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

user argument는 user1과 같은 단순한 사용자 이름 또는 ser1@example.com과 같은 이메일 주소가 가능합니다. *username*은 최종 사용자가 등록 페이지에서 지정한 사용자 이름과 일치해야 합니다.

*username*은 권한 없는 사용자로 데이터베이스에 추가됩니다. 등록 권한을 부여하려면 **crypto ca server allow** 명령을 사용해야 합니다.

username 인수는 *OTP(1*회용 비밀번호)와 함께 등록 인터페이스 페이지에서 사용자를 등록하는 데 사용됩니다.

참고 OTP를 이메일로 알릴 경우 *username* 또는 *email-address* 인수 중 하나에 이메일 주소를 지정해야 합니다. 메일 발송 시 이메일 주소가 없으면 오류가 생성됩니다.

email *e-mail-address* 키워드-인수 쌍은 사용자에게 등록 및 갱신 알림을 전달할 때 이메일 주소로만 사용되며, 발급된 인증서에는 나타나지 않습니다.

이 이메일 주소를 포함하면 의문 사항이 있을 때 사용자에게 연락하고 등록에 필요한 OTP를 전달할 수 있습니다.

어떤 사용자에 대해 선택 사항인 DN이 지정되지 않을 경우 주체 이름 DN은 *username*과 주체 이름 기본 DN 설정을 사용하여 cn=*username*, subject-name-default의 형태로 구성됩니다.

예

다음 예에서는 사용자 이름이 user1@example.com이고 온전한 주체 이름 DN을 갖는 사용자를 사용자 데이터베이스에 추가합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db add dn "cn=Jane Doe, ou=engineering,
o=Example, l=RTP, st=NC, c=US"
ciscoasa(config-ca-server)#
```

다음 예에서는 user2라는 사용자에게 등록 권한을 부여합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user2
ciscoasa(config-ca-server)
```

관련 명령

명령	설명
crypto ca server	ca 서버 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다. 그러면 로컬 CA를 구성하고 관리할 수 있습니다.
crypto ca server user-db allow	CA 서버 데이터베이스의 특정 사용자 또는 일부 사용자가 CA에 등록하는 것을 허용합니다.
crypto ca server user-db remove	CA 서버 데이터베이스에서 사용자를 삭제합니다.
crypto ca server user-db write	CA 서버 데이터베이스의 사용자 정보를 **database path** 명령에 의해 지정되는 파일에 복사합니다.
database path	로컬 CA 데이터베이스의 경로 또는 위치를 지정합니다. 기본 위치는 플래시 메모리입니다.

crypto ca server user-db allow

어떤 사용자 또는 사용자 그룹이 로컬 CA 서버 데이터베이스에 등록하는 것을 허용하려면 특별 권한 EXEC 모드에서 **crypto ca server user-db allow** 명령을 사용합니다. 이 명령은 일회용 비밀번호를 생성하여 표시하거나 사용자에게 이메일로 발송하는 옵션도 있습니다.

crypto ca server user-db allow {*username* | **all-unenrolled** | **all-certholders**} **[display-otp] [email-otp] [replace-otp]**

구문 설명

all-certholders	인증서의 유효성 여부에 관계없이 인증서를 발급받았고 데이터베이스에 포함된 모든 사용자에게 등록 권한을 부여하도록 지정합니다. 이는 갱신 권한을 부여하는 것과 같습니다.
all-unenrolled	인증서를 발급받지 않았고 데이터베이스에 포함된 모든 사용자에게 등록 권한을 부여하도록 지정합니다.
email-otp	(선택 사항) 지정된 사용자에게 구성된 이메일 주소로 일회용 비밀번호를 보냅니다.
replace-otp	(선택 사항) 원래 유효한 일회용 비밀번호가 있었던 지정된 모든 사용자에게 일회용 비밀번호를 다시 생성하도록 지정합니다.
display-otp	(선택 사항) 지정된 모든 사용자의 일회용 비밀번호를 콘솔에 표시합니다.
username	등록 권한을 부여할 단일 사용자를 지정합니다. 사용자 이름은 간단한 사용자 이름 또는 이메일 주소일 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

replace-otp 키워드는 지정된 모든 사용자에게 OTP를 생성합니다. 이 새 OTP가 지정된 사용자에게 생성되었던 유효한 OTP를 대체합니다.

OTP는 ASA에 저장되지 않지만, 등록 과정에서 사용자에게 통지하거나 사용자를 인증하는 데 필요할 때 생성되고 다시 생성됩니다.

예

다음 예에서는 데이터베이스에 있고 아직 등록하지 않은 모든 사용자에게 등록 권한을 부여합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db allow all-unenrolled
ciscoasa(config-ca-server)#
```

다음 예에서는 user1라는 사용자에게 등록 권한을 부여합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user1
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	ca 서버 컨피그레이션 모드 명령 집합에 대한 액세스를 제공합니다. 그러면 로컬 CA를 구성하고 관리할 수 있습니다.
crypto ca server user-db add	CA 서버 사용자 데이터베이스에 사용자를 추가합니다.
crypto ca server user-db write	CA 서버 데이터베이스의 사용자 정보를 **database path** 명령에 의해 지정되는 파일에 복사합니다.
enrollment-retrieval	등록된 사용자가 PKCS12 등록 파일을 검색할 수 있는 기간(시간)을 지정합니다.
show crypto ca server cert-db	로컬 CA에서 발급한 모든 인증서를 표시합니다.

crypto ca server user-db email-otp

로컬 CA 서버 데이터베이스에서 특정 사용자 또는 일부 사용자에게 이메일로 OTP를 보내려면 특별 권한 EXEC 모드에서 **crypto ca server user-db email-otp** 명령을 사용합니다.

crypto ca server user-db email-otp {*username* | **all-unenrolled** | **all-certholders**}

구문 설명

all-certholders	인증서의 유효성 여부에 관계없이 인증서를 발급받았고 데이터베이스에 포함된 모든 사용자에게 이메일로 OTP를 보내도록 지정합니다.
all-unenrolled	데이터베이스에 있고 인증서를 발급받은 적이 없거나 만료된 또는 폐기된 인증서만 있는 모든 사용자에게 이메일로 OTP를 보내도록 지정합니다.
username	단일 사용자에게 이메일로 OTP를 보내도록 지정합니다. 사용자 이름은 사용자 이름 또는 이메일 주소일 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

예

다음 예에서는 데이터베이스에 있는 모든 미등록 사용자에게 이메일로 OTP를 보냅니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp all-unenrolled
ciscoasa(config-ca-server)#
```

다음 예에서는 user1이라는 사용자에게 이메일로 OTP를 보냅니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp user1
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server user-db show-otp	CA 서버 데이터베이스에 있는 특정 사용자 또는 일부 사용자의 일회용 비밀번호를 표시합니다.
show crypto ca server cert-db	로컬 CA에서 발급한 모든 인증서를 표시합니다.
show crypto ca server user-db	CA 서버 사용자 데이터베이스에 포함된 사용자를 표시합니다.

crypto ca server user-db remove

로컬 CA 서버 사용자 데이터베이스에서 어떤 사용자를 삭제하려면 특별 권한 EXEC 모드에서 **crypto ca server user-db remove** 명령을 사용합니다.

crypto ca server user-db remove *username*

구문 설명

username	삭제할 사용자의 이름을 사용자 이름 또는 이메일 주소의 형식으로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 CA 사용자 데이터베이스에서 사용자 이름을 삭제하여 사용자가 등록할 수 없게 합니다. 이미 발급된 유효한 인증서를 폐기하는 옵션도 제공합니다.

예

다음 예에서는 user1이라는 사용자 이름을 CA 서버 사용자 데이터베이스에서 삭제합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db remove user1

WARNING: No certificates have been automatically revoked. Certificates issued to user
user1 should be revoked if necessary.

ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server crl issue	강제적으로 CRL을 발행합니다.
crypto ca server revoke	로컬 CA 서버가 발급한 인증서를 인증서 데이터베이스 및 CRL에서 폐기된 것으로 표시합니다.
show crypto ca server user-db	CA 서버 사용자 데이터베이스에 포함된 사용자를 표시합니다.
crypto ca server user-db write	로컬 CA 서버 데이터베이스에 구성된 사용자 정보를 **database path** 명령에 의해 지정되는 파일에 기록합니다.

crypto ca server user-db show-otp

로컬 CA 서버 데이터베이스에서 특정 사용자 또는 일부 사용자의 OTP를 표시하려면 특별 권한 EXEC 모드에서 **crypto ca server user-db show-otp** 명령을 사용합니다.

crypto ca server user-db show-otp {*username* **| all-certholders | all-unenrolled}**

구문 설명

all-certholders	인증서의 현재 유효성 여부에 관계없이 데이터베이스에 있고 인증서를 발급받은 모든 사용자의 OTP를 표시합니다.
all-unenrolled	데이터베이스에 있고 인증서를 발급받은 적이 없거나 만료된 또는 폐기된 인증서만 있는 모든 사용자의 OTP를 표시합니다.
username	단일 사용자의 OTP를 표시하도록 지정합니다. *username*은 사용자 이름 또는 이메일 주소일 수 있습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

예

다음 예에서는 유효하거나 유효하지 않은 인증서를 보유한, 데이터베이스에 있는 모든 사용자에 대해 OTP를 표시합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp all-certholders
ciscoasa(config-ca-server)#
```

다음 예에서는 user1이라는 사용자의 OTP를 표시합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp user1
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server user-db add	CA 서버 사용자 데이터베이스에 사용자를 추가합니다.
crypto ca server user-db allow	CA 서버 데이터베이스의 특정 사용자 또는 일부 사용자가 로컬 CA에 등록하는 것을 허용합니다.
crypto ca server user-db email-otp	CA 서버 데이터베이스에 있는 특정 사용자 또는 일부 사용자에게 이메일로 일회용 비밀번호를 보냅니다.
show crypto ca server cert-db	로컬 CA에서 발급한 모든 인증서를 표시합니다.

crypto ca server user-db write

모든 로컬 CA 데이터베이스 파일을 저장하기 위해 디렉토리 위치를 구성하려면 특별 권한 EXEC 모드에서 **crypto ca server user-db write** 명령을 사용합니다.

crypto ca server user-db write

구문 설명

이 명령은 키워드 또는 인수가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—
글로벌 컨피그레이션	• 예	—	• 예	—	—
특별 권한 EXEC	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

crypto ca server user-db write 명령은 데이터베이스 경로 컨피그레이션에 의해 지정된 저장소에 새 사용자 기반 컨피그레이션 데이터를 저장하는 데 사용합니다. 이 정보는 **crypto ca server user-db add** 또는 **crypto ca server user-db allow** 명령으로 신규 사용자를 추가하거나 허용할 때 생성됩니다.

예

다음 예에서는 로컬 CA 데이터베이스에 구성된 사용자 정보를 스토리지에 기록합니다.

```
ciscoasa(config-ca-server)# crypto ca server user-db write
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server user-db add	CA 서버 사용자 데이터베이스에 사용자를 추가합니다.
database path	로컬 CA 데이터베이스의 경로 또는 위치를 지정합니다. 기본 위치는 플래시 메모리입니다.
crypto ca server user-db remove	CA 서버 사용자 데이터베이스에서 사용자를 삭제합니다.
show crypto ca server cert-db	로컬 CA에서 발급한 모든 인증서를 표시합니다.
show crypto ca server user-db	CA 서버 사용자 데이터베이스에 포함된 사용자를 표시합니다.

crypto ca trustpoint

지정된 신뢰 지점에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작하려면 글로벌 컨피그레이션 모드에서 **crypto ca trustpoint** 명령을 사용합니다. 지정된 신뢰 지점을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* **[noconfirm]**

구문 설명

noconfirm	모든 대화형 프롬프트를 억제합니다.
ipsec	이 신뢰 지점을 사용하여 IPsec 클라이언트 연결의 유효성을 검사할 수 있음을 나타냅니다.
ssl-client	이 신뢰 지점을 사용하여 SSL 클라이언트 연결의 유효성을 검사할 수 있음을 나타냅니다.
trustpoint-name	관리할 신뢰 지점의 이름을 나타냅니다. 이름은 최대 128자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	OCSP 지원 옵션을 추가했습니다. 여기에는 **match certificate map**, **ocsp disable-nonce**, **ocsp url**, **revocation-check**이 포함됩니다.
8.0(2)	인증서 유효성 검사 지원 옵션을 추가했습니다. 여기에는 **id-usage** 및 **validation-policy** 가 포함됩니다.더 이상 **accept-subordinates, id-cert-issuer**, **support-user-cert-validation**을 사용하지 않습니다.
8.0(4)	신뢰할 수 있는 기업 간, 이를테면 전화 프록시와 TLX 프록시 간 자체 서명 인증서의 등록을 지원하기 위해 **enrollment self** 옵션을 추가했습니다.

사용 지침

crypto ca trustpoint 명령을 사용하여 CA를 선언합니다. 이 명령을 실행하면 crypto ca trustpoint 컨피그레이션 모드가 됩니다.

이 명령으로 신뢰 지점 정보를 관리합니다. 신뢰 지점은 CA에서 발급한 인증서에 따라 CA ID 그리고 디바이스 ID가 될 수도 있습니다. 신뢰 지점 모드의 명령은 CA 관련 컨피그레이션 매개변수를 제어합니다. 이 매개변수는 ASA에서 CA 인증서를 받는 방법, ASA가 CA로부터 자신의 인증서를 받는 방법, CA에서 발급한 사용자 인증서에 대한 인증 정책을 지정합니다.

다음 명령을 사용하여 신뢰 지점에 대한 특성을 지정할 수 있습니다.

- **accept-subordinates**—더 이상 사용하지 않습니다. 신뢰 지점 관련 CA에 종속된 CA 인증서가 ASA에 설치된 적이 없는 상태에서 1단계 IKE 교환 중에 제공된 경우 이 인증서를 승인할지 여부를 나타냅니다.
- **crl required | optional | nocheck**—CRL 컨피그레이션 옵션을 지정합니다.
- **crl configure**—CRL 컨피그레이션 모드를 시작합니다(**crl** 명령 참조).
- **default enrollment**—모든 등록 매개변수를 시스템 기본값으로 되돌립니다. 이 명령의 호출은 활성 컨피그레이션의 일부가 되지 않습니다.
- **email** *address*—등록 과정에서 CA에게 지정된 이메일 주소를 인증서의 SAN(Subject Alternative Name) 확장에 포함하도록 요청합니다.
- **enrollment retry period** —SCEP 등록의 재시도 기간(분)을 지정합니다.
- **enrollment retry count**—SCEP 등록을 재시도할 수 있는 최대 횟수를 지정합니다.
- **enrollment terminal**—이 신뢰 지점과의 등록을 잘라서 붙여넣도록 지정합니다.
- **enrollment self**—자체 서명 인증서를 생성하는 등록을 지정합니다.
- **enrollment url** *url*—이 신뢰 지점과 등록하는 데 SCEP 등록을 지정하고 등록 URL(*url*)을 구성합니다.
- **exit**—컨피그레이션 모드를 종료합니다.
- **fqdn** *fqdn*—등록 과정에서 CA에게 지정된 FQDN을 인증서의 SAN 확장에 포함하도록 요청합니다.
- **id-cert-issuer**—더 이상 사용하지 않습니다. 이 신뢰 지점과 관련된 CA에서 발급한 피어 인증서를 승인할지 여부를 나타냅니다.
- **id-usage**— 신뢰 지점의 등록된 ID를 어떻게 사용할 수 있는지 지정합니다.
- **ip-addr** *ip-address*—등록 과정에서 CA에게 ASA의 IP 주소를 인증서에 포함하도록 요청합니다.
- **keypair** *name*—공개 키를 인증할 키 쌍을 지정합니다.
- **match certificate** *map-name* **override ocsp**—인증서 맵을 OCSP 재정의 규칙에 매칭합니다.
- **ocsp disable-nonce**—암호 기술을 사용하여 폐기 요청과 응답을 바인딩함으로써 반복 공격을 방지하는 nonce 확장을 비활성화합니다.
- **ocsp url**—이 URL의 OCSP 서버가 이 신뢰 지점과 관련된 모든 인증서를 검사하여 폐기 상태를 확인하도록 지정합니다.
- **exit**—컨피그레이션 모드를 종료합니다.
- **password** *string*—등록 과정에서 CA에 등록되는 챌린지 구문(challenge phrase)을 지정합니다. 일반적으로 CA는 후속 폐기(revocation) 요청을 인증하는 데 이 구문을 사용합니다.
- **revocation check**—폐기 검사 방식(예: CRL, OCSP, none)을 지정합니다.
- **serial-number**—등록 과정에서 CA에게 ASA 일련 번호를 인증서에 포함하도록 요청합니다.

- **subject-name** *X.500 name*—등록 과정에서 CA에게 지정된 주체 DN을 인증서에 포함하도록 요청합니다. DN 문자열에 쉼표가 있을 경우 큰따옴표로 값 문자열을 묶습니다(예: O="Company, Inc.").
- **support-user-cert-validation**—더 이상 사용하지 않습니다. 활성화된 경우 원격 사용자 인증서의 유효성을 검사하기 위한 컨피그레이션 설정을 이 신뢰 지점에서 가져올 수 있습니다. 단, 원격 인증서를 발급한 CA에 인증한 것이어야 합니다. 이 옵션은 하위 명령 **crl required | optional | nocheck**와 관련된 컨피그레이션 데이터 및 CRL 모드의 모든 설정에 적용됩니다.
- **validation-policy**—사용자 연결과 관련된 인증서의 유효성 검사를 위해 신뢰 지점 조건을 지정합니다.

참고 연결을 시도할 때 신뢰 지점에서 ID 인증서를 검색하려 하면 신뢰 지점에 ID 인증서가 없다는 경고가 표시됩니다.

예

다음 예에서는 central이라는 신뢰 지점을 관리하기 위해 ca 신뢰 지점 컨피그레이션 모드를 시작합니다.

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

관련 명령

명령	설명
clear configure crypto ca trustpoint	모든 신뢰 지점을 제거합니다.
crypto ca authenticate	이 신뢰 지점에 대해 CA 인증서를 얻습니다.
crypto ca certificate map	crypto ca certificate map 컨피그레이션 모드를 시작합니다. 인증서 기반 ACL을 정의합니다.
crypto ca crl request	지정된 신뢰 지점의 컨피그레이션 매개변수를 기반으로 CRL을 요청합니다.
crypto ca import	수동 등록 요청에 대한 응답으로 CA로부터 받은 인증서를 설치합니다.

crypto ca trustpool export

PKI 신뢰 풀을 구성하는 인증서를 내보내려면 특별 권한 EXEC 컨피그레이션 모드에서 **crypto ca trustpool export** 명령을 사용합니다.

crypto ca trustpool export *filename*

구문 설명

filename	내보낸 신뢰 풀 인증서를 저장할 파일

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 활성 신뢰 풀의 전체 내용을 지정된 파일 경로에 PEM 코딩 형식으로 복사합니다.

예

```
ciscoasa# crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
ciscoasa#
ciscoasa# more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE

<More>
```

관련 명령

명령	설명
crypto ca trustpool import	PKI 신뢰 풀을 구성하는 인증서를 가져옵니다.

crypto ca trustpool import

PKI 신뢰 풀을 구성하는 인증서를 가져오려면 글로벌 컨피그레이션 모드에서 **crypto ca trustpool import** 명령을 사용합니다.

crypto ca trustpool import [clean] url *url* [**noconfirm** [**signature-required**]]

crypto ca trustpool import [clean] default [noconfirm]

구문 설명

clean	가져오기 전에 다운로드한 모든 신뢰 풀 인증서를 제거합니다.
default	신뢰받는 ASA의 기본 CA 목록을 복원합니다.
noconfirm	모든 대화형 프롬프트를 억제합니다.
signature-required	서명된 파일만 허용하도록 지정합니다.
url	가져올 신뢰 풀 파일의 위치.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 신뢰 풀 번들을 cisco.com에서 다운로드할 때 파일에 있는 서명의 유효성을 검사하는 기능을 제공합니다. 다른 소스의 번들 또는 서명을 지원하지 않는 형식의 번들을 다운로드할 때는 유효한 서명이 꼭 필요하지는 않습니다. 사용자는 서명의 상태를 알 수 있으며 번들을 승인하거나 거부하는 옵션이 주어집니다.

다음과 같은 대화형 경고가 나타날 수 있습니다.

- 유효하지 않은 서명의 Cisco 번들 형식
- 타사 번들 형식
- 유효한 서명의 Cisco 번들 형식

signature-required 키워드는 **noconfirm** 옵션을 선택한 경우에만 허용됩니다. **signature-required** 키워드가 포함되었지만 서명이 없거나 검증할 수 없을 경우 가져오기는 실패합니다.

참고 다른 방법으로 파일의 적법성을 입증하지 않는 한 파일 서명을 검증할 수 없다면 인증서를 설치하지 마십시오 .

다음 예에서는 대화형 프롬프트를 억제하고 서명을 필요로 하는 경우에 **crypto ca trustpool** import 명령의 동작을 보여줍니다.

```
ciscoasa(config)# crypto ca trustpool import url ?

configure mode commands/options:
disk0:   Import from disk0: file system
disk1:   Import from disk1: file system
flash:   Import from flash: file system
ftp:     Import from ftp: file system
http:    Import from http: file system
https:   Import from https: file system
smb:     Import from smb: file system
system:  Import from system: file system
tftp:    Import from tftp: file system

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com ?
exec mode commands/options:
noconfirm  Specify this keyword to suppress all interactive prompting.

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com  noconfirm ?
exec mode commands/options:
signature-required  Indicate that only signed files will be accepted
```

관련 명령

명령	설명
crypto ca trustpool export	PKI 신뢰 풀을 구성하는 인증서를 내보냅니다.

crypto ca trustpool policy

신뢰 풀 정책을 정의하는 명령을 제공하는 하위 모드를 시작하려면 글로벌 컨피그레이션 모드에서 **crypto ca trustpool policy** 명령을 사용합니다.

crypto ca trustpool policy

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

예

```
ciscoasa(config)# crypto ca trustpool ?

configure mode commands/options:
policy Define trustpool policy

ciscoasa(config)# crypto ca trustpool policy
ciscoasa(config-ca-trustpool)# ?

CA Trustpool configuration commands:
crl               CRL options
exit              Exit from certificate authority trustpool entry mode
match             Match a certificate map
no                Negate a command or set its defaults
revocation-check  Revocation checking options
ciscoasa(config-ca-trustpool)#
```

관련 명령

명령	설명
show crypto ca trustpool policy	구성된 신뢰 풀 정책을 표시합니다.

crypto ca trustpool remove

PKI 신뢰 풀에서 지정된 단일 인증서를 제거하려면 특별 권한 EXEC 컨피그레이션 모드에서 **crypto ca trustpool remove** 명령을 사용합니다.

crypto ca trustpool remove *cert fingerprint* **[noconfirm]**

구문 설명

cert fingerprint	Hex data.
noconfirm	모든 대화형 프롬프트를 억제하려면 이 키워드를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 신뢰할 수 있는 루트 인증서 콘텐츠에 대한 변경 사항을 커밋하므로 대화형 사용자는 작업을 확인하는 프롬프트가 표시됩니다.

예

```
ciscoasa# crypto ca trustpool remove ?

  Hex-data  Certificate fingerprint
ciscoasa# crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0 ?
noconfirm  Specify this keyword to suppress all interactive prompting.
```

관련 명령

명령	설명
clear crypto ca trustpool	신뢰 풀에서 모든 인증서를 제거합니다.
crypto ca trustpool export	PKI 신뢰 풀을 구성하는 인증서를 내보냅니다.
crypto ca trustpool import	PKI 신뢰 풀을 구성하는 인증서를 가져옵니다.

crypto dynamic-map match address

동적 암호화 맵 엔트리에 대한 액세스 목록 주소를 매칭하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map match address** 명령을 사용합니다. 주소 매칭을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

구문 설명

acl-name	동적 암호화 맵 엔트리에 대해 매칭할 액세스 목록을 나타냅니다.
dynamic-map-name	동적 암호화 맵 세트의 이름을 지정합니다.
dynamic-seq-num	동적 암호화 맵 엔트리에 해당하는 순차 번호를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령에 대한 자세한 내용은 **crypto map match address** 명령을 참조하십시오.

예

다음 예에서는 aclist1이라는 액세스 목록의 주소와 매칭하기 위해 **crypto dynamic-map** 명령을 사용하는 것을 보여줍니다.

```
ciscoasa(config)# crypto dynamic-map mymap 10 match address aclist1
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 표시합니다.

crypto dynamic-map set df-bit

SA(서명 알고리즘)별 DF(do-not-fragment) 정책을 설정하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set df-bit** 명령을 사용합니다. DF 정책을 비활성화하려면 이 명령의 the **no** 형식을 사용합니다.

crypto dynamic-map *name priority* **set df-bit [clear-df | copy-df | set-df]**

no crypto dynamic-map *name priority* **set df-bit [clear-df | copy-df | set-df]**

구문 설명

name	동적 암호화 맵 세트의 이름을 지정합니다.
priority	동적 암호화 맵 엔트리에 부여하는 우선순위를 지정합니다.

기본값

기본 설정은 off입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

원래의 DF 정책 명령은 유지되며 인터페이스에서 전역 정책 설정의 역할을 하지만, 이는 SA에서 **crypto map** 명령에 의해 대체됩니다.

crypto dynamic-map set nat-t-disable

이 암호화 맵 엔트리 기반의 연결에 NAT-T를 비활성화하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set nat-t-disable** 명령을 사용합니다. 이 암호화 맵 엔트리에 대해 NAT-T를 활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

구문 설명

dynamic-map-name	동적 암호화 맵 세트의 이름을 지정합니다.
dynamic-seq-num	동적 암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

기본 설정은 off입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

전역에서 NAT-T를 활성화하려면 **isakmp nat-traversal** 명령을 사용합니다. 그런 다음 **crypto dynamic-map set nat-t-disable** 명령을 사용하여 특정 암호화 맵 엔트리에서 NAT-T를 비활성화할 수 있습니다.

예

다음 명령은 mymap이라는 동적 암호화 맵에 대해 NAT-T를 비활성화합니다.

```
ciscoasa(config)# crypto dynamic-map mymap 10 set nat-t-disable
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 표시합니다.

crypto dynamic-map set peer

이 명령에 대한 자세한 내용은 **crypto map set peer** 명령을 참조하십시오.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

구문 설명

dynamic-map-name	동적 암호화 맵 세트의 이름을 지정합니다.
dynamic-seq-num	동적 암호화 맵 엔트리에 해당하는 순차 번호를 지정합니다.
hostname	동적 암호화 맵 엔트리의 피어를 **name** 명령에 의해 정의된 호스트 이름을 통해 식별합니다.
ip_address	동적 암호화 맵 엔트리의 피어를 **name** 명령에 의해 정의된 IP 주소를 통해 식별합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 예에서는 mymap이라는 동적 맵의 피어를 IP 주소 10.0.0.1로 설정하는 것을 보여줍니다.

```
ciscoasa(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 표시합니다.

crypto dynamic-map set pfs

동적 암호화 맵 세트를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map dynamic-map set pfs** 명령을 사용합니다. 지정된 동적 맵 암호화 맵 세트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

이 명령에 대한 자세한 내용은 **crypto map set pfs** 명령을 참조하십시오.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

구문 설명

dynamic-map-name	동적 암호화 맵 세트의 이름을 지정합니다.
dynamic-seq-num	동적 암호화 맵 엔트리에 해당하는 순차 번호를 지정합니다.
group1	IPsec에서 새 DH 교환을 수행할 때 768비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group2	IPsec에서 새 DH 교환을 수행할 때 1024비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group5	IPsec에서 새 DH 교환을 수행할 때 1536비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
set pfs	이 동적 암호화 맵 엔트리에 대한 새 보안 연결을 요청할 때 PFS(perfect forward secrecy)를 요구하도록 IPsec을 구성하거나 새 보안 연결에 대한 요청을 수신할 때 PFS를 요구하도록 IPsec을 구성합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	DH 그룹 7을 추가하기 위해 이 명령을 수정했습니다.
8.0(4)	**group 7** 명령 옵션은 더 이상 사용되지 않습니다. 그룹 7을 구성하려고 시도하면 오류 메시지가 생성되고 그룹 5가 대신 사용됩니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

crypto dynamic-map 명령(**match address**, **set peer**, **set pfs** 등)을 **crypto map** 명령과 함께 설명합니다. 피어가 협상을 시작하고 로컬 컨피그레이션에서 PFS를 지정할 경우 피어는 PFS 교환을 수행해야 합니다. 그렇지 않으면 협상은 실패합니다. 로컬 컨피그레이션에서 그룹을 지정하지 않을 경우 ASA는 기본값인 group2를 적용합니다. 로컬 컨피그레이션에서 PFS를 지정하지 않을 경우 피어의 어떤 PFS 제안도 수용합니다.

Cisco VPN Client와 상호 작용할 때 ASA는 PFS 값을 사용하는 게 아니라 1단계에서 협상한 값을 사용합니다.

예

다음 예에서는 동적 암호화 맵인 mymap 10에 대해 새 보안 연결이 협상될 때마다 PFS를 사용하도록 지정합니다. 지정된 그룹은 group 2입니다.

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 표시합니다.

crypto dynamic-map set reverse route

이 명령에 대한 자세한 내용은 crypto map set reverse-route 명령을 참조하십시오.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

구문 설명

dynamic-map-name	암호화 맵 세트의 이름을 지정합니다.
dynamic-seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

이 명령의 기본값은 off입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 명령은 mymap이라는 동적 암호화 맵에 대해 반대 경로 삽입(Reverse Route Injection)을 활성화합니다.

```
ciscoasa(config)# crypto dynamic-map mymap 10 set reverse route
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto dynamic-map	모든 동적 암호화 맵의 모든 컨피그레이션을 표시합니다.

crypto dynamic-map set ikev1 transform-set

동적 암호화 맵 엔트리에서 사용할 IKEv1 변환 세트를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set ikev1 transform-set** 명령을 사용합니다.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name11*]

동적 암호화 맵 엔트리에서 변환 세트를 제거하려면 이 명령의**no** 형식에서 변환 세트 이름을 지정합니다.

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name11*]

동적 암호화 맵 엔트리를 제거하려면 이 명령의 **no** 형식을 사용하고 변환 세트를 모두 지정하거나 하나도 지정하지 않습니다.

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set**

구문 설명

dynamic-map-name	동적 암호화 맵 세트의 이름을 지정합니다.
dynamic-seq-num	동적 암호화 맵 엔트리에 해당하는 순차 번호를 지정합니다.
transform-set-name1 *transform-set-name11*	변환 세트의 이름을 하나 이상 지정합니다. 이 명령에서 명명된 어떤 변환 세트도 **crypto ipsec ikev1 transform-set** 명령에서 정의되어야 합니다. 각 암호화 맵 엔트리는 최대 11개의 변환 세트를 지원합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0	이 명령을 도입했습니다.
7.2(1)	암호화 맵 엔트리에 있는 변환 세트의 최대 개수를 변경했습니다.
8.4(1)	**ikev1** 키워드를 추가했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

동적 암호화 맵은 모든 매개변수가 구성되지 않은 암호화 맵입니다. 정책 템플릿과 같은 기능을 하는데, 추후 IPsec 협상의 결과에 따라 누락된 매개변수를 동적으로 습득하면서 피어 요구사항과 매칭합니다. ASA는 피어의 IP 주소가 이전의 고정 또는 동적 암호화 맵에서 식별되지 않은 경우 터널 협상이 가능하도록 동적 암호화 맵을 적용합니다. 다음 유형의 피어가 해당됩니다.

- 동적으로 할당되는 공용 IP 주소를 사용하는 피어.

  LAN-LAN 및 원격 액세스 피어 모두 DHCP를 사용하여 공용 IP 주소를 얻을 수 있습니다. ASA에서는 이 주소를 터널을 시작하는 용도로만 사용합니다.

- 동적으로 할당되는 사설 IP 주소를 사용하는 피어.

  원격 액세스 터널을 요청하는 피어는 대개 헤드엔드를 통해 사설 IP 주소가 할당되어 있습니다. 일반적으로 LAN-LAN 터널은 미리 결정된 사설 네트워크 세트가 있으며, 이는 고정 맵을 구성하고 궁극적으로는 IPsec SA를 설정하는 데 사용됩니다.

고정 암호화 맵을 구성하는 관리자는 (DHCP 또는 기타 방법을 통해) 동적으로 할당되는 IP 주소를 모를 수 있습니다. 또한 할당 방식에 관계없이 다른 클라이언트의 사설 IP 주소도 모를 것입니다. VPN 클라이언트는 고정 IP 주소를 거의 사용하지 않습니다. IPsec 협상이 이루어지려면 동적 암호화 맵이 필요합니다. 예를 들어, 헤드엔드에서 IKE 협상 중에 Cisco VPN 클라이언트에 IP 주소를 할당합니다. 클라이언트는 IPec SA를 협상하는 데 이를 사용합니다.

동적 암호화 맵으로 더 편리하게 IPsec 컨피그레이션을 수행할 수 있으며, 피어가 미리 결정되지 않을 때도 있는 네트워크에서 이를 사용하면 효과적입니다. Cisco VPN 클라이언트(예: 모바일 사용자) 및 동적으로 할당된 IP 주소가 있는 라우터에는 동적 암호화 맵을 사용하십시오.

팁 동적 암호화 맵에서 **any** 키워드를 **permit** 엔트리에서 사용할 경우 주의하십시오 . 만약 **permit** 엔트리가 다루는 트래픽에 멀티캐스트 또는 브로드캐스트 트래픽이 포함될 경우 알맞은 주소 범위에 대한 **deny** 엔트리를 액세스 목록에 삽입합니다 . 네트워크 및 서브넷 브로드캐스트 트래픽 그리고 IPsec 에서 보호하지 않는 기타 트래픽에 반드시 **deny** 엔트리를 삽입해야 합니다 .

동적 암호화 맵은 연결을 시작하는 원격 피어와 SA를 협상할 때만 효과적입니다. ASA는 원격 피어와의 연결을 시작하는 데 동적 암호화 맵을 사용할 수 없습니다. 동적 암호화 맵이 구성된 상태에서 아웃바운드 트래픽이 액세스 목록의 허가 엔트리와 매칭할 경우 그에 해당하는 SA가 아직 없다면 ASA는 트래픽을 삭제합니다.

암호화 맵 세트는 동적 암호화 맵을 포함할 수 있습니다. 동적 암호화 맵 세트는 암호화 맵 세트에서 우선 순위가 가장 낮은 암호화 맵이어야 합니다. 그러면 ASA에서 다른 암호화 맵을 먼저 평가합니다. 다른 (고정) 맵 엔트리가 매칭하지 않을 때에만 동적 암호화 맵 세트를 점검합니다.

고정 암호화 맵 세트와 유사한 동적 암호화 맵 세트는 동적 맵 이름이 동일한 모든 동적 암호화 맵으로 구성됩니다. 동적 순차 번호로 세트 내에서 동적 암호화 맵을 구별합니다. 동적 암호화 맵을 구성할 경우 암호화 액세스 목록에서 IPsec 피어의 데이터 흐름을 식별하기 위해 허가 ACL을 삽입합니다. 그렇지 않으면 ASA는 어떤 데이터 흐름 ID와 피어 목적도 수용합니다.

주의 동적 암호화 맵 세트로 구성된 ASA 인터페이스에 터널링되는 트래픽에 고정(기본) 경로를 할당하지 마십시오. 터널링해야 할 트래픽을 식별하려면 동적 암호화 맵에 ACL을 추가합니다. 원격 액세스 터널과 관련된 ACL을 구성할 때는 알맞은 주소 풀을 식별하도록 주의하십시오. 터널이 설정된 후에 경로를 설치하려면 반대 경로 삽입을 이용합니다.

하나의 암호화 맵 세트에서 고정 맵 엔트리와 동적 맵 엔트리를 조합할 수 있습니다.

예

다음 예에서는 동일한 10개의 변환 세트로 구성된 "dynamic0"라는 동적 암호화 맵 엔트리를 생성합니다.

```
ciscoasa(config)# crypto dynamic-map dynamic0 1 set ikev1 transform-set 3des-md5 3des-sha
56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ipsec ikev1 transform-set	IKEv1 변환 세트를 구성합니다.
crypto map set transform-set	암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
clear configure crypto dynamic-map	컨피그레이션에서 모든 동적 암호화 맵을 지웁니다.
show running-config crypto dynamic-map	동적 암호화 맵 컨피그레이션을 표시합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto dynamic-map set ikev2 ipsec-proposal

동적 암호화 맵 엔트리에서 사용할 IKEv2를 위한 IPsec 제안을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set ikev2 ipsec-proposal** 명령을 사용합니다. 동적 암호화 맵 엔트리에서 변환 세트 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다**.**

crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

no crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

구문 설명

dynamic-map-name	동적 암호화 맵 세트의 이름을 지정합니다.
transform-set-name1 *transform-set-name11*	변환 세트의 이름을 하나 이상 지정합니다. 이 명령에서 명명된 어떤 변환 세트도 **crypto ipsec ikev2 transform-set** 명령에서 정의되어야 합니다. 각 암호화 맵 엔트리는 최대 11개의 변환 세트를 지원합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

crypto dynamic-map set ikev2 ipsec-proposal

동적 암호화 맵 엔트리에서 사용할 IKEv2를 위한 IPsec 제안을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set ikev2 ipsec-proposal** 명령을 사용합니다. 동적 암호화 맵 엔트리에서 변환 세트 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다**.**

crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

no crypto dynamic-map *dynamic-map-name* **set ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

구문 설명

dynamic-map-name	동적 암호화 맵 세트의 이름을 지정합니다.
transform-set-name1 *transform-set-name11*	변환 세트의 이름을 하나 이상 지정합니다. 이 명령에서 명명된 어떤 변환 세트도 **crypto ipsec ikev2 transform-set** 명령에서 정의되어야 합니다. 각 암호화 맵 엔트리는 최대 11개의 변환 세트를 지원합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

crypto dynamic-map set pfs

이 동적 암호화 맵 엔트리와의 새 보안 연결을 요청할 때 또는 새 보안 연결에 대한 요청을 수신할 때 PFS를 요구하도록 IPsec을 설정하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set pfs** 명령을 사용합니다. IPsec에서 PFS를 요청하지 않도록 지정하려면 이 명령의 **no** 형식을 사용합니다.

crypto dynamic-map *map-name map-index* **set pfs [group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24]**

no crypto dynamic-map *map-name map-index* **set pfs[group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24]**

구문 설명

group1	IPsec에서 새 DH 교환을 수행할 때 768비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group2	IPsec에서 새 DH 교환을 수행할 때 1024비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group5	IPsec에서 새 DH 교환을 수행할 때 1536비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group14	어떤 Diffie-Hellman 키 교환 그룹을 사용할지 지정합니다.
group19	어떤 Diffie-Hellman 키 교환 그룹을 사용할지 지정합니다.
group20	어떤 Diffie-Hellman 키 교환 그룹을 사용할지 지정합니다.
group21	어떤 Diffie-Hellman 키 교환 그룹을 사용할지 지정합니다.
group24	어떤 Diffie-Hellman 키 교환 그룹을 사용할지 지정합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
map-index	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

기본적으로 PFS는 설정되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	DH 그룹 7을 추가하기 위해 이 명령을 수정했습니다.
8.0(4)	**group 7** 명령 옵션은 더 이상 사용되지 않습니다. 그룹 7을 구성하려고 시도하면 오류 메시지가 생성되고 그룹 5가 대신 사용됩니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

PFS를 사용하면 새 보안 연결이 협상될 때마다 새 DH 교환이 일어나며, 따라서 추가적인 처리 시간이 필요합니다. PFS는 보안을 한층 더 강화합니다. 어떤 키가 공격자에 의해 크래킹될 경우 그 키와 함께 전송된 데이터만 위험해집니다.

crypto dynamic-map set tfc-packets

IPsec SA에서 더미 TFC(Traffic Flow Confidentiality) 패킷을 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set tfc-packets** 명령을 사용합니다. IPsec SA에서 TFC 패킷을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto dynamic-map *name priority* **set tfc-packets [burst length | auto] [payload-size bytes | auto] [timeout second | auto]**

no crypto dynamic-map *name priority* **set tfc-packets [burst length | auto] [payload-size bytes | auto] [timeout second | auto]**

구문 설명

name	암호화 맵 세트의 이름을 지정합니다.
priority	암호화 맵 엔트리에 부여하는 우선순위를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 암호화 맵에 대한 기존 DF 정책(SA 레벨)을 구성합니다.

crypto dynamic-map set validate-icmp-errors

IPsec 터널을 지나고 사설 네트워크의 내부 호스트로 향하는 수신 ICMP 오류 메시지를 검증할지 여부를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto dynamic-map set validate-icmp-errors** 명령을 사용합니다. 동적 암호화 맵 엔트리에서 수신 ICMP 오류 메시지 검증을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto dynamic-map *name priority* **set validate-icmp-errors**

no crypto dynamic-map *name priority* **set validate-icmp-errors**

구문 설명

name	동적 암호화 맵 세트의 이름을 지정합니다.
priority	동적 암호화 맵 엔트리에 부여하는 우선순위를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 암호화 맵 명령은 수신 ICMP 오류 메시지를 검증하는 데에만 유효합니다.

crypto engine accelerator-bias

SMP(Symmetric Multi-Processing) 플랫폼에서 암호화 코어의 할당을 변경하려면 글로벌 컨피그레이션 모드에서 **crypto engine accelerator-bias** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto engine accelerator-bias [balanced | ipsec | ssl]

no crypto engine accelerator-bias [**balanced | ipsec | ssl**]

구문 설명

balanced	암호화 하드웨어 리소스를 균등하게 배분합니다(관리/SSL, IPsec 코어).
ipsec -client	IPsec 코어(SRTP 암호화 음성 트래픽 포함)에 유리하게 암호화 하드웨어 리소스를 할당합니다.
ssl-client	관리/SSL 코어에 유리하게 암호화 하드웨어 리소스를 할당합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

ASA 5585, 5580, 5545/5555, ASASM 플랫폼에서 암호화 코어 리밸런싱을 이용할 수 있습니다.

예

다음 예에서는 crypto engine acccelerator-bias 명령을 구성하면서 사용할 수 있는 옵션을 보여줍니다.

```
ciscoasa (config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors

ciscoasa (config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec-client - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl-client - Allocate crypto hardware resources to favor SSL

ciscoasa (config)# crypto engine accelerator-bias ssl
```

crypto engine large-mod-accel

ASA 5510, 5520, 5540 또는 5550의 대규모 모듈러스 연산을 소프트웨어에서 하드웨어로 전환하려면 글로벌 컨피그레이션 모드에서 **crypto engine large-mod-accel** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto engine large-mod-accel

no crypto engine large-mod-accel

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본적으로 ASA는 대규모 모듈러스 연산을 소프트웨어에서 수행합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.3(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 ASA 모델 5510, 5520, 5540, 5550에서만 사용할 수 있습니다. 대규모 모듈러스 연산을 소프트웨어에서 하드웨어로 전환합니다. 이와 같이 하드웨어로 전환하면 다음 항목이 빨라집니다.

- 2048비트 RSA 공개 키 인증서 처리
- Diffie Hellman Group 5(DH5) 키 생성

초당 연결 수를 늘리기 위해 필요할 때 이 명령을 사용하는 것이 좋습니다. 부하에 따라 SSL 처리 성능에 다소 영향을 미칠 수 있습니다.

또한 이 명령의 어떤 형식이든 소프트웨어에서 하드웨어로 또는 하드웨어에서 소프트웨어로 전환하는 과정에 일시적인 패킷 손실을 최소화하기 위해 사용량이 적은 기간이나 유지 보수 기간에 사용하는 것이 좋습니다.

참고 ASA 5580/5500-X 플랫폼은 이미 이 기능을 통합하여 대규모 모듈러스 연산을 전환합니다 . 따라서 **crypto engine** 명령은 이 플랫폼에 적용되지 않습니다 .

예

다음 예에서는 대규모 모듈러스 연산을 소프트웨어에서 하드웨어로 전환합니다.

```
ciscoasa(config)# crypto engine large-mod-accel
```

다음 예에서는 앞의 명령을 컨피그레이션에서 제거하고 대규모 모듈러스 연산을 다시 소프트웨어로 전환합니다.

```
ciscoasa(config)# no crypto engine large-mod-accel
```

관련 명령

명령	설명
show running-config crypto engine	대규모 모듈러스 연산이 하드웨어로 전환되었는지 표시합니다.
clear configure crypto engine	대규모 모듈러스 연산을 소프트웨어로 돌려놓습니다. 이 명령은 **no crypto engine large-mod-accel** 명령과 동일합니다.

crypto ikev1 enable

IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP IKEv1 협상을 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto ikev1 enable** 명령을 사용합니다. 인터페이스에서 ISAKMP IKEv1을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev1 enable *interface-name*

no crypto ikev1 enable *interface-name*

구문 설명

interface-name	ISAKMP IKEv1 협상을 활성화하거나 비활성화할 인터페이스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp enable** 명령을 도입했습니다.
7.2(1)	**crypto isakmp enable** 명령으로 **isakmp enable** 명령을 대체했습니다.
8.4(1)	IKEv2 기능을 추가함에 따라 **crypto isakmp enable** 명령을 **crypto ikev1 enable** 명령으로 변경했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 내부 인터페이스에서 ISAKMP를 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# no crypto isakmp enable inside
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev1 ipsec-over-tcp

IPsec over TCP를 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto ikev1 ipsec-over-tcp** 명령을 사용합니다. IPsec over TCP를 비활성화하려면 이 명령의 the **no** 형식을 사용합니다.

crypto ikev1 ipsec-over-tcp [**port** *port1...port10*]

no crypto ikev1 ipsec-over-tcp [**port** *port1...port10*]

구문 설명

port *port1...port10*	(선택 사항) 디바이스가 TCP 연결을 통해 IPsec을 승인하는 포트를 지정합니다. 최대 10개의 포트를 나열할 수 있습니다. 포트 번호는 1~65535입니다. 기본 포트 번호는 10000입니다.

기본값

기본값은 disabled입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp ipsec-over-tcp** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp ipsec-over-tcp** 명령으로 **isakmp ipsec-over-tcp** 명령을 대체했습니다**.**
8.4(1)	명령의 이름을 **crypto isakmp ipsec-over-tcp** 에서 **crypto ikev1 ipsec-over-tcp**로 변경했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 이 예에서는 포트 45에서 IPsec over TCP를 활성화합니다.

```
ciscoasa(config)# crypto ikev1 ipsec-over-tcp port 45
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev1 limit max-in-negotiation-sa

ASA에서 IKEv2 협상 중인(열린) SA의 수를 제한하려면 글로벌 컨피그레이션 모드에서 **crypto ikev1 limit max-in-negotiation-sa** 명령을 사용합니다. 열린 SA의 수 제한을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

no crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

구문 설명

threshold percentage	ASA에 대해 협상 중(열린) 상태가 될 수 있는 총 SA의 비율. 임계값에 도달하면 더 이상의 연결이 거부됩니다. 범위는 1%~100%입니다. 기본값은 100%입니다.

기본값

기본값은 disabled입니다. ASA는 열린 SA의 수를 제한하지 않습니다.

사용 지침

crypto ikev1 limit-max-in-negotiation-sa 명령은 임의의 시점에서 협상 중 상태일 수 있는 SA의 최대 개수를 제한합니다.

crypto kev2 limit max in-negotiation-sa 명령은 현재의 연결을 보호하고 쿠키-챌린지 기능으로 막을 수 없는 메모리 및/또는 CPU 공격을 방지하기 위해 더 이상의 연결이 협상하는 것을 차단합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

예

다음 예에서는 협상 가능한 IKEv1 연결의 수를 최대 허용 IKEv1 연결의 70%로 제한합니다.

```
ciscoasa(config)# crypto ikev1 limit max in-negotiation-sa 70
```

관련 명령

명령	설명
crypto ikev1 limit max-sa	ASA의 IKEv1 연결 수를 제한합니다.
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev1 policy

IPsec 연결을 위한 IKEv1 SA(security association)를 생성하려면 글로벌 컨피그레이션 모드에서 **crypto ikev2 policy** 명령을 사용합니다. 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev1 policy *priority*

no crypto ikev1 policy *priority*

구문 설명

priority	정책 모음의 우선 순위. 범위는 1~65535이며, 1이 가장 높고 65535가 가장 낮습니다.

기본값

기본 동작 또는 기본값이 없습니다.

사용 지침

이 명령은 IKEv1 정책 컨피그레이션 모드를 시작합니다. 여기서 추가 IKEv1 SA 설정을 지정할 수 있습니다. IKEv1 SA는 1단계에서 사용되는 키로서 IKEv1 피어가 2단계에서 안전하게 통신할 수 있게 합니다. **crypto ikev1 policy** 명령을 입력한 다음 추가 명령을 사용하여 SA 암호화 알고리즘, DH 그룹, 무결성 알고리즘, 수명, 해시 알고리즘을 설정할 수 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 추가됩니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 예에서는 우선 순위 1 IKEv1 SA를 생성하며 IKEv1 정책 컨피그레이션 모드를 시작합니다.

```
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev2-policy)#
```

관련 명령

명령	설명
crypto ikev2 cookie-challenge	ASA에서 SA 개시 패킷에 대한 응답으로 피어 디바이스에 쿠키 챌린지를 보낼 수 있게 합니다.
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev2 enable

IPsec 피어가 ASA와 통신하는 인터페이스에서 ISAKMP IKEv2 협상을 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto ikev2 enable** 명령을 사용합니다. 인터페이스에서 ISAKMP IKEv2을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev2 enable *interface-name* [**client-services [port** *port*]]

no crypto ikev2 enable *interface-name* [**client-services [port** *port*]]

구문 설명

interface-name	ISAKMP IKEv2 협상을 활성화하거나 비활성화할 인터페이스의 이름을 지정합니다.
client-services	인터페이스에서 IKEv2 연결을 위한 클라이언트 서비스를 활성화합니다. 클라이언트 서비스에는 향상된 Anyconnect Secure Mobility클라이언트 기능, 이를테면 소프트웨어 업데이트, 클라이언트 프로필, GUI 현지화(번역) 및 사용자 지정, Cisco Secure Desktop, SCEP 프록시 등이 포함됩니다. 클라이언트 서비스를 비활성화할 경우 AnyConnect 클라이언트는 계속 IKEv2와 기본 IPsec 연결을 설정합니다.
port *port*	IKEv2 연결을 위한 클라이언트 서비스를 활성화할 포트를 지정합니다. 범위는 1~65535입니다. 기본 포트는 443입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 추가됩니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령만 사용하면 클라이언트 서비스가 활성화되지 않습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 외부 인터페이스에서 IKEv2를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# crypto ikev2 enable outside client-services port 443
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev2 cookie-challenge

ASA에서 SA 개시 패킷에 대한 응답으로 피어 디바이스에 쿠키 챌린지를 보낼 수 있게 하려면 글로벌 컨피그레이션 모드에서 **crypto ikev2 cookie-challenge** 명령을 사용합니다. 쿠키 챌린지를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

no crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

구문 설명

threshold percentage	ASA에서 협상 중일 수 있는 총 SA의 비율. 그에 따라 향후 SA 협상에서 쿠키 챌린지가 트리거됩니다. 범위는 0%~99%입니다. 기본값은 50%입니다.
always	항상 수신 SA에 대해 쿠키 챌린지를 실행합니다.
never	결코 수신 SA에 대해 쿠키 챌린지를 실행하지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

사용 지침

피어에 대한 쿠키 챌린지는 만일의 DoS(서비스 거부) 공격을 방지합니다. 피어 디바이스에서 SA 개시 패킷을 보내고 ASA에서 응답을 보내지만 피어 디바이스에서 더 이상 응답하지 않을 때 DoS 공격이 시작됩니다. 피어 디바이스가 이 작업을 계속할 경우 ASA에서 가능한 전체 SA 요청 한도가 소진되어야 응답이 중단됩니다.

crypto ikev2 cookie-challenge 명령을 사용하여 임계 백분율을 활성화하면 열린 SA 협상의 수를 제한합니다. 예를 들어, 기본 설정이 50%라면 허용된 SA의 50%가 협상 중(열린) 상태일 경우 ASA는 추가적으로 수신되는 SA 개시 패킷에 대해 쿠키 챌린지를 수행합니다. IKEv2 SA 1,000개가 허용되는 Cisco ASA 5580의 경우 SA 500개가 열렸다면 그 이후의 수신 SA는 모두 쿠키 챌린지됩니다.

crypto kev2 limit max in-negotiation-sa 명령과 함께 사용할 경우 쿠키 챌린지 임계값을 최대 협상 중 임계값보다 낮게 구성함으로써 효과적인 교차 점검이 가능해집니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 추가됩니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 예에서는 쿠키 챌린지 임계값이 30%로 설정됩니다.

```
ciscoasa(config)# crypto ikev2 cookie-challenge 30
```

관련 명령

명령	설명
crypto ikev2 limit max-sa	ASA의 IKEv2 연결 수를 제한합니다.
crypto ikev2 limit max-in-negotiation-sa	ASA에서 IKEv2 협상 중(열린) SA의 수를 제한합니다.
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev2 limit max-in-negotiation-sa

ASA에서 IKEv2 협상 중인(열린) SA의 수를 제한하려면 글로벌 컨피그레이션 모드에서 **crypto ikev2 limit max-in-negotiation-sa** 명령을 사용합니다. 열린 SA의 수 제한을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev2 limit max in-negotiation-sa *threshold percentage*

no crypto ikev2 limit max in-negotiation-sa *threshold percentage*

구문 설명

threshold percentage	ASA에 대해 협상 중(열린) 상태가 될 수 있는 총 SA의 비율. 임계값에 도달하면 더 이상의 연결이 거부됩니다. 범위는 1%~100%입니다. 기본값은 100%입니다.

기본값

기본값은 disabled입니다. ASA는 열린 SA의 수를 제한하지 않습니다.

사용 지침

crypto ikev2 limit-max-in-negotiation-sa 명령은 임의의 시점에서 협상 중 상태일 수 있는 SA의 최대 개수를 제한합니다. **crypto ikev2 cookie-challenge** 명령과 함께 사용할 경우 효과적인 교차 점검을 위해 쿠키 챌린지 임계값을 이 한도보다 낮게 구성합니다.

수신 연결에 쿠키로 챌린지하는 **crypto ikev2 cookie-challenge** 명령과 달리 **crypto kev2 limit max in-negotiation-sa** 명령은 현재 연결을 보호하고 쿠키 챌린지 기능에서 막지 못할 수 있는 메모리 및/또는 CPU 공격을 방지하기 위해 더 이상의 연결이 협상할 수 없게 합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 예에서는 협상 가능한 IKEv2 연결의 수를 최대 허용 IKEv2 연결의 70%로 제한합니다.

```
ciscoasa(config)# crypto ikev2 limit max in-negotiation-sa 70
```

관련 명령

명령	설명
crypto ikev2 limit max-sa	ASA의 IKEv2 연결 수를 제한합니다.
crypto ikev2 cookie-challenge	ASA에서 SA 개시 패킷에 대한 응답으로 피어 디바이스에 쿠키 챌린지를 보낼 수 있게 합니다.
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev2 limit max-sa

ASA에서 IKEv2 연결 수를 제한하려면 글로벌 컨피그레이션 모드에서 **crypto ikev2 limit max-sa** 명령을 사용합니다. 연결 수 제한을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev2 limit max-sa *number*

no crypto ikev2 limit max-sa *number*

구문 설명

number	ASA에서 허용되는 IKEv2 연결 수. 한도에 도달하면 더 이상의 연결이 거부됩니다. 범위는 1~10000입니다.

기본값

기본값은 disabled입니다. ASA는 IKEv2 연결의 수를 제한하지 않습니다. 허용되는 IKEv2 연결의 최대 수는 라이센스에 규정된 최대 연결 수와 같습니다.

사용 지침

crypto ikev2 limit max-sa 명령은 ASA의 최대 SA 수를 제한합니다.

crypto ikev2 cookie-challenge 명령과 함께 사용할 경우 효과적인 교차 점검을 위해 쿠키 챌린지 임계값을 이 한도보다 낮게 구성합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 예에서는 IKEv2 연결의 수를 5000으로 제한합니다.

```
ciscoasa(config)# crypto ikev2 limit max-sa 5000
```

관련 명령

명령	설명
crypto ikev2 cookie-challenge	ASA에서 SA 개시 패킷에 대한 응답으로 피어 디바이스에 쿠키 챌린지를 보낼 수 있게 합니다.
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev2 policy

AnyConnect 연결을 위한 IKEv2 SA(security association)를 생성하려면 글로벌 컨피그레이션 모드에서 **crypto ikev2 policy** 명령을 사용합니다. 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev2 policy *priority policy_index*

no crypto ikev2 policy *priority policy_index*

구문 설명

policy index	IKEv2 정책 컨피그레이션 모드에 액세스합니다.
priority	정책 모음의 우선 순위. 범위는 1~65535이며, 1이 가장 높고 65535가 가장 낮습니다. IKEv2 키 파생의 일환으로 그룹 [1] [2] [5]가 그룹 [1] [2] [5] [14] [24가 되어 DH 그룹 14 및 24를 지원합니다.

기본값

기본 동작 또는 값이 없습니다.

사용 지침

IKEv2 SA는 1단계에서 사용되는 키로서 IKEv2 피어가 2단계에서 안전하게 통신할 수 있게 합니다. **crypto ikev2 policy** 명령을 입력하여 IKEv2 정책 컨피그레이션 모드를 시작하고, 여기서 추가 IKEv2 SA 설정을 지정합니다. 추가 명령을 사용하여 SA 암호화 알고리즘, DH 그룹, 무결성 알고리즘, 수명, 해시 알고리즘을 설정할 수 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다. 정책 색인 옵션을 추가했습니다.

예

다음 예에서는 우선 순위 1 IKEv2 SA를 생성하며 IKEv2 정책 컨피그레이션 모드를 시작합니다.

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

관련 명령

명령	설명
crypto ikev2 cookie-challenge	ASA에서 SA 개시 패킷에 대한 응답으로 피어 디바이스에 쿠키 챌린지를 보낼 수 있게 합니다.
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev2 redirect

마스터에서 클러스터 멤버로 로드 밸런싱 리디렉션이 일어나는 IKEv2 단계를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto ikev2 redirect** 명령을 사용합니다. 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev2 redirect {during-init | during-auth}

no crypto ikev2 redirect {during-init | during-auth}

구문 설명

during-auth	IKEv2 인증 교환 중 클러스터 멤버에 대한 로드 밸런싱 리디렉션을 활성화합니다.
during-init	IKEv2 SA 개시 교환 중 클러스터 멤버에 대한 로드 밸런싱 리디렉션을 활성화합니다.

기본값

기본적으로 클러스터 멤버에 대한 로드 밸런싱 리디렉션이 이루어지며, 이는 IKEv2 인증 교환 과정에서 일어납니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.

예

다음 예에서는 IKEv2 개시 교환 과정에서 클러스터 멤버에 대한 로드 밸런싱 리디렉션이 일어나도록 설정합니다.

```
ciscoasa(config)# crypto ikev2 redirect during-init
```

관련 명령

명령	설명
crypto ikev2 cookie-challenge	ASA에서 SA 개시 패킷에 대한 응답으로 피어 디바이스에 쿠키 챌린지를 보낼 수 있게 합니다.
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto ikev2 remote-access trust-point

AnyConnect IKEv2 연결에서 어떤 전역 신뢰 지점을 ASA의 ID 인증서 신뢰 지점으로 참조하고 사용하도록 지정하려면 터널 그룹 컨피그레이션 모드에서 **crypto ikev2 remote-access trust-point** 명령을 사용합니다 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ikev2 remote-access trust-point *name* [*line number*]

no crypto ikev2 remote-access trust-point *name* [*line number*]

구문 설명

name	신뢰 지점의 이름이며 최대 65자입니다.
line number	라인 번호상 어디에 신뢰 지점을 삽입할지 지정합니다. 일반적으로 이 옵션은 다른 라인을 제거하고 다시 추가하는 일 없이 맨 위에 신뢰 지점을 삽입하는 데 사용합니다. 라인을 지정하지 않을 경우 ASA는 목록의 맨 끝에 신뢰 지점을 추가합니다.

기본값

기본 동작 또는 값이 없습니다.

사용 지침

crypto ikev2 remote-access trust-point 명령을 사용하면 ASA에 대한 신뢰 지점이 모든 KIEv2 연결에서 AnyConnect 클라이언트에 자신을 인증하도록 구성할 수 있습니다. 이 명령을 사용하면 AnyConnect 클라이언트에서 사용자에 대한 그룹 선택을 지원할 수 있습니다.

RSA 2개, ECDSA 2개 또는 각각 하나씩인 두 신뢰 지점을 동시에 구성할 수 있습니다. ASA는 구성된 신뢰 지점 목록을 검사하고 클라이언트가 지원하는 첫 번째 신뢰 지점을 선택합니다. ECDSA를 선호할 경우 이 신뢰 지점을 RSA 신뢰 지점보다 먼저 구성해야 합니다.

이미 있는 신뢰 지점을 추가하려고 하면 오류가 발생합니다. 제거할 신뢰 지점 이름을 지정하지 않고 **no crypto ikev2 remote-access trustpoint** 명령을 사용할 경우 모든 신뢰 지점 컨피그레이션이 제거됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
터널 그룹 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 및 두 신뢰 지점 컨피그레이션에 대한 지원을 추가했습니다.

예

다음 예에서는 신뢰 지점인 *cisco_asa_trustpoint*를 지정합니다.

```
ciscoasa(config)# crypto ikev2 remote-access trust-point cisco_asa_trustpoint
```

crypto ipsec df-bit

IPsec 패킷에 대한 DF 비트 정책을 구성하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec df-bit** 명령을 사용합니다.

crypto ipsec df-bit [clear-df | copy-df | set-df] *interface*

구문 설명

clear-df	(선택 사항) 외부 IP 헤더에서 DF 비트를 지우도록 지정하고 ASA에서 추가할 패킷 및 IPsec 캡슐화를 단편화할 수 있도록 지정합니다.
copy-df	(선택 사항) ASA가 원래의 패킷에서 외부 DF 비트 설정을 찾도록 지정합니다.
set-df	(선택 사항) 외부 IP 헤더에 DF 비트가 설정되도록 지정합니다. 그러나 원래의 패킷에서 DF 비트가 지워진 경우 ASA가 패킷을 단편화할 수 있습니다.
interface	인터페이스 이름을 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다. 지정된 설정 없이 이 명령을 활성화할 경우 ASA에서는 **copy-df** 설정을 기본으로 사용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

IPsec 터널의 DF 비트 기능으로 ASA가 캡슐화된 헤더에서 DF(Don't Fragment) 비트를 지우거나 설정하거나 복사할지 여부를 지정할 수 있습니다. IP 헤더 내의 DF 비트는 어떤 디바이스에서 패킷의 단편화를 허용할지 여부를 결정합니다.

글로벌 컨피그레이션 모드에서 **crypto ipsec df-bit** 명령을 사용하면 ASA에서 캡슐화된 헤더에 DF 비트를 지정하도록 구성할 수 있습니다. 이 명령은 일반 텍스트 패킷의 DF 비트 설정을 처리하며 암호화 적용 시 이를 지우거나 설정하거나 외부 IPsec 헤더에 복사합니다.

터널 모드 IPsec 트래픽을 캡슐화할 때 DF 비트에 대해 **clear-df** 설정을 사용합니다. 이 설정으로 디바이스에서 사용 가능한 MTU 크기보다 큰 패킷을 보낼 수 있게 됩니다. 또한 이 설정은 사용 가능한 MTU 크기를 모르는 경우에 유용합니다.

주의 다음과 같이 충돌하는 컨피그레이션을 설정할 경우 패킷이 삭제됩니다.
crypto ipsec fragmentation after-encryption(패킷 단편화)
crypto ipsec df-bit set-df outside(DF 비트 설정)

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 IPsec DF 정책을 **clear-df**로 설정합니다.

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ipsec fragmentation	IPsec 패킷에 대한 단편화 정책을 구성합니다.
show crypto ipsec df-bit	지정된 인터페이스에 대한 DF 비트 정책을 표시합니다.
show crypto ipsec fragmentation	지정된 인터페이스에 대한 단편화 정책을 표시합니다.

crypto ipsec fragmentation

IPsec 패키에 대한 단편화 정책을 구성하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec fragmentation** 명령을 사용합니다.

crypto ipsec fragmentation {after-encryption | before-encryption} *interface*

구문 설명

after-encryption	ASA에서 암호화한 후 최대 MTU 크기와 비슷한 IPsec 패킷을 단편화하도록 지정합니다(사전 단편화 비활성화).
before-encryption	ASA에서 암호화하기 전에 최대 MTU 크기와 비슷한 IPsec 패킷을 단편화하도록 지정합니다(사전 단편화 활성화).
interface	인터페이스 이름을 지정합니다.

기본값

기본적으로 before-encryption이 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

패킷이 암호화하는 ASA의 아웃바운드 링크 MTU 크기에 근접할 경우 IPsec 헤더와 함께 캡슐화된다면 아웃바운드 링크 MTU를 초과할 가능성이 높습니다. 그러면 암호화 이후에 패킷 단편화가 일어나며, 해독하는 디바이스는 프로세스 경로에서 이를 다시 합치게 됩니다. IPsec VPN에 대한 사전 단편화를 통해 해독 시 디바이스의 성능을 높일 수 있습니다. 프로세스 경로가 아닌 고성능 CEF 경로에서 작동할 수 있기 때문입니다.

IPsec VPN에 대한 사전 단편화를 통해 암호화하는 디바이스는 IPsec SA의 일부로 구성된 변환 세트의 정보를 바탕으로 캡슐화된 패킷 크기를 미리 판단할 수 있습니다. 패킷이 출력 인터페이스의 MTU를 초과할 것으로 예상될 경우 디바이스는 암호화하기 전에 패킷을 단편화합니다. 그러면 해독하기 전에 프로세스 레벨에서 다시 합칠 필요가 없으므로 해독 성능 및 전반적인 IPsec 트래픽 처리량이 향상됩니다.

IPv6 활성 인터페이스에서 허용되는 최소 MTU는 1280바이트입니다. 그러나 IPsec이 인터페이스에서 활성화된 경우, IPsec 암호화의 오버헤드 때문에 MTU가 1380보다 작은 값으로 설정되어야 합니다. 1380바이트보다 낮게 인터페이스를 설정하면 패킷이 폐기될 수 있습니다.

주의 다음과 같이 충돌하는 컨피그레이션을 설정할 경우 패킷이 삭제됩니다.
crypto ipsec fragmentation after-encryption(패킷 단편화)
crypto ipsec df-bit set-df outside(DF 비트 설정)

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 디바이스의 전역에서 IPsec 패킷에 대한 사전 단편화를 활성화합니다.

```
ciscoasa(config)# crypto ipsec fragmentation before-encryption inside
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 인터페이스에서 IPsec 패킷에 대한 사전 단편화를 비활성화합니다.

```
ciscoasa(config)# crypto ipsec fragmentation after-encryption inside
ciscoasa(config)#
```

관련 명령

명령	설명
crypto ipsec df-bit	IPsec 패킷에 대한 DF 비트 정책을 구성합니다.
show crypto ipsec fragmentation	IPsec 패킷에 대한 단편화 정책을 표시합니다.
show crypto ipsec df-bit	지정된 인터페이스에 대한 DF 비트 정책을 표시합니다.

crypto ipsec security-association pmtu-aging

PMTU path maximum transfer unit) 에이징을 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec security-association pmtu-aging** 명령을 사용합니다. PMTU 에이징을 비활성화하려면 이 명령의 no 형식을 사용합니다.

crypto ipsec security-association pmtu-aging *reset-interval*

[no] crypto ipsec security-association pmtu-aging *reset-interval*

구문 설명

reset-interval	PMTU 값을 재설정하는 간격을 설정합니다.

기본값

이 기능은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

재설정 간격은 초 단위로 지정됩니다.

crypto ipsec ikev2 ipsec-proposal

IKEv2 프로토콜을 생성하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec ikev2 ipsec-proposal** 명령을 사용합니다. 제안을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

no crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

구문 설명

proposal name	IPsec ESP 제안 하위 모드에 액세스합니다.
proposal tag	IKEv2 IPsec 제안의 이름이며 1자~64자의 문자열입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 제안을 생성하고 ipsec 제안 컨피그레이션 모드를 시작합니다. 여기서 해당 제안에 대해 여러 암호화 및 무결성 유형을 지정할 수 있습니다.

예

다음 예에서는 secure라는 IPsec 제안을 생성하고 IPsec 제안 컨피그레이션 모드를 시작합니다.

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal secure
ciscoasa(config-ipsec-proposal)#
```

관련 명령

명령	설명
show running-config ipsec	모든 변환 세트의 컨피그레이션을 표시합니다.
crypto map set transform-set	암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
crypto dynamic-map set transform-set	동적 암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.
show running-config crypto dynamic-map	동적 암호화 맵 컨피그레이션을 표시합니다.

crypto ipsec ikev2 sa-strength-enforcement

IKEv2 암호화 암호의 강도가 그 하위 IPsec SA 암호화 암호의 강도보다 높게 합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto ipsec ikev2 sa-strength-enforcement

no crypto ipsec ikev2 sa-strength-enforcement

기본값

기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

사용 지침

하위 SA가 상위 IKEv2 연결보다 강력한 암호화의 암호를 사용할 경우 보안이 향상되지 않습니다. 그러한 일이 생기지 않게 IPsec을 구성하는 것이 보안상 바람직합니다. 강도 강제 적용 설정은 암호화의 암호에만 적용됩니다. 무결성 또는 키 교환 알고리즘을 변경하지 않습니다. IKEv2 시스템은 각 하위 SA의 선택된 암호화 암호의 상대적 강도를 다음과 같이 비교합니다.

활성화되면 하위 SA에 대해 구성된 암호화 암호가 상위 IKEv2 암호화 암호보다 강력하지 않음을 확인합니다. 하위 SA를 찾으면 상위 암호를 사용하도록 업데이트합니다. 호환되는 암호가 없을 경우 하위 SA 협상이 중단됩니다. syslog 및 디버그 메시지에서 이 작업을 로깅합니다.

지원되는 암호화 암호가 아래에 강도가 높은 것부터 나열되어 있습니다. 동일한 라인의 암호는 이 검사에 관한 한 동일한 강도입니다.

- AES-GCM-256, AES-CBC-256
- AES-GCM-192, AES-CBC, 192
- AES-GCM-128, AES-CBC-128
- 3DES
- DES
- AES-GMAC(모든 크기), NULL

관련 명령

명령	설명
show running-config ipsec	활성화되면 crypto ipsec ikev2 sa-strength-enforcement를 표시합니다.

crypto ipsec security-association lifetime

전역 수명의 값을 구성하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec security-association lifetime** 명령을 사용합니다. 전역 수명의 값을 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

crypto ipsec security-association lifetime {seconds *seconds* **| kilobytes** *kilobytes* | unlimited}

no crypto ipsec security-association lifetime {seconds *seconds* **| kilobytes** *kilobytes* | *unlimited*}

구문 설명

kilobytes	어떤 보안 연결이 만료되기 전에 그 보안 연결을 사용하여 피어를 통과할 수 있는 트래픽의 볼륨(킬로바이트)을 지정합니다. 범위는 10kbyte~2147483647kbyte입니다. 기본값은 4,608,000킬로바이트입니다.
seconds	보안 연결이 만료되기 전까지의 수명을 초 단위로 지정합니다. 범위는 120초~214783647초입니다. 기본값은 28,800초(8시간)입니다.
unlimited	ASA가 터널의 개시자일 때 빠른 모드 1 패킷에 Kilobytes를 보내지 않습니다.

기본값

kilobytes의 기본값은 4,608,000이고 seconds의 기본값은 28,800입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.
9.1(2)	unlimited 인수를 추가했습니다.

사용 지침

이 **crypto ipsec security-association lifetime** 명령은 IPsec 보안 연결을 협상할 때 사용되는 전역 수명의 값을 변경합니다.

IPsec 보안 연결에서는 공유 암호 키를 사용합니다. 이 키와 그 보안 연결은 동시에 시간 초과됩니다.

해당 암호화 맵 엔트리의 수명 값이 구성되지 않았다고 가정하면, ASA에서 협상 중에 새로운 보안 연결을 요청할 때 피어에 보내는 요청에서 전역 수명의 값을 지정합니다. 이 값을 새 보안 연결의 수명으로 사용합니다. ASA에서 피어로부터 협상 요청을 받을 때 피어에서 제안한 수명 값과 새 보안 연결의 수명으로 로컬에 구성된 수명 값 중 더 작은 값을 사용합니다.

수명에는 "timed" 수명과 "traffic-volume" 수명의 2가지가 있습니다. 이 수명 중 더 짧은 것에 도달하면 보안 연결이 만료됩니다.

ASA에서는 사용자가 암호화 맵, 동적 맵, IPsec 설정을 즉시 변경할 수 있습니다. 변경할 경우 ASA는 변경이 적용되는 연결만 종료합니다. 사용자가 액세스 목록에서 엔트리를 삭제하는 방법으로 암호화 맵과 연결된 기존 액세스 목록을 변경할 경우, 해당 연결만 종료됩니다. 액세스 목록의 다른 엔트리를 기반으로 한 연결은 영향을 받지 않습니다.

전역 timed 수명을 변경하려면 **crypto ipsec security-association lifetime seconds** 명령을 사용합니다. timed 수명은 지정된 시간(초)이 경과하면 보안 연결이 시간 초과됩니다.

전역 traffic-volume 수명을 변경하려면 **crypto ipsec security-association lifetime kilobytes** 명령을 사용합니다. traffic-volume 수명은 지정된 트래픽의 양(킬로바이트)만큼 보안 연결의 키에 의해 보호받았으면 보안 연결이 시간 초과됩니다.

수명이 더 짧으면 성공적인 키 복구 공격을 마운트하기가 더 어려워질 수 있습니다. 공격자가 사용할 수 있는 동일한 키로 암호화된 데이터가 줄어들기 때문입니다. 그러나 더 짧은 수명을 사용하려면 새 보안 연결을 설정하느라 더 많은 CPU 처리 시간이 필요합니다.

보안 연결(및 그 키)은 지정된 시간(초)이 경과했을 때 또는 지정된 트래픽의 양(킬로바이트)이 통과했을 때 중 더 빠른 시점에 만료됩니다.

예

다음 예에서는 보안 연결에 대해 전역 timed 수명을 지정합니다.

```
ciscoasa(config)# crypto ipsec-security association lifetime seconds 240
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 IPsec 컨피그레이션(즉 전역 수명과 변환 세트)을 지웁니다.
show running-config crypto map	모든 암호 맵에 대한 모든 컨피그레이션을 표시합니다.

crypto ipsec security-association replay

IPsec 재생 방지 윈도우(antireplay window) 크기를 구성하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec security-association replay** 명령을 사용합니다. 윈도우 크기를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

crypto ipsec security-association replay {window-size *n* **| disable}**

no crypto ipsec security-association replay {window-size *n* **| disable}**

구문 설명

n	윈도우 크기를 설정합니다. 값은 64, 128, 256, 512 또는 1024가 될 수 있습니다. 기본값은 64입니다.
disable	재생 방지 검사를 비활성화합니다.

기본값

기본 윈도우 크기는 64입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(4)/8.0(4)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

Cisco IPsec 인증은 암호화된 패킷 각각에 고유 일련 번호를 부여함으로써 암호화된 패킷을 복제하는 수법의 공격자를 차단하는 재생 방지 보호 기능을 제공합니다 (보안 연결 재생 방지는 수신자가 재생 공격으로부터 스스로를 지키기 위해 오래되었거나 중복된 패킷을 거부할 수 있는 보안 서비스입니다.). 해독기는 이전에 확인한 일련 번호와 대조하면서 검사합니다. 암호기에서는 점점 증가하는 일련 번호를 부여합니다. 해독기는 이미 확인한 적이 있는 가장 큰 일련 번호의 값 X를 기억하고 있습니다. N은 윈도우 크기이며, 해독기는 X-N+1~X 범위의 일련 번호를 가진 패킷을 봤는지 여부도 기억합니다. 일련 번호가 X-N인 패킷은 모두 삭제됩니다. 현재 N은 64로 설정되었으므로 해독기는 64개 패킷만 추적할 수 있습니다.

그러나 64패킷 윈도우 크기가 충분하지 않을 때도 있습니다. 이를테면 QoS에 따라 우선 순위가 높은 패킷을 먼저 처리하는데, 그러면 우선 순위가 낮은 일부 패킷이 해독기에서 최근에 수신한 64개 패킷 중 하나임에도 불구하고 삭제될 수도 있습니다. 그로 인해 경고 syslog 메시지가 생성될 수 있는데, 이는 오경보입니다. **crypto ipsec security-association replay** 명령으로 윈도우 크기를 확장하여 해독기에서 64개보다 많은 수의 패킷을 추적하게 할 수 있습니다.

재생 방지 윈도우 크기를 늘리더라도 처리량 및 보안에 아무런 영향을 주지 않습니다. 메모리에 미치는 영향도 미미합니다. 수신하는 IPsec SA당 추가로 128바이트를 사용하여 해독기에 일련 번호를 저장하기 때문입니다. 향후 재생 방지와 관련된 문제가 없도록 전체 1024 윈도우 크기를 사용하는 것이 좋습니다.

예

다음 예에서는 보안 연결에 대해 재생 방지 윈도우 크기를 지정합니다.

```
ciscoasa(config)# crypto ipsec security-association replay window-size 1024
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 IPsec 컨피그레이션(즉 전역 수명과 변환 세트)을 지웁니다.
shape	트래픽 셰이핑을 활성화합니다.
priority	우선 순위 큐잉을 활성화합니다.
show running-config crypto map	모든 암호 맵에 대한 모든 컨피그레이션을 표시합니다.

crypto ipsec ikev1 transform-set

IKEv1 변환 세트를 생성하거나 제거하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec ikev1 transform-set** 명령을 사용합니다. 변환 세트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ipsec ikev1 transform-set *transform-set-name encryption* **[***authentication***]**

no crypto ipsec ikev1 transform-set *transform-set-name encryption* **[***authentication***]**

구문 설명

authentication	(선택 사항) IPsec 데이터 흐름의 무결성을 보장하기 위해 다음 인증 방법 중 하나를 지정합니다. **esp-md5-hmac**은 MD5/HMAC-128을 해시 알고리즘으로 사용합니다. **esp-sha-hmac**은 SHA/HMAC-160을 해시 알고리즘으로 사용합니다. **esp-none**은 HMAC 인증을 사용하지 않습니다.
encryption	IPsec 데이터 흐름을 보호하려면 다음 암호화 방법 중 하나를 지정합니다. **esp-aes**는 128비트 키와 함께 AES를 사용합니다. **esp-aes-192**는 192비트 키와 함께 AES를 사용합니다. **esp-aes-256**은 256비트 키와 함께 AES를 사용합니다. **esp-des**는 56비트 DES-CBC를 사용합니다. **esp-3des**는 3DES 알고리즘을 사용합니다. **esp-null**는 암호화를 사용하지 않습니다.
transform-set-name	생성하거나 수정하는 변환 세트의 이름. 이미 컨피그레이션에 있는 변환 세트를 보려면 **show running-config ipsec** 명령을 입력합니다.

기본값

기본 인증 설정은 esp-none(인증 없음)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0	이 명령을 도입했습니다.
7.2(1)	이 섹션을 다시 작성했습니다.
8.4(1)	**ikev1** 키워드가 추가되었습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 변환 세트에서 사용할 IPsec 암호화 및 해시 알고리즘을 식별합니다.

변환 세트를 구성한 다음 암호화 맵에 이를 지정합니다. 하나의 암호화 맵에 최대 6개의 변환 세트를 지정할 수 있습니다. 피어가 IPsec 세션을 설정하려고 할 때 ASA는 각 암호화 맵의 액세스 목록을 사용하여 매칭하는 항목을 찾을 때까지 피어를 평가합니다. 그러면 ASA는 피어가 협상하는 모든 프로토콜, 알고리즘, 기타 설정을 평가합니다. 암호화 맵에 지정된 변환 세트의 값을 참조하면서 매칭하는 항목을 찾습니다. ASA에서 피어의 IPsec 협상을 변환 세트의 설정에 매칭할 경우 이를 IPsec 보안 연결의 일부로 보호 대상 트래픽에 적용합니다. ASA는 피어와 액세스 목록의 매칭에 실패하고 암호화 맵에 지정된 변환 세트에서 피어 보안 설정의 정확한 매칭을 찾을 경우 IPsec 세션을 종료합니다.

암호화 또는 인증 중 어느 것이든 먼저 지정할 수 있습니다. 인증을 지정하지 않고 암호화를 지정할 수 있습니다. 생성하는 변환 세트에서 인증을 지정할 경우 그와 함께 암호화를 지정해야 합니다. 수정하는 변환 세트에서 인증만 지정할 경우 그 변환 세트는 기존의 암호화 설정을 유지합니다.

AES 암호화를 사용하는 경우 역시 글로벌 컨피그레이션 모드에서 **isakmp policy priority group 5** 명령을 사용하여 DF 그룹 5를 지정함으로써 AES에서 제공하는 큰 키를 수용할 수 있게 하는 것이 좋습니다.

팁 암호화 맵 또는 동적 암호화 맵에 변환 세트를 적용하고 여기에 지정된 변환 세트를 볼 때 변환 세트의 이름이 그 컨피그레이션을 반영한다면 편리할 것입니다 . 예를 들어 , 아래의 첫 번째 예에서 "3des-md5" 라는 이름은 변환 세트에 사용된 암호화 및 인증을 보여줍니다 . 이름 다음에 오는 값이 변환 세트에 지정된 실제 암호화 및 인증 설정입니다 .

예

다음 명령은 사용 가능한 모든 암호화 및 인증 옵션을 보여줍니다. 암호화 및 인증을 지정하지 않는 것은 제외됩니다.

```
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-md5 esp-3des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-sha esp-3des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-md5 esp-des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-sha esp-3des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-md5 esp-aes esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-sha esp-aes esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-sha esp-aes-192 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-sha esp-aes-256 esp-sha-hmac
ciscoasa(config)#
```

관련 명령

명령	설명
show running-config ipsec	모든 변환 세트의 컨피그레이션을 표시합니다.
crypto map set transform-set	암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
crypto dynamic-map set transform-set	동적 암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.
show running-config crypto dynamic-map	동적 암호화 맵 컨피그레이션을 표시합니다.

crypto ipsec ikev1 transform-set mode transport

IPsec IKEv1 연결을 위한 전송 모드를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto ipsec ikev1 transform-set mode transport** 명령을 사용합니다. 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto ipsec ikev1 transform-set *transform-set-name* **mode {transport}**

no crypto ipsec ikev1 transform-set *transform-set-name* **mode** {**transport}**

구문 설명

transform-set-name	수정하는 변환 세트의 이름. 이미 컨피그레이션에 있는 변환 세트를 보려면 **show running-config ipsec** 명령을 입력합니다.

기본값

전송 모드의 기본 설정은 disabled입니다. IPsec은 네트워크 터널 모드를 사용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	이 명령을 다시 작성했습니다.
8.4(1)	**ikev1** 키워드가 추가되었습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

기본 네트워크 터널 모드 대신 IPsec에 대해 호스트-호스트 전송 모드를 지정하려면 **crypto ipsec ikev1 transform-set mode transport** 명령을 사용합니다.

예

다음 명령은 사용 가능한 모든 암호화 및 인증 옵션을 보여줍니다. 암호화 및 인증을 지정하지 않는 것은 제외됩니다.

```
ciscoasa(config)# crypto ipsec ikev1 transform-set
ciscoasa(config)#
```

관련 명령

명령	설명
show running-config ipsec	모든 변환 세트의 컨피그레이션을 표시합니다.
crypto map set transform-set	암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
crypto dynamic-map set transform-set	동적 암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.
show running-config crypto dynamic-map	동적 암호화 맵 컨피그레이션을 표시합니다.

10 장

crypto isakmp disconnect-notify through cxsc auth-proxy port 명령

crypto isakmp disconnect-notify

피어에 대한 연결 종료 알림을 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp disconnect-notify** 명령을 사용합니다. 연결 종료 알림을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본값은 disabled입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp disconnect-notify** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp disconnect-notify** 명령이 **isakmp disconnect-notify** 명령을 대체했습니다**.**
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

다음과 같은 삭제 사유를 사용하여 피어에 대한 연결 종료 알림을 활성화할 수 있습니다.

- IKE_DELETE_RESERVED = 0
  잘못된 코드입니다. 보내지 마십시오.
- IKE_DELETE_BY_ERROR = 1
  keepalive에 대한 응답 또는 그 밖의 IKE 패킷 ACK를 기다리는 동안 시간 초과 또는 장애로 인해 전송 오류가 발생했습니다. 기본 텍스트는 "Connectivity to client lost"입니다.
- IKE_DELETE_BY_USER_COMMAND = 2
  사용자 또는 관리자가 직접 개입하여 SA를 삭제했습니다. 기본 텍스트는 "Manually Disconnected by Administrator"입니다.
- IKE_DELETE_BY_EXPIRED_LIFETIME = 3
  SA가 만료되었습니다. 기본 텍스트는 "Maximum Configured Lifetime Exceeded"입니다.
- IKE_DELETE_NO_ERROR = 4
  알 수 없는 오류로 인해 삭제되었습니다.
- IKE_DELETE_SERVER_SHUTDOWN = 5
  서버가 종료되고 있습니다.

- IKE_DELETE_SERVER_IN_FLAMES = 6
  서버에 심각한 문제가 있습니다. 기본 텍스트는 "Peer is having heat problems"입니다.
- IKE_DELETE_MAX_CONNECT_TIME = 7
  활성 터널의 최대 허용 시간이 지났습니다. 이 사유는 EXPIRED_LIFETIME과 달리 해당 SA뿐 아니라 IKE 협상/제어 터널 전체가 연결 종료됨을 나타냅니다. 기본 텍스트는 "Maximum Configured Connection Time Exceeded"입니다.
- IKE_DELETE_IDLE_TIMEOUT = 8
  터널이 최대 허용 시간 동안 유휴 상태였습니다. 따라서 이 SA뿐 아니라 IKE 협상 터널 전체가 연결 종료되었습니다. 기본 텍스트는 "Maximum Idle Time for Session Exceeded"입니다.
- IKE_DELETE_SERVER_REBOOT = 9
  서버가 재부팅됩니다.
- IKE_DELETE_P2_PROPOSAL_MISMATCH = 10
  Phase2 제안이 일치하지 않습니다.
- IKE_DELETE_FIREWALL_MISMATCH = 11
  방화벽 매개변수가 일치하지 않습니다.
- IKE_DELETE_CERT_EXPIRED = 12
  사용자 인증이 필요합니다. 기본 메시지는 "User or Root Certificate has Expired"입니다.
- IKE_DELETE_CLIENT_NOT_ALLOWED = 13
  허용되지 않는 클라이언트 유형 또는 버전입니다.
- IKE_DELETE_FW_SERVER_FAIL = 14
  Zone Integrity Server에 연결하지 못했습니다.
- IKE_DELETE_ACL_ERROR = 15
  AAA에서 다운로드한 ACL을 삽입할 수 없습니다. 기본 메시지는 "ACL parsing error"입니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 피어에 대한 연결 종료 알림을 활성화합니다.

```
ciscoasa(config)# crypto isakmp disconnect-notify
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp identity

피어에 보낼 1단계 ID를 설정하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp identity** 명령을 사용합니다. 기본 설정으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

crypto isakmp identity {address | hostname | key-id *key-id-string* **| auto}**

no crypto isakmp identity {address | hostname | key-id *key-id-string* **| auto}**

구문 설명

address	ISAKMP ID 정보를 교환하는 호스트의 IP 주소를 사용합니다.
auto	연결 유형별로 ISAKMP 협상을 결정합니다. 사전 공유 키는 IP 주소, 인증서 인증은 인증서 DN입니다.
hostname	ISAKMP ID 정보를 교환하는 호스트의 FQND(fully qualified domain name)을 사용합니다. 이 이름은 호스트 이름과 도메인 이름으로 구성됩니다.
key-id *key_id_string*	원격 피어에서 사전 공유 키를 조회할 때 사용하는 문자열을 지정합니다.

기본값

기본 ISAKMP ID는 **crypto isakmp identity auto**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp identity** 명령을 도입했습니다.
7.2(1)	**crypto isakmp identity** 명령이 **isakmp identity** 명령을 대체했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 연결 유형에 따라 IPsec 피어와의 통신을 위해 인터페이스에서 ISAKMP 협상을 활성화합니다.

```
ciscoasa(config)# crypto isakmp identity auto
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp nat-traversal

전역에서 NAT 통과를 활성화하려면 글로벌 컨피그레이션 모드에서 ISAKMP가 활성화되었는지(**crypto isakmp enable** 명령으로 활성화) 확인합니다. NAT 통과를 비활성화하려면 이 명령의 the **no** 형식을 사용합니다.

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

구문 설명

natkeepalive	NAT keep alive 간격을 10초~3600초 범위에서 설정합니다. 기본값은 20초입니다.

기본값

기본적으로 NAT 통과는 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp nat-traversal** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp nat-traversal** 명령이 **isakmp nat-traversal** 명령을 대체했습니다.
8.0(2)	기본적으로 NAT 통과가 활성화되어 있습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

PAT를 포함한 NAT는 IPsec도 쓰이는 여러 네트워크에서 사용되지만, 여러 가지 비호환성 때문에 IPsec 패킷이 NAT 디바이스를 통과하지 못합니다. NAT 통과 시 ESP 패킷이 하나 이상의 NAT 디바이스를 지날 수 있습니다.

ASA는 IETF "IPsec 패킷의 UDP 캡슐화" 초안 버전 2와 버전 3(http://www.ietf.org/html.charters/ipsec-charter.html)에 기술된 대로 NAT 통과를 지원하며, 동적 및 고정 암호화 맵 모두에서 NAT 통과를 지원합니다.

이 명령은 ASA의 전역에서 NAT-T를 활성화합니다. crypto-map 엔트리에서 비활성화하려면 **crypto map set nat-t-disable** 명령을 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 ISAKMP를 활성화한 다음 keepalive 간격을 30초로 하여 NAT 통과를 설정합니다.

```
ciscoasa(config)# crypto isakmp enable
ciscoasa(config)# crypto isakmp nat-traversal 30
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp policy authentication

IKE 정책 내에서 인증 방법을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp policy authentication** 명령을 사용합니다. ISAKMP 인증 방법을 제거하려면 해당 **clear configure** 명령을 사용합니다.

crypto isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

구문 설명

crack	IKE CRACK을 인증 방법으로 지정합니다.
pre-share	사전 공유 키를 인증 방법으로 지정합니다.
priority	IKE 정책을 고유하게 식별하고 해당 정책에 우선순위를 부여합니다. 1~65,534의 정수를 사용합니다. 1이면 우선순위가 가장 높고 65,534는 가장 낮습니다.
rsa-sig	RSA 서명을 인증 방법으로 지정합니다. RSA 서명은 IKE 협상에 대해 부인 방지(non-repudiation) 기능을 수행합니다. 즉 근본적으로 피어와의 IKE 협상이 있는지 여부를 제3자에게 입증할 수 있습니다.

기본값

기본 ISAKMP 정책 인증은 **pre-share**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp policy authentication** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp policy authentication** 명령이 **isakmp policy authentication** 명령을 대체했습니다**.**

사용 지침

IKE 정책은 IKE 협상을 위한 매개변수의 집합을 정의합니다.

RSA 서명을 지정할 경우 ASA와 그 피어에서 CA 서버의 인증서를 받도록 구성해야 합니다. 사전 공유 키를 지정할 경우 ASA와 그 피어 내에서 이 사전 공유 키를 각각 구성해야 합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 **crypto isakmp policy authentication** 명령을 사용하는 방법을 보여줍니다. 이 예에서는 우선순위 번호가 40인 IKE 정책에 사용할 인증 방법으로 RSA 서명을 설명합니다.

```
ciscoasa(config)# crypto isakmp policy 40 authentication rsa-sig
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp policy encryption

IKE 정책 내에서 사용할 암호화 알고리즘을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp policy encryption** 명령을 사용합니다. 암호화 알고리즘을 기본값인 **des**로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

crypto isakmp policy *priority* **encryption** {**aes | aes-192 | aes-256 | des | 3des**}

no crypto isakmp policy *priority* **encryption** {**aes | aes-192 | aes-256 | des | 3des**}

구문 설명

3des	Triple DES 암호화 알고리즘을 IKE 정책에 사용하도록 지정합니다.
aes	IKE 정책에 사용할 암호화 알고리즘을 128비트 키의 AES로 지정합니다.
aes-192	IKE 정책에 사용할 암호화 알고리즘을 192비트 키의 AES로 지정합니다.
aes-256	IKE 정책에 사용할 암호화 알고리즘을 256비트 키의 AES로 지정합니다.
des	IKE 정책에 사용할 암호화 알고리즘을 56비트 DES-CBC로 지정합니다.
priority	IKE 정책을 고유하게 식별하고 해당 정책에 우선순위를 부여합니다. 1~65,534의 정수를 사용합니다. 1이면 우선순위가 가장 높고 65,534는 가장 낮습니다.

기본값

기본 ISAKMP 정책 암호화는 **3des**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp policy encryption** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp policy encryption** 명령이 **isakmp policy encryption** 명령을 대체했습니다**.**

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 **crypto isakmp policy encryption** 명령의 사용을 보여줍니다. 여기서는 우선순위 번호가 25인 IKE 정책 내에서 사용할 알고리즘으로 128비트 키 AES 암호화를 설정합니다.

```
ciscoasa(config)# crypto isakmp policy 25 encryption aes
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 우선순위 번호가 40인 IKE 정책 내에서 사용할 3DES 알고리즘을 설정합니다.

```
ciscoasa(config)# crypto isakmp policy 40 encryption 3des
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp policy group

IKE 정책에 대해 Diffie-Hellman(DH) 그룹을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp policy group** 명령을 사용합니다. DH 그룹 식별자를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

crypto isakmp policy *priority* **group** {**1** | **2** | **5**}

no crypto isakmp policy *priority* **group**

구문 설명

group 1	768비트 DH 그룹을 IKE 정책에 사용하도록 지정합니다. 이는 기본값입니다.
group 2	1024비트 DH 그룹 2를 IKE 정책에 사용하도록 지정합니다.
group 5	1536비트 DH 그룹 5를 IKE 정책에 사용하도록 지정합니다.
priority	IIKE 정책을 고유하게 식별하고 해당 정책에 우선순위를 부여합니다. 1~65,534의 정수를 사용합니다. 1이면 우선순위가 가장 높고 65,534는 가장 낮습니다.

기본값

기본 그룹 정책은 group 2입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp policy group** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp policy group** 명령이 **isakmp policy group** 명령을 대체했습니다**.**
8.0(4)	**group 7** 명령 옵션은 더 이상 사용되지 않습니다. 그룹 7을 구성하려고 시도하면 오류 메시지가 생성되고 그룹 5가 대신 사용됩니다.

사용 지침

IKE 정책에서는 IKE 협상 과정에 사용할 매개변수의 집합을 정의합니다.

768비트(DH 그룹 1), 1024비트(DH 그룹 2), 1536비트(DH 그룹 5)의 3가지 그룹 옵션이 있습니다. 1024비트 및 1536비트 DH 그룹은 더 강력한 보안을 제공하지만 더 많은 CPU 시간이 필요합니다.

참고 Cisco VPN Client Version 3.x 이상은 ISAKMP 정책에서 DH 그룹 2를 사용해야 합니다. DH 그룹 1을 구성할 경우 Cisco VPN Client는 연결되지 않습니다.

AES는 VPN-3DES 라이센스가 있는 ASA에서만 사용할 수 있습니다. AES에서 제공하는 키가 크기 때문에 ISAKMP 협상에서는 DH 그룹 1 또는 그룹 2 대신 그룹 5를 사용해야 합니다. 그룹 5를 구성하려면 **crypto isakmp policy priority group 5** 명령을 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 **crypto isakmp policy group** 명령을 사용하는 방법을 보여줍니다. 이 예에서는 우선순위 번호가 40인 IKE 정책에 그룹 2, 1024비트 DH를 사용하도록 설정합니다.

```
ciscoasa(config)# crypto isakmp policy 40 group 2
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp policy hash

IKE 정책을 위한 해시 알고리즘을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp policy hash** 명령을 사용합니다. 해시 알고리즘을 기본값인 SHA-1로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

crypto isakmp policy *priority* **hash** {**md5** | **sha**}

no crypto isakmp policy *priority* **hash**

구문 설명

md5	MD5(HMAC variant)를 IKE 정책의 해시 알고리즘으로 지정합니다.
priority	정책을 고유하게 식별하고 우선순위를 부여합니다. 1~65,534의 정수를 사용합니다. 1이면 우선순위가 가장 높고 65,534는 가장 낮습니다.
sha	SHA-1(HMAC variant)을 IKE 정책의 해시 알고리즘으로 지정합니다.

기본값

기본 해시 알고리즘은 SHA-1 (HMAC variant)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp policy hash** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp policy hash** 명령이 **isakmp policy hash** 명령을 대체했습니다**.**

사용 지침

IKE 정책에서는 IKE 협상 과정에 사용할 매개변수의 집합을 정의합니다.

SHA-1과 MD5의 2가지 해시 알고리즘 옵션이 있습니다. MD5는 다이제스트가 더 작으며, SHA-1보다 약간 더 빠르다고 알려져 있습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 **crypto isakmp policy hash** 명령을 사용하는 방법을 보여줍니다. 이 예에서는 우선순위 번호가 40인 IKE 정책에 대해 MD5 해시 알고리즘을 지정합니다.

```
ciscoasa(config)# crypto isakmp policy 40 hash md5
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp policy lifetime

IKE 보안 연결이 만료되기 전의 수명을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp policy lifetime** 명령을 사용합니다. 보안 연결 수명을 기본값인 86,400초(1일)로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

crypto isakmp policy *priority* **lifetime** *seconds*

no crypto isakmp policy *priority* **lifetime**

구문 설명

priority	IKE 정책을 고유하게 식별하고 해당 정책에 우선순위를 부여합니다. 1~65,534의 정수를 사용합니다. 1이면 우선순위가 가장 높고 65,534는 가장 낮습니다.
seconds	각 보안 연결이 얼마 후에 만료되는지 초 단위로 지정합니다. 유한 수명을 제안하려면 120초~2147483647초 범위의 정수를 사용합니다. 무한 수명으로 하려면 0초를 사용합니다.

기본값

기본값은 86,400초(1일)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp policy lifetime** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp policy lifetime** 명령이 **isakmp policy lifetime** 명령을 대체했습니다**.**

사용 지침

IKE에서 협상을 시작할 때 해당 세션의 보안 매개변수에 대한 합의를 구합니다. 그러면 각 피어의 보안 연결에서 이 합의된 매개변수를 참조합니다. 피어는 보안 연결의 수명이 끝날 때까지 보안 연결을 유지합니다. 피어가 수명을 제안하지 않을 경우 무한 수명을 지정할 수 있습니다. 보안 연결이 만료되기 전에 후속 IKE 협상에서 이를 사용할 수 있습니다. 그러면 신규 IPsec 보안 연결을 설정할 때 시간이 절약될 수 있습니다. 피어는 현재 보안 연결이 만료되기 전에 새로운 보안 연결을 협상합니다.

보안 연결의 수명이 길수록 ASA는 더 신속하게 향후 IPsec 보안 연결을 설정합니다. 암호화 강도는 (몇 분에 불과한) 극히 짧은 rekey 시간을 사용하지 않고도 보안을 보장할 정도로 양호합니다. 기본값을 적용하는 것이 좋습니다.

참고 IKE 보안 연결이 무한 수명으로 설정되었지만 피어에서 유한 수명을 제한할 경우 피어에서 협상된 유한 수명이 사용됩니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 우선순위 번호가 40인 IKE 정책에 대해 IKE 보안 연결의 수명을 50,4000초(14시간)로 설정합니다.

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 50400
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 IKE 보안 연결을 무한 수명으로 설정합니다.

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 0
```

관련 명령

clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto isakmp reload-wait

ASA를 재부팅하기 전에 모든 활성 세션이 자동으로 종료할 때까지 기다리게 하려면 글로벌 컨피그레이션 모드에서 **crypto isakmp reload-wait** 명령을 사용합니다. 활성 세션의 종료를 기다리지 않고 ASA의 재부팅을 진행하려면 이 명령의 **no** 형식을 사용합니다.

crypto isakmp reload-wait

no crypto isakmp reload-wait

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**isakmp reload-wait** 명령을 도입했습니다.
7.2.(1)	**crypto isakmp reload-wait** 명령이 **isakmp reload-wait** 명령을 대체했습니다**.**
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 ASA에게 재부팅하기 전에 모든 활성 세션이 종료할 때까지 기다리도록 지시합니다.

```
ciscoasa(config)# crypto isakmp reload-wait
```

관련 명령

명령	설명
clear configure crypto isakmp	모든 ISAKMP 컨피그레이션을 지웁니다.
clear configure crypto isakmp policy	모든 ISAKMP 정책 컨피그레이션을 지웁니다.
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 컨피그레이션을 표시합니다.

crypto key generate rsa

ID 인증서를 위한 RSA 키 쌍을 생성하려면 글로벌 컨피그레이션 모드에서 **crypto key generate rsa** 명령을 사용합니다.

crypto key generate rsa [usage-keys | general-keys] [label *key-pair-label***] [modulus** *size***] [noconfirm] dsa [label name | elliptic-curve [256 | 384 | 521]**

구문 설명

dsa [**label name**]	키 쌍을 생성할 때 Suite B EDCSA 알고리즘을 사용합니다.
elliptic-curve [**256** | **384** | **521**]	키 쌍을 생성할 때 Suite B EDCSA 알고리즘을 사용합니다.
general-keys	범용 키 쌍 하나를 생성합니다. 이것이 기본 키 쌍 유형입니다.
label *key-pair-label*	키 쌍과 연결할 이름을 지정합니다. 이 키 쌍은 고유한 레이블이 지정되어야 합니다. 동일한 레이블로 다른 키 쌍을 생성하려 하면 ASA는 경고 메시지를 표시합니다. 키가 생성될 때 어떤 레이블도 제공되지 않으면 그 키 쌍은 Default-RSA-Key라는 고정 이름을 갖습니다.
modulus *size*	키 쌍의 모듈러스 크기를 512, 768, 1024, 2048로 지정합니다. 기본 모듈러스 크기는 1024입니다.
noconfirm	모든 대화형 프롬프트를 억제합니다.
usage-keys	2개의 키 쌍(서명용 1개, 암호화용 1개)을 생성합니다. 즉 동일한 ID에 대해 2개의 인증서가 필요합니다.

기본값

기본 키 쌍 유형은 **general key**입니다. 기본 모듈러스 크기는 1024입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

SSL, SSH, IPsec 연결을 지원하기 위해 RSA 키 상을 생성하는 데 **crypto key generate rsa** 명령을 사용합니다. 생성된 키 쌍은 명령 구문의 일부로 제공할 수 있는 레이블에 의해 식별됩니다. 키 쌍을 참조하지 않는 신뢰 지점은 기본값인 Default-RSA-Key를 사용할 수 있습니다. SSH 연결은 항상 이 키를 사용합니다. 이는 SSL에 영향을 주지 않습니다. 신뢰 지점에서 구성되지 않는 한 SSL은 자체 인증서 또는 키를 동적으로 생성하기 때문입니다.

참고 키 쌍을 저장하는 NVRAM 공간의 크기는 ASA 플랫폼에 따라 달라집니다. 생성하는 키 쌍이 30개를 초과하면 한계에 도달할 수 있습니다.

참고 4096비트 RSA 키는 ASA5580, 5585 또는 그 이상의 플랫폼에서만 지원됩니다.

주의 RSA 키 쌍이 1024비트를 초과하는 ID 인증서를 사용하는 SSL 연결 중 상당수는 ASA 및 거부된 클라이언트리스(clientless) 로그인에서 CPU 사용량이 많아질 수 있습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 mypubkey라는 레이블로 RSA 키 쌍을 생성합니다.

```
ciscoasa(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 실수로 mypubkey라는 레이블을 사용하여 중복되는 RSA 키 쌍을 생성하려고 합니다.

```
ciscoasa(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 기본 레이블로 RSA 키 쌍을 생성합니다.

```
ciscoasa(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 RSA 키 쌍을 저장하기에 충분한 공간이 없어 경고 메시지를 생성합니다.

```
ciscoasa(config)# crypto key generate rsa label mypubkey mod 2048
INFO: The name for the keys will be: mypubkey
Keypair generation process begin. Please wait...
NV RAM will not have enough space to save keypair mypubkey. Remove any unnecessary
keypairs and save the running config before using this keypair.
ciscoasa(config)#
```

관련 명령

명령	설명
crypto key zeroize	RSA 키 쌍을 제거합니다.
show crypto key	RSA 키 쌍을 표시합니다.

crypto key zeroize

표시된 유형(rsa 또는 dsa)의 키 쌍을 제거하려면 글로벌 컨피그레이션 모드에서 **crypto key zeroize** 명령을 사용합니다.

crypto key zeroize {rsa | dsa} [label *key-pair-label***] [default] [noconfirm]**

구문 설명

default	레이블이 없는 RSA 키 쌍을 제거합니다. 이 키워드는 RSA 키 쌍과 함께 사용할 때만 허용됩니다.
dsa	DSA를 키 유형으로 지정합니다.
label *key-pair-label*	표시된 유형(**rsa** 또는 **dsa**)의 키 쌍을 제거합니다. 레이블을 제공하지 않을 경우 ASA는 표시된 유형의 키 쌍을 모두 제거합니다.
noconfirm	모든 대화형 프롬프트를 억제합니다.
rsa	RSA를 키 유형으로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 모든 RSA 키 쌍을 제거합니다.

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
ciscoasa(config)#
```

관련 명령

명령	설명
crypto key generate dsa	ID 인증서를 위해 DSA 키 쌍을 생성합니다.
crypto key generate rsa	ID 인증서를 위해 RSA 키 쌍을 생성합니다.

crypto large-cert-acceleration enable

ASA가 하드웨어에서 2048비트 RSA 키 작업을 수행할 수 있게 하려면 글로벌 컨피그레이션 모드에서 **crypto large-cert-acceleration enable** 명령을 사용합니다. 소프트웨어에서 2048비트 RSA 키 작업을 수행하려면 **no crypto large-cert-acceleration enable** 명령을 사용합니다.

crypto large-cert-acceleration enable

no crypto large-cert-acceleration enable

구문 설명

이 명령은 키워드 또는 인수가 없습니다.

기본값

기본적으로 2048비트 RSA 키 작업은 소프트웨어에서 수행됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(3)	이 명령을 도입했습니다.

사용 지침

이 명령은 ASA 5510, ASA 5520, ASA 5540, 5550에서만 사용할 수 있습니다. 이 명령은 ASA 5580에서 사용할 수 없습니다.

예

다음 예에서는 2048비트 RSA 키 작업이 하드웨어에서 활성화되었음을 보여줍니다.

```
ciscoasa (config)# show running-config crypto large-cert-acceleration
crypto large-cert-acceleration enable
ciscoasa (config)#
```

관련 명령

명령	설명
clear configure crypto	나머지 crypto 컨피그레이션과 함께 2048비트 RSA 키 컨피그레이션을 지웁니다.
show running-config crypto	나머지 crypto 컨피그레이션과 함께 2048비트 RSA 키 컨피그레이션을 표시합니다.

crypto map interface

이미 정의된 암호화 맵 세트를 인터페이스에 적용하려면 글로벌 컨피그레이션 모드에서 **crypto map interface** 명령을 사용합니다. 인터페이스에서 암호화 맵 세트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

no crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

구문 설명

interface-name	ASA에서 VPN 피어와의 터널을 설정하는 데 사용할 인터페이스를 지정합니다. ISAKMP가 활성화되어 있고 CA를 사용하여 인증서를 취득하는 경우, 이는 CA 인증서에 지정된 주소의 인터페이스가 되어야 합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
ipv6-local-address *ipv6-address*	IPv6 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.3(1)	**ipv6-local-address** 키워드를 추가했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

임의의 활성 ASA 인터페이스에 암호화 맵 세트를 지정하려면 이 명령을 사용합니다. ASA는 임의의 또는 모든 활성 인터페이스에서 IPSec 종료를 지원합니다. 인터페이스에서 IPsec 서비스를 제공하려면 먼저 이 인터페이스에 암호화 맵 세트를 지정해야 합니다.

하나의 인터페이스에 암호화 맵 세트를 하나만 지정할 수 있습니다. 여러 암호화 맵 엔트리가 맵 이름이 동일하지만 순차 번호가 다를 경우, 이는 동일한 세트의 구성원이므로 모두 인터페이스에 적용됩니다. ASA에서는 순차 번호가 가장 낮은 임호 맵 엔트리를 가장 먼저 평가합니다.

인터페이스에 여러 개의 IPv6 주소가 구성된 가운데 IPv6 환경에서 LAN-to-LAN VPN 터널을 지원하도록 ASA를 구성하는 경우에는 **ipv6-local-address** 키워드를 사용합니다.

참고 ASA에서는 암호화 맵, 동적 맵, IPsec 설정을 즉시 변경할 수 있습니다. 그럴 경우 ASA는 변경이 적용되는 연결만 종료합니다. 액세스 목록에서 엔트리를 삭제하는 방법으로 암호화 맵과 연결된 기존 액세스 목록을 변경할 경우, 해당 연결만 종료됩니다. 액세스 목록의 다른 엔트리를 기반으로 한 연결은 영향을 받지 않습니다.

모든 고정 암호화 맵은 액세스 목록(access list), 변환 세트(transform set), IPsec 피어의 세 부분을 정의해야 합니다. 그중 하나라도 없으면 암호화 맵은 불완전하며, ASA는 다음 엔트리로 진행합니다. 그러나 암호화 맵이 액세스 목록과 매칭하지만 나머지 두 요구 사항 중 하나 또는 둘 다와 매칭하지 않을 경우 이 ASA는 트래픽을 폐기합니다.

모든 암호화 맵이 완전함을 확인하려면 **show running-config crypto map** 명령을 사용합니다. 불완전한 암호화 맵을 수정하려면 그 암호화 맵을 제거하고 누락된 엔트리를 추가한 다음 다시 적용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 외부 인터페이스에 mymap이라는 이름의 암호화 맵 세트를 지정합니다. 트래픽이 외부 인터페이스를 지날 때 ASA는 mymap 세트에 있는 모든 암호화 맵 엔트리를 사용하여 이 트래픽을 평가합니다. mymap 암호화 맵 엔트리 중 하나에서 아웃바운드 트래픽이 액세스 목록과 매칭하면 ASA는 그 암호화 맵 엔트리의 컨피그레이션을 사용하여 보안 연결을 생성합니다.

```
ciscoasa(config)# crypto map mymap interface outside
```

다음 예에서는 최소한 필요한 암호화 맵 컨피그레이션을 보여줍니다.

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap set transform-set my_t_set1
ciscoasa(config)# crypto map mymap set peer 10.0.0.1
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map ipsec-isakmp dynamic

특정 암호화 맵 엔트리에서 기존의 동적 암호화 맵을 반드시 참조하게 하려면 글로벌 컨피그레이션 모드에서 **crypto map ipsec-isakmp dynamic** 명령을 사용합니다. 상호 참조를 제거하려면 이 명령의 **no** 형식을 사용합니다.

동적 암호화 맵 엔트리를 만들려면 **crypto dynamic-map** 명령을 사용합니다. 동적 암호화 맵 세트를 만든 다음 **crypto map ipsec-isakmp dynamic** 명령을 사용하여 고정 암호화 맵에 동적 암호화 맵 세트를 추가합니다.

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

구문 설명

dynamic-map-name	기존 동적 암호화 맵을 참조하는 암호화 맵 엔트리의 이름을 지정합니다.
ipsec-isakmp	IKE에서 이 암호화 맵 엔트리에 대한 IPsec 보안 연결을 설정함을 나타냅니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 수정하여 **ipsec-manual** 키워드를 제거했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

암호화 맵 엔트리를 정의한 다음 **crypto map interface** 명령을 사용하여 인터페이스에 동적 암호화 맵 세트를 지정할 수 있습니다.

동적 암호화 맵은 2가지 기능, 즉 보호할 트래픽을 필터링/분류하는 기능과 트래픽에 적용할 정책을 정의하는 기능을 제공합니다. 전자는 인터페이스의 트래픽 흐름에, 후자는 그 트래픽을 위해 (IKE를 통해) 수행되는 협상에 적용됩니다.

IPsec 동적 암호화 맵에서는 다음을 식별합니다.

- 보호할 트래픽
- 보안 연결을 설정할 IPsec 피어
- 보호받는 트래픽과 함께 사용할 변환 세트
- 키와 보안 연결을 사용하거나 관리하는 방법

암호화 맵 세트는 암호화 맵 엔트리의 모음이며, 각 엔트리는 서로 다른 순차 번호(*seq-num*)를 갖지만 맵 이름은 동일합니다. 따라서 어떤 인터페이스에서 특정 트래픽을 그 트래픽에 적용되는 보안과 함께 어떤 피어에 전달하고, 또 다른 트래픽은 다른 IPsec 보안을 적용하면서 동일한 피어에 또는 다른 피어에 전달하는 것이 가능합니다. 그러기 위해서는 2개의 암호화 맵 엔트리를 만듭니다. 이들의 맵 이름은 동일하지만 순차 번호는 서로 다릅니다.

임의의 번호를 *seq-num* 인수로 지정해서는 안 됩니다. 이 번호는 어떤 암호화 맵 세트에 속한 여러 암호화 맵 엔트리의 순서를 결정합니다. 순차 번호가 낮은 암호화 맵 엔트리는 순차 번호가 높은 암호화 맵 엔트리보다 먼저 평가됩니다. 즉 번호가 낮을수록 우선순위가 높습니다.

참고 암호화 맵을 동적 암호화 맵에 연결할 때 동적 암호화 맵을 지정해야 합니다. 그러면 암호화 맵이 앞서 **crypto dynamic-map** 명령으로 정의되었던 기존 동적 암호화 맵에 연결됩니다. 이제는 암호화 맵이 변환된 후 변경한 어떤 사항도 적용되지 않습니다. 예를 들어 피어 설정을 변경했어도 적용되지 않습니다. 그러나 ASA는 시스템이 켜져 있는 동안 변경된 사항을 저장합니다. 동적 암호화 맵이 암호화 맵으로 다시 변환되면 변경 사항이 적용되며 **show running-config crypto map** 명령의 출력에 나타납니다. ASA는 재부팅할 때까지 이 설정을 유지합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 명령은 암호화 맵 mymap이 test라는 동적 암호화 맵을 참조하도록 구성합니다.

```
ciscoasa(config)# crypto map mymap ipsec-isakmp dynamic test
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map match address

암호화 맵 엔트리에 액세스 목록을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map match address** 명령을 사용합니다. 암호화 맵 엔트리에서 액세스 목록을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

구문 설명

acl_name	암호화 액세스 목록의 이름을 지정합니다. 이 이름이 매칭 대상인 명명된 암호화 액세스 목록의 name 인수와 같아야 합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 모든 고정 암호화 맵에 필요합니다. 동적 암호화 맵을 정의하는 경우(**crypto dynamic-map** 명령 사용), 이 명령이 꼭 필요하지는 않지만 사용하는 것이 좋습니다.

액세스 목록을 정의하려면 **access-list** 명령을 사용합니다. 액세스 제어 목록 수는 터널이 시작할 때만 증가합니다. 터널이 시작한 후에는 패킷 흐름당 히트 수는 증가하지 않습니다. 터널이 종료되었다가 다시 시작하면 히트 수는 증가합니다.

ASA에서는 IPsec 암호로 보호할 트래픽과 보호가 필요 없는 트래픽을 구별하는 데 액세스 목록을 사용합니다. 허용 ACE와 매칭하는 아웃바운드 패킷을 보호하며, 허용 ACE와 매칭하는 인바운드 패킷이 보호받음을 확인합니다.

ASA에서 어떤 패킷을 거부 구문과 매칭할 때, 암호화 맵의 나머지 ACE를 사용하는 패킷 검사를 건너뛰고 순차 번호상 다음 암호화 맵의 ACE를 사용하여 패킷 평가를 다시 시작합니다. *캐스케이딩 ACL*에서는 거부 ACE를 사용하여 ACL의 나머지 ACE 평가를 우회하고, 암호화 맵 세트의 다음 암호화 맵에 지정된 ACL을 사용하여 트래픽의 평가를 다시 시작합니다. 각 암호화 맵을 서로 다른 IPsec 설정과 연결하는 것이 가능하므로, 거부 ACE를 사용하여 특정 트래픽이 해당 암호화 맵에서 더 이상 평가받지 않고 다른 암호화 맵의 허용 구문과 매칭하게 함으로써 다양한 보안을 제공하거나 요구할 수 있습니다.

참고 암호화 액세스 목록은 인터페이스를 지나는 트래픽을 허용하거나 거부할지 여부를 결정하지 않습니다. **access-group** 명령으로 인터페이스에 직접 적용된 액세스 목록에 의해 결정됩니다.

투명 모드에서는 수신 주소가 관리 주소인 ASA의 IP 주소가 되어야 합니다. 투명 모드에서는 ASA에 대한 터널만 허용됩니다.

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set connection-type

이 암호화 맵 엔트리의 백업 사이트 대 사이트 기능을 위해 연결 유형을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set connection-type** 명령을 사용합니다. 기본 설정으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

no crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

구문 설명

answer-only	초기의 전용 교환 과정에서 연결 대상으로 적합한 피어를 찾기 위해 먼저 인바운드 IKE 연결에 응답만 하도록 지정합니다.
bidirectional	이 피어가 이 암호화 맵 엔트리 기반의 연결을 허용하고 시작할 수 있음을 나타냅니다. 이는 모든 사이트 대 사이트 연결의 기본 연결 유형입니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
originate-only	이 피어가 연결 대상으로 알맞은 피어를 찾기 위해 최초 전용 교환을 시작하도록 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.
set connection-type	이 암호화 맵 엔트리의 백업 사이트 대 사이트 기능을 위한 연결 유형을 지정합니다. answer-only, originate-only, bidirectional의 3가지 연결 유형이 있습니다.

기본값

기본 설정은 bidirectional입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0	이 명령을 도입했습니다.
9.0	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

crypto map set connection-type 명령은 백업 LAN-to-LAN 기능의 연결 유형을 지정합니다. 연결의 한 쪽에서 여러 백업 피어를 지정할 수 있게 합니다.

이 기능은 다음 플랫폼 사이에서만 사용할 수 있습니다.

- 두 Cisco ASA 5500 Series
- Cisco ASA 5500 Series와 Cisco VPN 3000 Concentrator
- Cisco ASA 5500 Series와 Cisco PIX Security Appliance Software Version 7.0 이상을 실행하는 보안 어플라이언스

백업 LAN-to-LAN 연결을 구성하려면 연결의 한 쪽은 **originate-only** 키워드를 사용하여 originate-only로 구성하고 다른 쪽은 **answer-only** 키워드를 사용하여 answer-only 다중 백업 피어로 구성하는 것이 좋습니다. originate-only 쪽에서 **crypto map set peer** 명령을 사용하여 피어의 우선 순위를 지정합니다. originate-only ASA는 목록의 첫 번째 피어와 협상을 시도합니다. 그 피어가 응답하지 않으면 ASA는 목록의 다음 피어에게 시도하며, 이는 어떤 피어가 응답하거나 목록에 더 이상 피어가 없을 때까지 계속됩니다.

이러한 컨피그레이션에서는 originate-only 피어가 처음에 전용 터널을 설정하고 피어와 협상하려고 시도합니다. 그 다음에는 양쪽 피어가 정상적인 LAN-to-LAN 연결을 설정할 수 있으며, 양쪽의 데이터에 의해 터널 연결이 시작될 수 있습니다.

투명 방화벽 모드에서는 이 명령을 볼 수 있으나, 인터페이스에 연결된 암호화 맵의 암호화 맵 엔트리에 대해 connection-type의 값이 answer-only로만 설정됩니다.

표 10-1에서 지원되는 모든 컨피그레이션을 보여줍니다. 여기에 포함되지 않은 조합은 예기치 않은 라우팅 문제를 일으킬 수 있습니다.

표 10-1 지원되는 백업 LAN-to-LAN 연결 유형

원격지	중앙
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 암호화 맵 mymap을 구성하고 connection-type을 originate-only로 설정합니다.

```
ciscoasa(config)# crypto map mymap 10 set connection-type originate-only
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set df-bit

SA(서명 알고리즘)별 DF(do-not-fragment) 정책을 설정하려면 글로벌 컨피그레이션 모드에서 **crypto map set df-bit** 명령을 사용합니다. DF 정책을 비활성화하려면 이 명령의 the **no** 형식을 사용합니다.

crypto map *name priority* **set df-bit [clear-df | copy-df | set-df]**

no crypto map *name priority* **set df-bit [clear-df | copy-df | set-df]**

구문 설명

name	암호화 맵 세트의 이름을 지정합니다.
priority	암호화 맵 엔트리에 부여하는 우선순위를 지정합니다.

기본값

기본 설정은 off입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

원래의 DF 정책 명령은 유지되며 인터페이스에서 전역 정책 설정의 역할을 하지만, 이는 SA에서 **crypto map** 명령에 의해 대체됩니다.

crypto map set ikev2 pre-shared-key

AnyConnect IKEv2 연결을 위해 사전 공유 키를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set ikev2 pre-shared-key** 명령을 사용합니다. 기본 설정으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

no crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

구문 설명

key	1자~128자의 영숫자 문자열입니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

예

다음 예에서는 사전 공유 키 SKTIWHT를 구성합니다.

```
ciscoasa(config)# crypto map crypto_map_example set ikev2 pre-shared-key SKTIWHT
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set inheritance

이 암호화 맵 엔트리에 대해 생성되는 보안 연결의 세분화(단일 또는 다중)를 설정하려면 글로벌 컨피그레이션 모드에서 **set inheritance** 명령을 사용합니다. 이 암호화 맵 엔트리의 상속 설정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set inheritance {data | rule}**

no crypto map *map-name seq-num* **set inheritance {data | rule}**

구문 설명

data	규칙에 지정된 주소 범위의 각 주소 쌍에 하나의 터널을 지정합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
rule	이 암호화 맵과 연결된 각 ACL 엔트리에 하나의 터널을 지정합니다. 이는 기본값입니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.
set inheritance	상속의 유형을 **data 또는 rule**로 지정합니다. 상속을 통해 각 SPD(보안 정책 데이터베이스)에 단일 SA(보안 연결)를 생성하거나 범위의 각 주소 쌍에 다수의 보안 SA를 생성할 수 있습니다.

기본값

기본값은 **rule**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 ASA가 터널에 응답할 때가 아니라 터널을 시작할 때에만 작동합니다. data 설정을 사용하면 수많은 IPsec SA가 생길 수 있습니다. 그러면 메모리 사용량이 늘어나 전체 터널 수가 적어집니다. 극히 보안이 중요한 애플리케이션에서만 data 설정을 사용해야 합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 암호화 맵 mymap을 구성하고 상속 유형을 data로 설정합니다.

```
ciscoasa(config)# crypto map mymap 10 set inheritance data
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set nat-t-disable

이 암호화 맵 엔트리 기반의 연결에 NAT-T를 비활성화하려면 글로벌 컨피그레이션 모드에서 **crypto map set nat-t-disable** 명령을 사용합니다. 이 암호화 맵 엔트리에 대해 NAT-T를 활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

구문 설명

map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

이 명령의 기본 설정은 not on입니다(즉 NAT-T는 기본적으로 활성화됨).

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

전역에서 NAT-T를 활성화하려면 **isakmp nat-traversal** 명령을 사용합니다. 그런 다음 **crypto map set nat-t-disable** 명령을 사용하여 특정 암호화 맵 엔트리에서 NAT-T를 비활성화할 수 있습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 명령에서는 mymap이라는 암호화 맵 엔트리에 대해 NAT-T를 비활성화합니다.

```
ciscoasa(config)# crypto map mymap 10 set nat-t-disable
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
isakmp nat-traversal	모든 연결에 대해 NAT-T를 활성화합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set peer

암호화 맵 엔트리에서 IPsec 피어를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set peer** 명령을 사용합니다. 암호화 맵 엔트리에서 IPsec 피어를 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

구문 설명

hostname	ASA **name** 명령에 의해 정의된 호스트 이름을 기준으로 피어를 지정합니다.
ip_address	IP 주소(IPv4 또는 IPv6)를 기준으로 피어를 지정합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
peer	암호화 맵 엔트리에서 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 기준으로 IPsec 피어를 지정합니다. IKEv2에 대해서는 다중 피어가 지원되지 않습니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	최대 10개의 피어 주소를 허용하도록 이 명령을 수정했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 모든 고정 암호화 맵에 필요합니다. (**crypto dynamic-map** 명령을 사용하여) 동적 암호화 맵을 정의하는 경우 이 명령은 필요하지 않습니다. 일반적으로 피어는 알려지지 않으므로 대개는 이 명령을 사용하지 않습니다.

다중 피어를 구성하는 것은 폴백(fallback) 목록을 제공하는 것과 같습니다. ASA는 각 터널에서 목록의 첫 번째 피어와 협상을 시도합니다. 그 피어가 응답하지 않으면 ASA는 목록의 다음 피어에게 시도하며, 이는 어떤 피어가 응답하거나 목록에 더 이상 피어가 없을 때까지 계속됩니다. 백업 LAN-to-LAN 기능을 사용하는 경우에만 (즉 암호화 맵 연결 유형이 originate-only일 때) 다중 피어를 설정할 수 있습니다. 자세한 내용은 **crypto map set connection-type** 명령을 참조하십시오.

참고 IKEv2에 대해서는 다중 피어가 지원되지 않습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 보안 연결을 설정하기 위해 IKE를 사용하는 암호화 맵 컨피그레이션을 보여줍니다. 이 예에서는 10.0.0.1의 피어 또는 10.0.0.2의 피어 중 하나와 보안 연결을 설정할 수 있습니다.

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap 10 set transform-set my_t_set1
ciscoasa(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set pfs

글로벌 컨피그레이션 모드에서 **crypto map set pfs** 명령을 사용하여 이 암호화 맵 엔트리에 대해 새 보안 연결을 요청할 때 IPsec에서 PFS를 요청하도록 설정합니다. 그렇지 않으면 새 보안 연결에 대한 요청을 받을 때 IPsec에서 PFS를 필요로 합니다. IPsec에서 PFS를 요청하지 않도록 지정하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24]**

구문 설명

group1	IPsec에서 새 DH 교환을 수행할 때 768비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group2	IPsec에서 새 DH 교환을 수행할 때 1024비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group5	IPsec에서 새 DH 교환을 수행할 때 1536비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

기본적으로 PFS는 설정되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	DH 그룹 7을 추가하기 위해 이 명령을 수정했습니다.
8.0(4)	**group 7** 명령 옵션은 더 이상 사용되지 않습니다. 그룹 7을 구성하려고 시도하면 오류 메시지가 생성되고 그룹 5가 대신 사용됩니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

PFS를 사용하면 새 보안 연결이 협상될 때마다 새 DH 교환이 일어나며, 따라서 추가적인 처리 시간이 필요합니다. PFS는 보안을 한층 더 강화합니다. 어떤 키가 공격자에 의해 크래킹될 경우 그 키와 함께 전송된 데이터만 위험해집니다.

이 명령은 협상 과정에서 IPsec이 암호화 맵 엔트리에 대해 새 보안 연결을 요청할 때 PFS를 요청하게 합니다. **set pfs** 문에서 그룹을 지정하지 않으면 ASA는 기본값(group2)을 보냅니다.

피어가 협상을 시작하고 로컬 컨피그레이션에서 PFS를 지정할 경우 피어는 PFS 교환을 수행해야 합니다. 그렇지 않으면 협상은 실패합니다. 로컬 컨피그레이션에서 그룹을 지정하지 않을 경우 ASA는 기본값인 group2를 적용합니다. 로컬 컨피그레이션에서 group2 또는 group5를 지정할 경우 해당 그룹이 피어의 제안에 포함되어 있어야 합니다. 그렇지 않으면 협상은 실패합니다.

협상이 성공하려면 LAN-to-LAN 태널의 양쪽 끝에서 (DH 그룹과 함께 또는 DH 그룹 없이) PFS를 설정해야 합니다. 설정되면 그룹이 정확하게 일치해야 합니다. ASA에서 피어의 어떤 PFS 제안도 수락하는 것은 아닙니다.

1536비트 DH 프라임 모듈러스 그룹인 group5는 group1 또는 group2보다 더 우수한 보안을 제공하지만, 더 많은 처리 시간을 필요로 합니다.

Cisco VPN Client와 상호 작용할 때 ASA는 PFS 값을 사용하는 게 아니라 1단계에서 협상한 값을 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 암호화 맵인 mymap 10에 대해 새 보안 연결이 협상될 때마다 PFS를 사용하도록 지정합니다.

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 set pfs group2
```

관련 명령

명령	설명
clear isakmp sa	활성 IKE 보안 연결을 삭제합니다.
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.
tunnel-group	터널 그룹과 그 매개변수를 구성합니다.

crypto map set ikev1 phase1-mode

main 또는 aggressive와의 연결을 시작할 때 1단계에 대해 IKEv1 모드를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set ikev1 phase1-mode** 명령을 사용합니다. 1단계 IKEv1 협상에 대한 설정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set ikev1 phase1-mode {main | aggressive [group1 | group2 | group5]}**

no crypto map *map-name seq-num* **set ikev1 phase1-mode {main | aggressive [group1 | group2 | group5]}**

구문 설명

aggressive	1단계 IKEv1 협상에 대해 aggressive 모드를 지정합니다.
group1	IPsec에서 새 DH 교환을 수행할 때 768비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group2	IPsec에서 새 DH 교환을 수행할 때 1024비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group5	IPsec에서 새 DH 교환을 수행할 때 1536비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
main	1단계 IKEv1 협상에 대해 main 모드를 지정합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

1단계의 기본 모드는 **main**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0(4)	**group 7** 명령 옵션은 더 이상 사용되지 않습니다. 그룹 7을 구성하려고 시도하면 오류 메시지가 생성되고 그룹 5가 대신 사용됩니다.
8.4(1)	**ikev1** 키워드가 추가되었습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 responder 모드가 아닌 initiator 모드에서만 작동합니다. aggressive 모드와 함께 DH 그룹을 포함하는 것은 선택 사항입니다. 포함된 그룹이 없으면 ASA는 그룹 2를 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 암호화 맵인 mymap을 구성하고 1단계 모드를 그룹 2를 사용하여 aggressive로 설정합니다.

```
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group2
ciscoasa(config)#
```

관련 명령

명령	설명
clear isakmp sa	활성 IKE 보안 연결을 삭제합니다.
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set ikev2 phase1-mode

main 또는 aggressive와의 연결을 시작할 때 1단계에 대해 IKEv2 모드를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set ikev2 phase1-mode** 명령을 사용합니다. 1단계 IKEv2 협상에 대한 설정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set ikev2 phase1-mode {main | aggressive [group1 | group2 | group5]}**

no crypto map *map-name seq-num* **set ikev2 phase1-mode {main | aggressive [group1 | group2 | group5]}**

구문 설명

aggressive	1단계 IKEv2 협상에 대해 aggressive 모드를 지정합니다.
group1	IPsec에서 새 DH 교환을 수행할 때 768비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group2	IPsec에서 새 DH 교환을 수행할 때 1024비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
group5	IPsec에서 새 DH 교환을 수행할 때 1536비트 DH 프라임 모듈러스 그룹을 사용하도록 지정합니다.
main	1단계 IKEv2 협상에 대해 main 모드를 지정합니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

1단계의 기본 모드는 **main**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0(4)	**group 7** 명령 옵션은 더 이상 사용되지 않습니다. 그룹 7을 구성하려고 시도하면 오류 메시지가 생성되고 그룹 5가 대신 사용됩니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 responder 모드가 아닌 initiator 모드에서만 작동합니다. aggressive 모드와 함께 DH 그룹을 포함하는 것은 선택 사항입니다. 포함된 그룹이 없으면 ASA는 그룹 2를 사용합니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 암호화 맵인 mymap을 구성하고 1단계 모드를 그룹 2를 사용하여 aggressive로 설정합니다.

```
ciscoasa(config)# crypto map mymap 10 set ikev2 phase1mode aggressive group2
ciscoasa(config)#
```

관련 명령

명령	설명
clear isakmp sa	활성 IKE 보안 연결을 삭제합니다.
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set reverse-route

이 암호화 맵 엔트리를 기반으로 한 임의의 연결에 대해 반대 경로 삽입을 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto map set reverse-route** 명령을 사용합니다. 이 암호화 맵 엔트리를 기반으로 한 임의의 연결에 대해 반대 경로 삽입을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set reverse-route**

no crypto map *map-name seq-num s***et reverse-route**

구문 설명

map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.

기본값

이 명령의 기본 설정은 off입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

ASA에서는 라우팅 테이블에 고정 경로를 자동으로 추가하고, OSPF를 사용하여 사설 네트워크 또는 경계선 라우터에 이 경로를 알릴 수 있습니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서 mymap이라는 암호화 맵에 대해 반대 경로 삽입을 활성화합니다.

```
ciscoasa(config)# crypto map mymap 10 set reverse-route
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set security-association lifetime

(특정 암호화 맵 엔트리에 대해) IPsec 보안 연결 협상에 쓰이는 전역 수명 값을 재정의하려면 글로벌 컨피그레이션 모드에서 **crypto map set security-association lifetime** 명령을 사용합니다. 암호화 맵 엔트리의 수명 값을 전역 값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* **|**
kilobytes *kilobytes* **| unlimited}**

no crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* **|**
kilobytes *kilobytes* **|** *unlimited*}

구문 설명

kilobytes	어떤 보안 연결이 만료되기 전에 그 보안 연결을 사용하여 피어를 통과할 수 있는 트래픽의 볼륨(킬로바이트)을 지정합니다. 기본값은 4,608,000킬로바이트입니다.
map-name	암호화 맵 세트의 이름을 지정합니다.
seconds	보안 연결이 만료되기 전까지의 수명을 초 단위로 지정합니다. 기본값은 28,800초(8시간)입니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.
unlimited	ASA가 터널의 개시자일 때 빠른 모드 1 패킷에 Kilobytes를 보내지 않습니다.

기본값

kilobytes의 기본값은 4,608,000이고 seconds의 기본값은 28,800입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.
9.1(2)	unlimited 인수를 추가했습니다.

사용 지침

암호화 맵의 보안 연결은 전역 수명에 따라 협상됩니다.

IPsec 보안 연결에서는 공유 암호 키를 사용합니다. 이 키와 그 보안 연결은 동시에 시간 초과됩니다.

해당 암호화 맵 엔트리의 수명 값이 구성되었다고 가정하면, ASA에서 보안 연결 협상 중에 새로운 보안 연결을 요청할 때 피어에 보내는 요청에서 암호화 맵 수명의 값을 지정합니다. 이 값을 새 보안 연결의 수명으로 사용합니다. ASA에서 피어로부터 협상 요청을 받을 때, 피어에서 제안한 수명 값과 새 보안 연결의 수명으로 로컬에 구성된 수명 값 중 더 작은 값을 사용합니다.

수명에는 timed lifetime과 traffic-volume lifetime의 2가지가 있습니다. 이 수명 중 빠른 쪽에 도달하면 세션 키와 보안 연결이 만료됩니다. 하나의 명령으로 둘 다 지정할 수 있습니다.

참고 ASA에서는 암호화 맵, 동적 맵, IPsec 설정을 즉시 변경할 수 있습니다. 그럴 경우 ASA는 변경이 적용되는 연결만 종료합니다. 액세스 목록에서 엔트리를 삭제하는 방법으로 암호화 맵과 연결된 기존 액세스 목록을 변경할 경우, 해당 연결만 종료됩니다. 액세스 목록의 다른 엔트리를 기반으로 한 연결은 영향을 받지 않습니다.

timed lifetime을 변경하려면 **crypto map set security-association lifetime seconds** 명령을 사용합니다. timed lifetime은 지정된 시간(초)이 경과하면 키와 보안 연결이 시간 초과됩니다.

예

글로벌 컨피그레이션 모드에서 입력한 다음 명령에서는 암호화 맵 mymap에 대해 보안 연결의 수명을 초 및 킬로바이트 단위로 지정합니다.

```
ciscoasa(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set ikev1 transform-set

암호화 맵 엔트리에서 사용할 IKEv1 변환 세트를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set transform-set** 명령을 사용합니다. 암호화 맵 엔트리에서 변환 세트의 이름을 제거하려면 이 명령의 **no** 형식을 지정된 변환 세트 이름과 함께 사용합니다. 변환 세트를 모두 지정하거나 하나도 지정하지 않고 암호화 맵 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set**

구문 설명

map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 해당하는 순차 번호를 지정합니다.
transform-set-name1 *transform-set-name11*	변환 세트의 이름을 하나 이상 지정합니다. 이 명령에서 명명된 어떤 변환 세트도 **crypto ipsec transform-set** 명령에서 정의되어야 합니다. 각 암호화 맵 엔트리는 최대 11개의 변환 세트를 지원합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(1)	암호화 맵 엔트리에 있는 변환 세트의 최대 개수를 수정했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령은 모든 암호화 맵 엔트리에 필요합니다.

IPsec 시작의 반대쪽에 있는 피어는 처음으로 매칭하는 변환 세트를 보안 연결에 사용합니다. 로컬 ASA에서 협상을 시작할 경우, **crypto map** 명령에 지정된 순서에 따라 ASA에서 변환 세트의 내용을 피어에 전달하는 순서가 결정됩니다. 피어가 협상을 시작할 경우, 로컬 ASA는 암호화 맵 엔트리에서 피어가 보낸 IPsec 매개변수와 매칭하는 첫 번째 변환 세트를 사용합니다.

IPsec 시작의 반대쪽에 있는 피어가 변환 세트의 값과 매칭하지 않을 경우 IPsec은 보안 연결을 설정하지 않습니다. 개시자는 트래픽을 폐기합니다. 이 트래픽을 보호할 보안 연결이 없기 때문입니다.

변환 세트의 목록을 변경하려면 기존 목록을 대체할 새 목록을 지정합니다.

암호화 맵을 수정하는 데 이 명령을 사용할 경우 ASA에서는 지정된 순차 번호의 암호화 맵 엔트리만 수정합니다. 예를 들어, 다음과 같이 입력하면 ASA는 56des-sha라는 변환 세트를 마지막 위치에 삽입합니다.

```
ciscoasa(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
ciscoasa(config)# crypto map map1 1 transform-set 56des-sha
ciscoasa(config)#
```

다음 명령에 대한 응답은 앞서 실행한 두 명령의 누적된 결과를 보여줍니다.

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

암호화 맵 엔트리에서 변환 세트의 순서를 재구성하려면 맵 이름과 순차 번호를 모두 지정한 다음 다시 만듭니다. 예를 들어, 다음 명령에서는 map2라는 암호화 맵 엔트리를 sequence 3로 재구성합니다.

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

예

crypto ipsec transform-set(변환 세트 생성 또는 제거) 섹션에서는 10개의 변환 세트 명령을 보여줍니다. 다음 예에서는 동일한 10개의 변환 세트로 구성된 map2라는 암호화 맵 엔트리를 생성합니다.

```
ciscoasa(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 ASA에서 IKE를 사용하여 보안 연결을 설정할 때 최소한 필요한 암호화 맵 컨피그레이션을 보여줍니다.

```
ciscoasa(config)# crypto map map2 10 ipsec-isakmp
ciscoasa(config)# crypto map map2 10 match address 101
ciscoasa(config)# crypto map map2 set transform-set 3des-md5
ciscoasa(config)# crypto map map2 set peer 10.0.0.1
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto dynamic-map	컨피그레이션에서 모든 동적 암호화 맵을 지웁니다.
clear configure crypto map	컨피그레이션에서 모든 암호화 맵을 지웁니다.
crypto dynamic-map set transform-set	동적 암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
crypto ipsec transform-set	변환 세트를 구성합니다.
show running-config crypto dynamic-map	동적 암호화 맵 컨피그레이션을 표시합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set ikev2 ipsec-proposal

암호화 맵 엔트리에서 사용할 IKEv2 제안을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set ikev2 ipsec-proposal** 명령을 사용합니다. 암호화 맵 엔트리에서 제안의 이름을 제거하려면 이 명령의 **no** 형식을 지정된 제안 이름과 함께 사용합니다. 제안을 모두 지정하거나 하나도 지정하지 않고 암호화 맵 엔트리를 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal**

구문 설명

map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 해당하는 순차 번호를 지정합니다.
propsal-name1 *proposal-name11*	IKEv2를 위한 IPsec 제안의 이름을 하나 이상 지정합니다. 이 명령에서 명명된 어떤 제안도 **crypto ipsec ikev2 ipsec-proposal** 명령에서 정의되어야 합니다. 각 암호화 맵 엔트리는 최대 11개의 제안을 지원합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

모든 암호화 맵 엔트리에서 IKEv1 변환 세트 또는 IKEv2 제안이 필요합니다.

IPsec IKEv2 시작의 반대쪽에 있는 피어는 처음으로 매칭하는 제안을 보안 연결에 사용합니다. 로컬 ASA에서 협상을 시작할 경우, **crypto map** 명령에 지정된 순서에 따라 ASA에서 제안의 내용을 피어에 전달하는 순서가 결정됩니다. 피어가 협상을 시작할 경우, 로컬 ASA는 암호화 맵 엔트리에서 피어가 보낸 IPsec 매개변수와 매칭하는 첫 번째 제안을 사용합니다.

IPsec 시작의 반대쪽에 있는 피어가 제안의 값과 매칭하지 않을 경우 IPsec은 보안 연결을 설정하지 않습니다. 개시자는 트래픽을 폐기합니다. 이 트래픽을 보호할 보안 연결이 없기 때문입니다.

제안의 목록을 변경하려면 새 목록을 만들고 기존 목록을 대체하도록 지정합니다.

암호화 맵을 수정하는 데 이 명령을 사용할 경우 ASA에서는 지정된 순차 번호의 암호화 맵 엔트리만 수정합니다. 예를 들어, 다음과 같이 입력하면 ASA는 56des-sha라는 제안을 마지막 위치에 삽입합니다.

```
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 128aes-md5 128aes-sha
192aes-md5
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 56des-sha
ciscoasa(config)#
```

다음 명령에 대한 응답은 앞서 실행한 두 명령의 누적된 결과를 보여줍니다.

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set ipsec-proposal 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

암호화 맵 엔트리에서 제안의 순서를 재구성하려면 맵 이름과 순차 번호를 모두 지정한 다음 다시 만듭니다. 예를 들어, 다음 명령에서는 *map2*라는 암호화 맵 엔트리를 sequence 3로 재구성합니다.

```
asa2(config)# no crypto map map2 3 set ikev2 ipsec-proposal
asa2(config)# crypto map map2 3 set ikev2 ipsec-proposal 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

예

다음 예에서는 10개의 제안으로 구성된 map2라는 암호화 맵 엔트리를 만듭니다.

```
ciscoasa(config)# crypto map map2 10 set ikev2 ipsec-proposal 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto dynamic-map	컨피그레이션에서 모든 동적 암호화 맵을 지웁니다.
clear configure crypto map	컨피그레이션에서 모든 암호화 맵을 지웁니다.
crypto dynamic-map set transform-set	동적 암호화 맵 엔트리에서 사용할 변환 세트를 지정합니다.
crypto ipsec transform-set	변환 세트를 구성합니다.
show running-config crypto dynamic-map	동적 암호화 맵 컨피그레이션을 표시합니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.

crypto map set tfc-packets

IPsec SA에서 더미 TFC(Traffic Flow Confidentiality) 패킷을 활성화하려면 글로벌 컨피그레이션 모드에서 **crypto map set tfc-packets** 명령을 사용합니다. IPsec SA에서 TFC 패킷을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *name priority* **set tfc-packets [burst** *length* **|** *auto***] [payload-size** *bytes* **|** *auto***] [timeout** *second* **|** *auto***]**

no crypto map *name priority* **set tfc-packets [burst** *length* **|** *auto***] [payload-size** *bytes* **|** *auto***] [timeout** *second* **|** *auto***]**

구문 설명

name	암호화 맵 세트의 이름을 지정합니다.
priority	암호화 맵 엔트리에 부여하는 우선순위를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 암호화 맵에 대한 기존 DF 정책(SA 레벨)을 구성합니다.

crypto map set trustpoint

암호화 맵 엔트리에 대해 1단계 협상 중에 인증을 위해 보낼 인증서를 식별하는 신뢰 지점을 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set trustpoint** 명령을 사용합니다. 암호화 맵 엔트리에서 신뢰 지점을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

구문 설명

chain	(선택 사항) 인증서 체인을 보냅니다. CA 인증서 체인은 루트 인증서부터 ID 인증서까지 인증서 계층 구조에 있는 모든 CA 인증서를 포함합니다. 기본값은 disable입니다(체인 없음).
map-name	암호화 맵 세트의 이름을 지정합니다.
seq-num	암호화 맵 엔트리에 부여하는 번호를 지정합니다.
trustpoint-name	1단계 협상 중에 보낼 인증서를 식별합니다. 기본값은 none입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 암호화 맵 명령은 연결을 시작하는 데에만 유효합니다. 응답자 쪽에 대한 자세한 내용은 **tunnel-group** 명령을 참조하십시오.

예

글로벌 컨피그레이션 모드에서 입력한 다음 예에서는 암호화 맵 mymap에 대해 tpoint1이라는 신뢰 지점을 지정하고 인증서 체인을 포함시킵니다.

```
ciscoasa(config)# crypto map mymap 10 set trustpoint tpoint1 chain
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure crypto map	모든 암호화 맵의 모든 컨피그레이션을 지웁니다.
show running-config crypto map	암호화 맵 컨피그레이션을 표시합니다.
tunnel-group	터널 그룹을 구성합니다.

crypto map set validate-icmp-errors

IPsec 터널을 지나고 사설 네트워크의 내부 호스트로 향하는 수신 ICMP 오류 메시지를 검증할지 여부를 지정하려면 글로벌 컨피그레이션 모드에서 **crypto map set validate-icmp-errors** 명령을 사용합니다. 암호화 맵 엔트리에서 신뢰 지점을 제거하려면 이 명령의 **no** 형식을 사용합니다.

crypto map *name priority* **set validate-icmp-errors**

no crypto map *name priority* **set validate-icmp-errors**

구문 설명

name	암호화 맵 세트의 이름을 지정합니다.
priority	암호화 맵 엔트리에 부여하는 우선순위를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

이 암호화 맵 명령은 수신 ICMP 오류 메시지를 검증하는 데에만 유효합니다.

csc

ASA에서 CSC SSM에 네트워크 트래픽을 보낼 수 있게 하려면 클래스 컨피그레이션 모드에서 **csc** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

csc {fail-open | fail-close}

no csc

구문 설명

fail-close	CSC SSM에 오류가 생길 경우 적응형 ASA에서 트래픽을 차단하도록 지정합니다. 이는 클래스 맵에 의해 선택된 트래픽에만 적용됩니다. CSC SSM에 전송되지 않는 다른 트래픽은 CSC SSM 오류의 영향을 받지 않습니다.
fail-open	CSC SSM에 오류가 생길 경우 적응형 ASA에서 트래픽을 허용하도록 지정합니다. 이는 클래스 맵에 의해 선택된 트래픽에만 적용됩니다. CSC SSM에 전송되지 않는 다른 트래픽은 CSC SSM 오류의 영향을 받지 않습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다.

csc 명령은 해당 클래스 맵과 매칭하는 모든 트래픽을 CSC SSM에 보내도록 보안 정책을 구성합니다. 이 동작은 ASA에서 트래픽이 계속 목적지로 향하도록 허용하기 전에 수행됩니다.

ASA에서 트래픽 검사에 CSC SSM을 사용할 수 없을 때 매칭하는 트래픽을 어떻게 처리할지 지정할 수 있습니다. **fail-open** 키워드는 CSC SSM을 사용할 수 없더라도 ASA에서 트래픽이 계속 목적지로 향하는 것을 허용하도록 지정합니다. **fail-close** 키워드는 ASA에서 CSC SSM을 사용할 수 없을 때 매칭하는 트래픽이 계속 목적지로 향하는 것을 결코 허용하지 않도록 지정합니다.

CSC SSM에서는 HTTP, SMTP, POP3, FTP 트래픽을 검사할 수 있습니다. 연결을 요청하는 패킷의 목적지 포트가 잘 알려진 해당 프로토콜의 포트일 때만 이 프로토콜을 지원합니다. 즉 CSC SSM에서는 다음 연결만 검사할 수 있습니다.

- TCP 포트 21에 열린 FTP 연결
- TCP 포트 80에 열린 HTTP 연결
- TCP 포트 110에 열린 POP3 연결
- TCP 포트 25에 열린 SMTP 연결

csc 명령을 사용하는 정책에서 다른 프로토콜에 이 포트를 잘못 사용하는 연결을 선택할 경우 ASA는 그 패킷을 CSC SSM에 전달합니다. 그러나 CSC SSM에서는 검사 없이 패킷을 전달합니다.

CSC SSM의 효율성을 극대화하려면 **csc** 명령을 구현하는 정책에 쓰이는 클래스 맵을 다음과 같이 구성합니다.

- CSC SSM에서 검사할, 지원되는 프로토콜만 선택합니다. 예를 들어, HTTP 트래픽을 검사하지 않으려면 서비스 정책에서 HTTP 트래픽을 CSC SSM로 전환하지 않게 합니다.
- ASA에서 보호하는 신뢰받는 호스트에 위험 부담이 될 연결만 선택합니다. 이는 외부 네트워크 또는 신뢰할 수 없는 네트워크에서 내부 네트워크로의 연결입니다. 다음 연결을 검사하는 것이 좋습니다.
  - 아웃바운드 HTTP 연결
  - ASA 내부 클라이언트에서 ASA 외부 서버로의 FTP 연결
  - ASA 내부 클라이언트에서 ASA 외부 서버로의 POP3 연결
  - 내부 메일 서버로 향하는 수신 SMTP 연결

FTP 검사

CSC SSM에서는 FTP 세션의 기본 채널이 표준 포트, 즉 TCP 포트 21을 사용할 때만 FTP 파일 전송의 검사를 지원합니다.

CSC SSM에서 검사하려는 FTP 트래픽에 대해 FTP 검사가 활성화되어야 합니다. FTP에서 동적으로 할당되는 보조 채널을 데이터 전송에 사용하기 때문입니다. ASA에서는 보조 채널에 할당된 포트를 확인하고, 데이터 전송이 이루어지도록 핀홀을 엽니다. CSC SSM에서 FTP 데이터를 검사하도록 구성된 경우 ASA에서는 CSC SSM에 데이터 트래픽을 전환합니다.

전역에 또는 **csc** 명령이 적용된 인터페이스에 FTP 검사를 적용할 수 있습니다. 기본적으로 FTP 검사는 전역에 활성화되어 있습니다. 기본 검사 컨피그레이션을 변경하지 않은 경우 CSC SSM의 FTP 검사를 활성화하는 데 더 이상의 FTP 검사 컨피그레이션은 필요하지 않습니다.

FTP 검사 또는 기본 검사 컨피그레이션에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

예

ASA는 외부 네트워크로 가는 HTTP, FTP, POP3 연결 및 외부 호스트에서 DMZ 네트워크 메일 서버로 가는 수신 SMTP 연결을 위해 트래픽을 내부 네트워크 클라이언트에서 보내는 CSC SSM 요청으로 전환하도록 구성해야 합니다. 내부 네트워크에서 DMZ 네트워크의 웹 서버에 보내는 HTTP 요청은 검사해서는 안 됩니다.

다음 컨피그레이션은 2개의 서비스 정책을 생성합니다. 첫 번째 정책인 csc_out_policy는 내부 인터페이스에 적용되는데, csc_out 액세스 목록을 사용하여 모든 아웃바운드 FTP 및 POP3 요청을 검사하게 합니다. csc_out 액세스 목록은 내부에서 외부 인터페이스 네트워크로 가는 HTTP 연결도 검사받게 하지만, 내부에서 DMZ 네트워크 서버로 가는 HTTP 연결을 제외하는 거부 ACE가 있습니다.

두 번째 정책인 csc_in_policy는 외부 인터페이스에 적용되는데, csc_in 액세스 목록을 사용하여 출발지가 외부 네트워크이고 목적지가 DMZ 네트워크인 SMTP 및 HTTP 요청을 CSC SSM에서 검사하게 합니다. HTTP 요청을 검사함으로써 웹 서버를 HTTP 파일 업로드로부터 보호합니다.

```
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
ciscoasa(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

ciscoasa(config)# class-map csc_outbound_class
ciscoasa(config-cmap)# match access-list csc_out

ciscoasa(config)# policy-map csc_out_policy
ciscoasa(config-pmap)# class csc_outbound_class
ciscoasa(config-pmap-c)# csc fail-close

ciscoasa(config)# service-policy csc_out_policy interface inside

ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

ciscoasa(config)# class-map csc_inbound_class
ciscoasa(config-cmap)# match access-list csc_in

ciscoasa(config)# policy-map csc_in_policy
ciscoasa(config-pmap)# class csc_inbound_class
ciscoasa(config-pmap-c)# csc fail-close

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

참고 CSC SSM에서 FTP에 의해 전송된 파일을 검사하려면 FTP 검사가 활성화되어야 합니다. 기본적으로 FTP 검사가 활성화되어 있습니다.

관련 명령

명령	설명
class (policy-map)	트래픽 분류를 위한 클래스 맵을 지정합니다.
class-map	정책 맵과 함께 사용할 트래픽 분류 맵을 생성합니다.
match port	목적지 포트를 사용하여 트래픽을 매칭합니다.
policy-map	트래픽 클래스를 하나 이상의 작업과 연결하여 정책 맵을 생성합니다.
service-policy	정책 맵을 하나 이상의 인터페이스와 연결하여 보안 정책을 생성합니다.

csd enable

클라이언트리스 SSL VPN 원격 액세스 또는 AnyConnect 클라이언트를 사용하는 원격 액세스를 위해 CSD(Cisco Secure Desktop)를 활성화하려면 webvpn 컨피그레이션 모드에서 **csd enable** 명령을 사용합니다. CSD를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

csd enable

no csd enable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

ASA에 대한 모든 원격 액세스 연결 시도에서는 CSD가 전역으로 활성화되거나 비활성화되는데, 한 가지 예외가 있습니다.

csd enable 명령은 다음을 수행합니다.

1. 앞선 **csd image** *path* 명령에서 수행한 검사를 보완하는 유효성 검사를 실시합니다.
2. disk0에 sdesktop 폴더가 없으면 만듭니다.
3. sdesktop 폴더에 data.xml(Cisco Secure Desktop 컨피그레이션) 파일이 없으면 삽입합니다.
4. 플래시 디바이스에서 실행 중인 컨피그레이션으로 data.xml을 로드합니다.
5. CSD를 활성화합니다.

참고

- CSD가 활성화되었는지 여부를 확인하기 위해 **show webvpn csd** 명령을 입력할 수 있습니다.
- **csd image** *path* 명령이 실행 중인 컨피그레이션에 있어야 **csd enable** 명령을 입력할 수 있습니다.
- **no csd enable** 명령은 실행 중인 컨피그레이션에서 CSD를 비활성화합니다. CSD가 비활성화되면 CSD Manager에 액세스할 수 없고 원격 사용자가 CSD를 사용할 수 없습니다.

- data.xml 파일을 전송하거나 대체할 경우 CSD를 비활성화했다가 활성화하여 실행 중인 컨피그레이션에 파일을 로드합니다.
- ASA에 대한 모든 원격 액세스 연결 시도에서는 CSD가 전역으로 활성화되거나 비활성화됩니다. 개별 연결 프로필 또는 그룹 정책에 대해 CSD를 활성화하거나 비활성화할 수 없습니다.

  예외: 클라이언트리스 SSL VPN 연결의 경우, 클라이언트 컴퓨터에서 그룹 URL을 사용하여 ASA 연결을 시도하고 CSD가 전역에서 활성화된 경우 CSD가 그 컴퓨터에서 실행되지 않도록 연결 프로필을 구성할 수 있습니다. 예:

```
ciscoasa(config)# tunnel-group group-name webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://www.url-string.com
ciscoasa(config-tunnel-webvpn)# without-csd
```

예

다음 명령은 CSD 이미지의 상태를 보고 활성화하는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
csd image	명령에서 명명된 CSD 이미지를 경로에 지정된 플래시 드라이브에서 실행 중인 컨피그레이션으로 복사합니다.
show webvpn csd	CSD가 활성화된 경우 그 버전을 확인합니다. 그렇지 않으면 CLI에서 "Secure Desktop is not enabled."라고 표시됩니다.
without-csd	클라이언트리스 SSL VPN 세션의 연결 프로필은 클라이언트 컴퓨터에서 그룹 URL을 사용하여 ASA 연결을 시도하고 CSD가 전역에서 활성화된 경우 CSD가 그 컴퓨터에서 실행되지 않도록 구성합니다.

csd hostscan image

Cisco Host Scan 배포 패키지를 설치하거나 업그레이드하고 이를 실행 중인 컨피그레이션에 추가하려면 webvpn 컨피그레이션 모드에서 **csd hostscan image** 명령을 사용합니다. 실행 중인 컨피그레이션에서 Host Scan 배포 패키지를 제거하려면 이 명령의 **no** 형식을 사용합니다.

csd hostscan image *path*

no csd hostscan image *path*

구문 설명

path	Cisco Host Scan 패키지의 경로와 파일 이름을 최대 255자로 지정합니다. Host Scan 패키지는 파일 이름 표기 규칙이 hostscan-*version*.pkg인 독립형 Host Scan 패키지이거나 Cisco.com에서 다운로드 가능하고 파일 이름 표기 규칙이 anyconnect-win-*version*-k9.pkg인 종합 AnyConnect Secure Mobility Client 패키지일 수 있습니다. 고객이 AnyConnect Secure Mobility Client를 지정하면 ASA는 AnyConnect 패키지에서 Host Scan 패키지를 추출하여 설치합니다. Host Scan 패키지는 Host Scan 소프트웨어, Host Scan 라이브러리와 보조 차트로 구성됩니다. 이 명령으로 CSD 이미지를 업로드할 수 없습니다. 그 작업에는 **csd image** 명령을 사용합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(1)	이 명령을 도입했습니다.

사용 지침

현재 설치되어 활성화된 Host Scan 이미지의 버전을 확인하려면 **show webvpn csd hostscan** 명령을 입력합니다.

csd hostscan image 명령으로 Host Scan을 설치한 다음 **csd enable** 명령을 사용하여 이미지를 활성화합니다.

write memory 명령을 입력하여 실행 중인 컨피그레이션을 저장합니다. 그러면 다음에 ASA가 재부팅될 때 Host Scan 이미지를 사용할 수 있습니다.

예

다음 명령은 Cisco Host Scan 패키지를 설치하여 활성화하고 확인한 다음 플래시 드라이브에 컨피그레이션을 저장하는 방법을 보여줍니다.

```
ciscoasa> en
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# csd hostscan image disk0:/hostscan_3.0.0333-k9.pkg
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e

22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
show webvpn csd hostscan	Cisco Host Scan이 활성화되었으면 그 버전을 식별합니다. 그렇지 않으면 CLI에서 "Secure Desktop is not enabled."라고 표시됩니다.
csd enable	관리 및 원격 사용자 액세스를 위해 CSD를 활성화합니다.

csd image

CSD 배포 패키지를 검증하고 CSD를 설치하여 실행 중인 컨피그레이션에 추가하려면 webvpn 컨피그레이션 모드에서 **csd image** 명령을 사용합니다. 실행 중인 컨피그레이션에서 CSD 배포 패키지를 제거하려면 이 명령의 **no** 형식을 사용합니다.

csd image *path*

no csd image *path*

구문 설명

path	CSD 패키지의 경로와 파일 이름을 최대 255자로 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

이 명령을 입력하기 전에 **show webvpn csd** 명령을 입력하여 CSD 이미지가 활성화되었는지 여부를 확인합니다. CLI는 CSD가 활성화된 경우 현재 설치된 CSD 이미지의 버전을 표시합니다.

컴퓨터에 CSD 이미지를 다운로드하고 플래시 드라이브로 전송한 다음 **csd image** 명령을 사용하여 새 CSD 이미지를 설치하거나 기존 이미지를 업그레이드합니다. 다운로드할 때 ASA에 적합한 파일을 정확하게 선택해야 합니다. securedesktop_asa_<n>_<n>*.pkg 형식으로 되어 있습니다.

no csd image 명령을 입력하면 CSD Manager에 대한 관리 액세스 및 CSD에 대한 원격 사용자 액세스가 모두 제거됩니다. 이 명령을 입력할 때 ASA에서는 플래시 드라이브의 CSD 소프트웨어 및 CSD 컨피그레이션을 변경하지 않습니다.

참고 **write memory** 명령을 입력하여 실행 중인 컨피그레이션을 저장합니다. 그러면 다음에 ASA가 재부팅할 때 CSD를 사용할 수 있습니다.

예

다음 명령은 현재 CSD 배포 패키지를 보고 플래시 파일 시스템의 내용을 보며 새 버전으로 업그레이드하는 방법을 보여줍니다.

```
ciscoasa# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
ciscoasa(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

관련 명령

명령	설명
show webvpn csd	CSD가 활성화된 경우 그 버전을 확인합니다. 그렇지 않으면 CLI에서 "Secure Desktop is not enabled."라고 표시됩니다.
csd enable	관리 및 원격 사용자 액세스를 위해 CSD를 활성화합니다.

ctl

CTL(Certificate Trust List) 제공자가 CTL 클라이언트에서 보낸 CTL 파일을 구문 분석하고 신뢰 지점을 설치할 수 있게 하려면 ctl 제공자 컨피그레이션 모드에서 **ctl** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ctl install

no ctl install

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ctl 제공자 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

CTL 제공자가 CTL 클라이언트에서 보낸 CTL 파일을 구분 분석하고 CTL 파일의 엔트리에 대해 신뢰 지점을 설치할 수 있게 하려면 ctl 제공자 컨피그레이션 모드에서 **ctl** 명령을 사용합니다. 이 명령으로 설치한 신뢰 지점의 이름은 "_internal_CTL_<ctl_name>"이라는 접두사가 붙습니다.

이 명령이 비활성화된 경우, **crypto ca trustpoint** 및 **crypto ca certificate chain** 명령을 사용하여 각 CallManager 서버와 CAPFs 인증서를 직접 가져와 설치해야 합니다.

예

다음 예에서는 CTL 제공자 인스턴스를 생성하는 방법을 보여줍니다.

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

관련 명령

명령	설명
ctl-provider	CTL 제공자 인스턴스를 정의하고 제공자 컨피그레이션 모드를 시작합니다.
server trust-point	TLS 핸드셰이크 과정에서 제시할 프록시 신뢰 지점 인증서를 지정합니다.
show tls-proxy	TLS 프록시를 표시합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

ctl-file(global)

전화 프록시를 위해 생성할 CTL 인스턴스를 지정하거나 플래시 메모리에 저장된 CTL 파일을 구문 분석하려면 글로벌 컨피그레이션 모드에서 **ctl-file** 명령을 사용합니다. CTL 인스턴스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ctl-file *ctl_name* **noconfirm**

no ctl-file *ctl_name* **noconfirm**

구문 설명

ctl_name	CTL 인스턴스의 이름을 지정합니다.
noconfirm	(선택 사항) **no** 명령과 함께 사용하면, CTL 파일이 제거될 때 신뢰 지점이 삭제된다는 경고가 ASA 콘솔에 더 이상 출력되지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

사용자에게 LSC 프로비저닝이 필요한 전화기가 있을 경우, **ctl-file** 명령을 사용하여 CTL 파일 인스턴스를 구성할 때 CUMC에서 ASA로 CAPF 인증서도 가져와야 합니다. 자세한 내용은 CLI 컨피그레이션 가이드를 참조하십시오.

참고 CTL 파일을 만들려면 ctl 파일 컨피그레이션 모드에서 **no shutdown** 명령을 사용합니다. CTL 파일을 수정하거나 엔트리를 추가하거나 CTL 파일을 삭제하려면 **shutdown** 명령을 사용합니다.

이 명령의 **no** 형식을 사용하면 CTL 파일과 함께 전화 프록시에서 내부에 생성한 등록된 신뢰 지점이 모두 제거됩니다. 또한 CTL 파일을 제거하면 관련 인증 기관에서 받은 모든 인증서도 삭제됩니다.

예

다음 예에서는 전화 프록시 기능을 위해 CTL 파일을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# ctl-file myctl
```

관련 명령

명령	설명
ctl-file (phone-proxy)	전화 프록시 인스턴스를 구성할 때 사용할 CTL 파일을 지정합니다.
cluster-ctl-file	플래시 메모리에 저장된 CTL 파일에서 신뢰 지점을 설치하기 위해 이 파일을 구문 분석합니다.
phone-proxy	전화 프록시 인스턴스를 구성합니다.
record-entry	CTL 파일을 생성하는 데 사용할 신뢰 지점을 지정합니다.
sast	CTL 레코드에 생성할 SAST 인증서의 수를 지정합니다.

ctl-file(phone-proxy)

전화 프록시를 구성할 때 사용할 CTL 인스턴스를 지정하려면 전화 프록시 컨피그레이션 모드에서 **ctl-file** 명령을 사용합니다. CTL 인스턴스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ctl-file *ctl_name*

no ctl-file *ctl_name*

구문 설명

ctl_name	CTL 인스턴스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
전화 프록시 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

예

다음 예에서는 **ctl-file** 명령을 사용하여 전화 프록시 기능을 위한 CTL 파일을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-phone-proxy)# ctl-file myctl
```

관련 명령

명령	설명
ctl-file(global)	전화 프록시 구성을 위해 생성할 CTL 파일 또는 플래시 메모리에 있는, 구문 분석할 CTL 파일을 지정합니다.
phone-proxy	전화 프록시 인스턴스를 구성합니다.

ctl-provider

CTL 제공자 모드에서 CTL 제공자 인스턴스를 구성하려면 글로벌 컨피그레이션 모드에서 **ctl-provider** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

구문 설명

ctl_name	CTL 제공자 인스턴스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

CTL 제공자 인스턴스를 만들기 위해 CTL 제공자 컨피그레이션 모드를 시작하려면 **ctl-provider** 명령을 사용합니다.

예

다음 예에서는 CTL 제공자 인스턴스를 생성하는 방법을 보여줍니다.

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

관련 명령

명령	설명
client	CTL 제공자에 액세스할 수 있는 클라이언트와 클라이언트 인증을 위한 사용자 이름 및 비밀번호를 지정합니다.
ctl	CTL 클라이언트의 CTL 파일을 구문 분석하고 신뢰 지점을 설치합니다.
export	클라이언트에 내보낼 인증서를 지정합니다.
service	CTL 제공자가 수신하는 포트를 지정합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

cts import-pac

Cisco ISE에서 PAC(Protected Access Credential) 파일을 가져오려면 글로벌 컨피그레이션 모드에서 **cts import-pac** 명령을 사용합니다.

cts import-pac *filepath* **password** *value*

구문 설명

filepath	다음 **exec** 모드 명령과 옵션 중 하나를 지정합니다. **단일 모드** • **disk0**: disk0의 경로 및 파일 이름 • **disk1**: disk1의 경로 및 파일 이름 • **flash**: 플래시의 경로 및 파일 이름 • **ftp**: FTP의 경로 및 파일 이름 • **http**: HTTP의 경로 및 파일 이름 • **https**: HTTPS의 경로 및 파일 이름 • **smb**: SMB의 경로 및 파일 이름 • **tftp**: TFTP의 경로 및 파일 이름 **다중 모드** • **http**: HTTP의 경로 및 파일 이름 • **https**: HTTPS의 경로 및 파일 이름 • **smb**: SMB의 경로 및 파일 이름 • **tftp**: TFTP의 경로 및 파일 이름
password *value*	PAC 파일을 암호화하는 데 사용되는 비밀번호를 지정합니다. 비밀번호는 디바이스 자격 증명의 일부로서 ISE에 구성된 비밀번호와는 별개입니다. 이 비밀번호는 PAC 파일이 요청되었을 때 제공된 것과 일치해야 하며, PAC 데이터를 해독하는 데 필요합니다. 이 비밀번호는 ISE에서 디바이스 자격 증명의 일부로 구성된 것과 상관없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에 PAC 파일을 가져오면 ISE와의 연결이 설정됩니다. 채널이 설정되면 ASA는 ISE와 보안 RADIUS 트랜잭션을 시작하고 Cisco TrustSec 환경 데이터를 다운로드합니다. 즉 ASA는 보안 그룹 테이블을 다운로드합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다. 보안 그룹 이름은 ISE에서 만들어지며, 보안 그룹을 위해 사용하기 편리한 이름을 제공합니다. RADIUS 트랜잭션 이전에는 어떤 채널도 설정되지 않습니다. ASA는 인증에 PAC를 사용하면서 ISE와의 RADIUS 트랜잭션을 시작합니다.

팁 PAC 파일은 ASA와 ISE 간의 RADIUS 트랜잭션을 보호할 수 있는 공유 키를 포함합니다. 이 키는 매우 중요하므로 ASA에 안전하게 저장되어야 합니다.

성공적으로 파일을 가져왔으면 ASA는 ISE로부터 Cisco TrustSec 환경 데이터를 다운로드합니다. ISE에 구성된 디바이스 비밀번호는 필요 없습니다.

ASA는 사용자 인터페이스를 통해 접근할 수 없는 NVRAM 영역에 PAC 파일을 저장합니다.

전제 조건

- ASA가 SE에 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있어야 ASA가 PAC 파일을 생성할 수 있습니다. ASA는 어떤 PAC 파일이든 가져올 수 있지만, 바르게 구성된 ISE에 의해 생성된 파일만 ASA만 작동합니다.
- ISE에서 생성할 때 PAC 파일 암호화에 사용되는 비밀번호를 확보합니다.

  ASA는 PAC 파일 가져오기 및 암호 해독에 이 비밀번호를 필요로 합니다.
- ISE가 PAC 파일에 대한 액세스를 생성합니다. ASA은(는) 플래시 메모리 또는 TFTP, FTP, HTTP, HTTPS, SMB를 통한 원격 서버로부터 PAC 파일을 가져올 수 있습니다. PAC 파일은 파일을 가져오기 전에 ASA 플래시에 상주하지 않아도 됩니다.
- 서버 그룹이 ASA에 대해 구성되었습니다.

제한 사항

- ASA가 HA 구성의 일부라면 기본 ASA 디바이스에 PAC 파일을 가져와야 합니다.
- ASA가 클러스터링 컨피그레이션의 일부인 경우 PAC 파일을 마스터 디바이스로 가져와야 합니다.

예

다음 예에서는 ISE에서 PAC를 가져옵니다.

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

관련 명령

명령	설명
cts refresh environment-data	ASA가 Cisco TrustSec과 통합될 때 ISE로부터 Cisco TrustSec 환경 데이터를 새로 가져옵니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

cts manual

SGT plus Ethernet Tagging(레이어 2 SGT Imposition이라고도 함)을 활성화하고 cts 수동 인터페이스 컨피그레이션 모드를 시작하려면 인터페이스 컨피그레이션 모드에서 **cts manual** 명령을 사용합니다. SGT plus Ethernet Tagging을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts manual

no cts manual

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 레이어 2 SGT Imposition을 활성화하고 CTS 수동 인터페이스 컨피그레이션 모드를 시작합니다.

제한 사항

- 물리적 인터페이스, VLAN 인터페이스, 포트 채널 인터페이스 및 중복 인터페이스에서만 지원됩니다.
- BVI, TVI, VNI와 같은 논리적 인터페이스나 가상 인터페이스에서는 지원되지 않습니다.
- 장애 조치 링크를 지원하지 않습니다.
- 클러스터 제어 링크를 지원하지 않습니다.

예

다음 예에서는 레이어 2 SGT Imposition을 활성화하고 CTS 수동 인터페이스 컨피그레이션 모드를 시작합니다.

```
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)#
```

관련 명령

명령	설명
policy static sgt	수동으로 구성된 CTS 링크에 정책을 적용합니다.
propagate sgt	인터페이스에서 보안 그룹 태그(**sgt**라고 함) 전파를 활성화합니다.

cts refresh environment-data

ISE로부터 Cisco TrustSec 환경 데이터를 새로 가져오고 조정 타이머를 구성된 기본값으로 재설정하려면 글로벌 컨피그레이션 모드에서 **cts refresh environment-data** 명령을 사용합니다.

cts refresh environment-data

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

ASA가 Cisco TrustSec과 통합될 때 ASA는 ISE로부터 환경 데이터를 다운로드하며, 여기에는 SGT(보안 그룹 태그) 이름 테이블이 포함되어 있습니다. ASA는 ASA에서 다음 작업이 완료되면 ISE로부터 가져온 환경 데이터를 자동으로 업데이트합니다.

- ISE와 통신할 AAA 서버를 구성합니다.
- ISE에서 PAC 파일을 가져옵니다.
- ASA가 Cisco TrustSec 환경 데이터의 검색에 사용할 AAA 서버 그룹을 식별합니다.

일반적으로 ISE에서 가져온 환경 데이터를 직접 업데이트할 필요는 없습니다. 그러나 ISE에서 보안 그룹이 변경될 수 있습니다. 이러한 변경이 ASA에서 적용되려면 ASA 보안 그룹 테이블의 데이터를 새로 고쳐야 합니다. ASA의 데이터를 새로 고쳐 ISE에서 생성된 어떤 보안 그룹도 ASA에 적용되게 합니다.

팁 ISE의 정책 컨피그레이션 변경과 ASA의 수동 데이터 갱신을 유지 관리 기간 중에 예약하는 것이 좋습니다. 이 방법으로 정책 컨피그레이션 변경 사항을 처리하면 ASA에서 보안 그룹 이름이 확인되고 보안 정책이 즉시 활성화될 가능성이 극대화됩니다.

전제 조건

ASA가 ISE에서 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있고 ASA가 PAC 파일 가져오기에 성공해야만 Cisco TrustSec에 대한 변경 사항이 ASA에 적용됩니다.

제한 사항

- ASA가 HA 컨피그레이션의 일부인 경우 기본 ASA 디바이스에서 환경 데이터를 갱신해야 합니다.
- ASA가 클러스터링 컨피그레이션의 일부인 경우 마스터 디바이스에서 환경 데이터를 갱신해야 합니다.

예

다음 예에서는 ISE로부터 Cisco TrustSec 환경 데이터를 다운로드합니다.

```
ciscoasa(config)# cts refresh environment-data
```

관련 명령

명령	설명
cts import-pac	ASA가 Cisco TrustSec과 통합될 때 Cisco ISE로부터 PAC(Protected Access Credential) 파일을 가져옵니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

cts role-based sgt-map

수동으로 IP-SGT 바인딩을 구성하려면 글로벌 컨피그레이션 모드에서 **role-based sgt-map** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

cts role-based sgt-map [*IPv4_addr* **|** *IPv6_addr***] sgt** *sgt_value*

no cts role-based sgt-map [*IPv4_addr* **|** *IPv6_addr***] sgt** *sgt_value*

구문 설명

IPv4_addr	사용할 IPv4 주소를 지정합니다.
IPv6_addr	사용할 IPv6 주소를 지정합니다.
sgt *sgt_value*	IP 주소를 매핑할 SGT 번호를 지정합니다. 유효한 값은 2~65519입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(1)	이 명령을 도입했습니다.

사용 지침

이 명령을 사용하면 IP-SGT 바인딩을 수동으로 구성할 수 있습니다.

예

다음 예에서는 IP-SGT 바인딩 테이블 엔트리를 구성합니다.

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

관련 명령

명령	설명
clear configure cts role-based [**sgt-map**]	사용자 정의 IP-SGT 바인딩 테이블 엔트리를 제거합니다.
show running-config [**all**] **cts role-based [sgt-map]**	사용자 정의 IP-SGT 바인딩 테이블 엔트리를 표시합니다.

cts server-group

ASA에서 환경 데이터를 가져오기 위해 Cisco TrustSec과 통합하는 데 사용하는 AAA 서버 그룹을 식별하려면 글로벌 컨피그레이션 모드에서 **cts server-group** 명령을 사용합니다. 명령에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts server-group *aaa-server-group-name*

no cts server-group [*aaa-server-group-name***]**

구문 설명

aaa-server-group-name	로컬에 구성된 기존 AAA 서버 그룹의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

Cisco TrustSec과의 통합을 위한 ASA 구성의 일부로써 ASA가 ISE와 통신할 수 있도록 구성해야 합니다. Cisco TrustSec에 대해 서버 그룹의 인스턴스 1개만 ASA에서 구성할 수 있습니다.

전제 조건

- 참조된 서버 그룹이 존재해야 합니다. *aaa-server-group-name* 인수에서 정의되지 않은 서버 그룹을 지정할 경우 ASA는 오류 메시지를 표시합니다.
- 참조 서버 그룹은 RADIUS 프로토콜을 사용하도록 구성되어야 합니다. 비 RADIUS 서버 그룹을 ASA에 추가하면 기능 컨피그레이션이 실패합니다.
- ISE가 사용자 인증에도 사용되는 경우 ISE에 ASA를 등록할 때 ISE에 입력한 공유 암호를 얻으십시오. 이 정보가 없을 경우 ISE 관리자에게 문의하십시오.

예

다음 예에서는 ASA 로컬에서 ISE를 위한 AAA 서버 그룹을 구성하고 ASA에서 ASA와 Cisco TrustSec과의 통합에 이 AAA 서버 그룹을 사용하도록 구성합니다.

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

관련 명령

명령	설명
aaa-server *server-tag* **protocol radius**	ASA에서 ISE 서버와 통신할 수 있도록 AAA 서버 그룹을 만들고 AAA 서버 매개변수를 구성합니다. 여기서 *server-tag*는 서버 그룹 이름을 지정합니다.
aaa-server *server-tag* (*interface-name*) **host** *server-ip*	AAA 서버를 AAA 서버 그룹의 일부로 구성하고 호스트별 연결 데이터를 설정합니다. 여기서 (*interface-name*)은 ISE 서버가 상주하는 네트워크 인터페이스를 가리키며, *server-tag*는 Cisco TrustSec 통합을 위한 AAA 서버 그룹의 이름이며, *server-ip*에서는 ISE 서버의 IP 주소를 지정합니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

cts sxp connection peer

SXP 피어와의 SXP 연결을 설정하려면 글로벌 컨피그레이션 모드에서 **cts sxp connection peer** 명령을 사용합니다. 명령에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts sxp connection peer *peer_ip_address* **[source** *source_ip_address***] password {default | mode} [mode {local | peer}] {speaker | listener}**

no cts sxp connection peer *peer_ip_address* **[source** *source_ip_address***] [password {default | none}] [mode {local | peer}] [speaker | listener]**

구문 설명

default	**password** 키워드와 함께 사용합니다. SXP 연결을 위해 구성된 기본 비밀번호를 사용하도록 지정합니다.
listener	ASA가 SXP 연결을 위한 리스너의 역할을 하도록 지정합니다. 즉 ASA는 다운스트림 디바이스로부터 IP-SGT 매핑을 수신할 수 있습니다. ASA에 SPX 연결을 위한 스피커 또는 리스너 역할을 지정해야 합니다.
local	**mode** 키워드와 함께 사용합니다. 로컬 SXP 디바이스를 사용하도록 지정합니다.
mode	(선택 사항) SXP 연결의 모드를 지정합니다.
none	**password** 키워드와 함께 사용합니다. SXP 연결에 비밀번호를 사용하지 않도록 지정합니다.
password	(선택 사항) SXP 연결에 인증 키를 사용할지 여부를 지정합니다.
peer	**mode** 키워드와 함께 사용합니다. 피어 SXP 디바이스를 사용하도록 지정합니다.
peer_ip_address	SXP 피어의 IPv4 또는 IPv6 주소를 지정합니다. 피어 IP 주소는 ASA 발신 인터페이스에서 연결 가능해야 합니다.
source *source_ip_address*	(선택 사항) SXP 연결의 로컬 IPv4 또는 IPv6 주소를 지정합니다.
speaker	ASA가 SXP 연결을 위한 스피커의 역할을 하도록 지정합니다. 즉 ASA는 업스트림 디바이스에 IP-SGT 매핑을 전달할 수 있습니다. ASA에 SPX 연결을 위한 스피커 또는 리스너 역할을 지정해야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

피어 간 SXP 연결은 point-to-point 연결이며 TCP를 기본 전송 프로토콜로 사용합니다. SXP 연결은 IP 주소별로 설정됩니다. 단일 디바이스 쌍이 여러 SXP 연결을 담당할 수 있습니다.

제한 사항

- ASA는 SXP 연결을 위해 연결별 비밀번호를 지원하지 않습니다.
- 기본 SXP 비밀번호를 구성하기 위해 **cts sxp default password**를 사용할 때 SXP 연결에서 기본 비밀번호를 사용하도록 구성해야 합니다. 이와 달리 기본 비밀번호를 구성하지 않을 경우 SXP 연결에 대해 기본 비밀번호를 구성해서는 안 됩니다. 이 2가지 지침을 따르지 않으면 SXP 연결이 실패할 수 있습니다.
- 기본 비밀번호를 사용하여 SXP 연결을 구성하지만 ASA에 기본 비밀번호가 구성되지 않았다면 SXP 연결은 실패합니다.
- SXP 연결을 위한 소스 IP 주소를 구성하는 경우 ASA 아웃바운드 인터페이스와 동일한 주소를 지정해야 합니다. 소스 IP 주소가 아웃바운드 인터페이스의 주소와 일치하지 않으면 SXP 연결이 실패합니다.

  SXP 연결에 대한 소스 IP 주소가 구성되지 않은 경우 ASA는 경로/ARP 조회를 실시하여 SXP 연결에 대한 아웃바운드 인터페이스를 결정합니다. SXP 연결에 대해 소스 IP 주소를 구성하지 않고 ASA에서 경로/ARP 조회를 통해 SXP 연결에 대한 소스 IP 주소를 확인할 수 있도록 하는 것이 좋습니다.
- SXP 피어 또는 소스에 대해 IPv6 로컬 링크 주소를 구성하는 것은 지원되지 않습니다.
- SXP 연결을 위해 하나의 인터페이스에서 여러 IPv6 주소를 구성하는 것은 지원되지 않습니다.

예

다음 예에서는 ASA에서 SXP 연결을 생성합니다.

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 source 192.168.1.1 password
default mode peer speaker
```

관련 명령

명령	설명
cts sxp default password	SXP 연결의 기본 비밀번호를 지정합니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

cts sxp default password

SXP 피어와의 TCP MD5 인증을 위해 기본 비밀번호를 구성하려면 글로벌 컨피그레이션 모드에서 **cts sxp default password** 명령을 사용합니다. 명령에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts sxp default password [0 | 8] *password*

no cts sxp default password [0 | 8] [*password***]**

구문 설명

0	(선택 사항) 기본 비밀번호에서 암호화 레벨에 암호화되지 않은 일반 텍스트를 사용하도록 지정합니다. 기본 비밀번호에 대해 하나의 암호화 레벨만 설정할 수 있습니다.
8	(선택 사항) 기본 비밀번호에서 암호화 레벨에 암호화된 텍스트를 사용하도록 지정합니다.
password	최대 162자의 암호화된 문자열 또는 최대 80자의 ASCII 키 문자열을 지정합니다.

기본값

기본적으로 SXP 연결에는 설정된 비밀번호가 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

기본 비밀번호를 사용하여 SXP 연결을 구성하지만 ASA에 기본 비밀번호가 구성되지 않았다면 SXP 연결은 실패합니다.

제한 사항

- ASA는 SXP 연결을 위해 연결별 비밀번호를 지원하지 않습니다.
- 기본 SXP 비밀번호를 구성하기 위해 **cts sxp default password**를 사용할 때 SXP 연결에서 기본 비밀번호를 사용하도록 구성해야 합니다. 이와 달리 기본 비밀번호를 구성하지 않을 경우 SXP 연결에 대해 기본 비밀번호를 구성해서는 안 됩니다. 이 2가지 지침을 따르지 않으면 SXP 연결이 실패할 수 있습니다.

예

다음 예에서는 SXP 연결의 기본 비밀번호를 포함하여 모든 SXP 연결의 기본값을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

관련 명령

명령	설명
cts sxp connection peer	ASA와 SXP 피어의 SXP 연결을 구성합니다. 이 명령과 함께 **password default** 키워드를 지정하면 해당 SXP 연결에 기본 비밀번호를 사용할 수 있습니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

cts sxp default source-ip

SXP 연결의 기본 로컬 IP 주소를 구성하려면 글로벌 컨피그레이션 모드에서 **cts sxp default source-ip** 명령을 사용합니다. 명령에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts sxp default source-ip *ipaddress*

no cts sxp default source-ip [*ipaddress*]

구문 설명

ipaddress	소스 IP 주소의 IPv4 또는 IPv6 주소를 지정합니다.

기본값

기본적으로 SXP 연결은 기본 소스 IP 주소가 설정되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

SXP 연결을 위한 기본 소스 IP 주소를 구성하는 경우 ASA 아웃바운드 인터페이스와 동일한 주소를 지정해야 합니다. 소스 IP 주소가 아웃바운드 인터페이스의 주소와 일치하지 않으면 SXP 연결이 실패합니다.

SXP 연결에 대한 소스 IP 주소가 구성되지 않은 경우 ASA는 경로/ARP 조회를 실시하여 SXP 연결에 대한 아웃바운드 인터페이스를 결정합니다. SXP 연결에 대해 기본 소스 IP 주소를 구성하지 않고 ASA에서 경로/ARP 조회를 통해 SXP 연결에 대한 소스 IP 주소를 찾을 수 있게 하는 것이 좋습니다.

예

다음 예에서는 SXP 연결의 기본 소스 IP 주소를 포함하여 모든 SXP 연결의 기본값을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

관련 명령

명령	설명
cts sxp connection peer	ASA의 SXP 연결을 구성합니다. 이 명령과 함께 **source** *source_ip_address* 키워드와 인수를 지정하면 해당 SXP 연결에서 기본 소스 IP 주소를 사용할 수 있게 됩니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

cts sxp enable

ASA에서 SXP 프로토콜을 활성화하려면 글로벌 컨피그레이션 모드에서 **cts sxp enable** 명령을 사용합니다. 명령에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts sxp enable

no cts sxp enable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본적으로 ASA에서는 SXP 프로토콜이 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 ASA에서 SXP 프로토콜을 활성화합니다.

```
ciscoasa(config)# cts sxp enable
```

관련 명령

명령	설명
clear cts	Cisco TrustSec과 통합할 때 ASA에서 사용하는 데이터를 지웁니다.
cts sxp connection peer	ASA와 SXP 피어의 SXP 연결을 구성합니다.

cts sxp reconciliation period

글로벌 컨피그레이션 모드에서 **cts sxp reconciliation period** 명령을 사용합니다. 명령에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts sxp reconciliation period *timervalue*

no cts sxp reconciliation period [*timervalue*]

구문 설명

timervalue	조정 타이머의 기본값을 지정합니다. 1초~64000초 범위에서 값을 입력합니다.

기본값

기본적으로 *timervalue*는 120초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

SXP 피어가 SXP 연결을 종료하고 나면 ASA가 보류 타이머를 시작합니다. SXP 피어가 보류 타이머 실행 중에 연결되는 경우 ASA에서 조정 타이머를 시작하고 ASA에서는 SXP 매핑 데이터베이스를 업데이트하여 가장 최근의 매핑을 습득합니다.

조정 타이머가 만료되면 ASA에서 SXP 매핑 데이터베이스를 검사하여 오래된 매핑 엔트리(이전 연결 세션에서 습득한 엔트리)를 식별합니다. ASA에서 이러한 연결을 오래된 연결로 표시합니다. 조정 타이머가 만료되면 ASA에서 오래된 엔트리를 SXP 매핑 데이터베이스에서 삭제합니다.

타이머에 0을 지정할 수 없습니다. 0을 지정하면 조정 타이머가 시작할 수 없게 됩니다. 조정 타이머 실행을 허용하지 않으면 오래된 엔트리가 무기한 남아 정책 적용에서 예기치 못한 결과가 생길 수 있습니다.

예

다음 예에서는 기본 조정 타이머를 포함하여 모든 SXP 연결의 기본값을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

관련 명령

명령	설명
cts sxp connection peer	ASA와 SXP 피어의 SXP 연결을 구성합니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

cts sxp retry period

SXP 피어 간의 새 SXP 연결을 설정하려는 ASA 시도의 기본 간격을 지정하려면 글로벌 컨피그레이션 모드에서 **cts sxp retry period** 명령을 사용합니다. 명령에 대한 지원을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

cts sxp retry period *timervalue*

no cts sxp retry period [*timervalue*]

구문 설명

timervalue	재시도 타이머의 기본값을 지정합니다. 0초~64000초 범위에서 값을 입력합니다.

기본값

기본적으로 *timervalue*는 120초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

SXP 피어 간의 새 SXP 연결을 설정하려는 ASA 시도의 기본 간격을 지정합니다. ASA는 성공할 때까지 연결을 시도합니다.

ASA에 설정되지 않은 SXP 연결이 있는 한 재시도 타이머가 트리거됩니다.

0초로 지정하면 타이머가 만료되지 않으며 ASA는 SXP 피어 연결을 시도하지 않습니다.

재시도 타이머가 만료되면 ASA는 연결 데이터베이스를 확인합니다. 데이터베이스에 꺼져 있거나 "보류" 상태인 연결이 있는 경우 ASA는 재시도 타이머를 다시 시작합니다.

재시도 타이머를 SXP 피어 디바이스와 다른 값으로 구성하는 것이 좋습니다.

예

다음 예에서는 기본 재시도 간격을 포함하여 모든 SXP 연결의 기본값을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

관련 명령

명령	설명
cts sxp connection peer	ASA와 SXP 피어의 SXP 연결을 구성합니다.
cts sxp enable	ASA에서 SXP 프로토콜을 활성화합니다.

customization

터널 그룹, 그룹 또는 사용자에 대한 사용자 지정을 설정하려면 unnel-group webvpn-attributes 컨피그레이션 모드 또는 webvpn 컨피그레이션 모드에서 **customization** 명령을 사용합니다. 사용자 지정을 설정하지 않으려면 이 명령의 **no** 형식을 사용합니다.

customization *name*

no customization *name*

customization {none | value *name***}**

no customization {none | value *name*}

구문 설명

name	그룹 또는 사용자에 적용할 WebVPN 사용자 지정을 명명합니다.
none	그룹 또는 사용자에 대한 사용자 지정을 비활성화하고 사용자 지정이 상속되지 않게 합니다.
value *name*	그룹 정책 또는 사용자에 적용할 사용자 지정을 명명합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tunnel-group webvpn-attributes 컨피그레이션	• 예	—	• 예	—	—
Webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

tunnel-group webvpn-attributes 컨피그레이션 모드에서 **customization** 명령을 입력하기 전에 webvpn 컨피그레이션 모드에서 **customization** 명령을 사용하여 사용자 지정을 명명하고 구성해야 합니다.

모드별 명령 옵션

customization 명령과 함께 사용하는 키워드는 현재의 모드에 따라 달라집니다. 그룹 정책 특성 컨피그레이션 모드 및 사용자 이름 특성 컨피그레이션 모드에서는 **none** 및 **value** 키워드가 추가로 나타납니다.

예를 들어, 사용자 이름 특성 컨피그레이션 모드에서 **customization none** 명령을 입력할 경우 ASA는 그룹 정책 또는 터널 그룹에서 그 값을 찾지 않습니다.

예

다음 예에서는 비밀번호 프롬프트를 정의하는 "123"이라는 WebVPN 사용자 지정을 가장 먼저 설정하는 명령 시퀀스를 보여줍니다. 그런 다음 "test"라는 WebVPN 터널 그룹을 정의하고, **customization** 명령을 사용하여 "123"이라는 WebVPN 사용자 지정을 사용하도록 설정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization 123
ciscoasa(config-webvpn-custom)# password-prompt Enter password
ciscoasa(config-webvpn)# exit
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# customization 123
ciscoasa(config-tunnel-webvpn)#
```

다음 예에서는 "cisco"라는 사용자 지정을 "cisco_sales"라는 그룹 정책에 적용하는 것을 보여줍니다. webvpn 컨피그레이션 모드를 통해 그룹 정책 특성 컨피그레이션 모드에서 **customization** 명령을 입력할 때 **value**라는 명령 옵션이 추가로 필요합니다.

```
ciscoasa(config)# group-policy cisco_sales attributes
ciscoasa(config-group-policy)#  webvpn
ciscoasa(config-group-webvpn)# customization value cisco
```

관련 명령

명령	설명
clear configure tunnel-group	모든 터널 정책 컨피그레이션을 제거합니다.
show running-config tunnel-group	현재 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group webvpn-attributes	WebVPN 터널 그룹 특성을 구성하기 위해 webvpn 컨피그레이션 모드를 시작합니다.

cxsc

ASA CX 모듈에 트래픽을 리디렉션하려면 클래스 컨피그레이션 모드에서 **cxsc** 명령을 사용합니다. ASA CX 작업을 제거하려면 이 명령의 **no** 형식을 사용합니다.

cxsc {fail-close | fail-open} [auth-proxy | monitor-only]

no cxsc {fail-close | fail-open} [auth-proxy | monitor-only]

구문 설명

auth-proxy	(선택 사항) 능동적 인증에 필요한 인증 프록시를 활성화합니다.
fail-close	ASA CX 모듈을 사용할 수 없을 경우 ASA에서 모든 트래픽을 차단하도록 설정합니다.
fail-open	ASA CX 모듈을 사용할 수 없을 경우 ASA에서 검사 없이 모든 트래픽을 허용하도록 설정합니다.
monitor-only	데모 목적에 한해 트래픽의 읽기 전용 복사본을 ASA CX에 보내려면 **monitor-only**를 지정합니다. 이 옵션을 구성하면 다음과 비슷한 경고 메시지가 표시됩니다. `WARNING: Monitor-only mode should be used for demonstrations and evaluations only. This mode prevents CXSC from denying or altering traffic.`

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(4.1)	이 명령을 도입했습니다.
9.1(2)	데모 기능을 지원하기 위해 **monitor-only** 키워드를 추가했습니다.
9.1(3)	컨텍스트별로 ASA CX 정책을 구성할 수 있습니다.

사용 지침

먼저 정책 맵 명령을 입력하여 클래스 컨피그레이션 모드에 액세스할 수 있습니다.

ASA에서 **cxsc** 명령을 구성하기 전에 또는 구성한 다음에 Cisco PRSM(Prime Security Manager)을 사용하여 ASA CX 모듈의 보안 정책을 구성합니다.

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

트래픽 흐름

ASA CX 모듈에서는 ASA와 별개의 애플리케이션을 실행합니다. 그러나 이는 ASA 트래픽 흐름에 통합되어 있습니다. ASA에서 어떤 클래스 또는 트래픽에 대해 **cxsc** 명령을 적용하면 트래픽은 다음과 같이 ASA와 ASA CX 모듈을 지납니다.

1. 트래픽이 ASA에 들어옵니다.
2. 수신 VPN 트래픽이 해독됩니다.
3. 방화벽 정책이 적용됩니다.
4. 트래픽이 백플레인을 통해 ASA CX 모듈에 보내집니다.
5. ASA CX 모듈은 트래픽에 보안 정책을 적용하고 적절한 조치를 수행합니다.
6. 유효한 트래픽은 다시 백플레인을 통해 ASA로 보내집니다. ASA CX 모듈에서 보안 정책에 따라 일부 트래픽을 차단할 수도 있으며, 그 트래픽은 전달되지 않습니다.
7. 발신 VPN 트래픽이 암호화됩니다.
8. 트래픽이 ASA를 떠납니다.

인증 프록시에 대한 정보

ASA CX에서 (ID 정책을 활용하기 위해) HTTP 사용자를 인증해야 하는 경우, ASA가 인증 프록시의 역할을 하도록 구성해야 합니다. ASA CX 모듈은 인증 요청을 ASA 인터페이스 IP 주소/프록시 포트에 리디렉션합니다. 기본적으로 포트는 885이며, 사용자가 **cxsc auth-proxy port** 명령으로 구성할 수 있습니다. ASA에서 보낸 트래픽을 ASA CX 모듈로 전환하도록 이 기능을 서비스 정책의 일부로 구성합니다. 인증 프록시를 활성화하지 않으면 수동적 인증만 가능합니다.

ASA 기능과의 호환성

ASA는 HTTP 검사를 비롯하여 여러 고급 애플리케이션 검사 기능을 갖추었습니다. 그러나 ASA CX 모듈에서는 ASA보다 더 우수한 HTTP 검사 기능을 제공할 뿐 아니라 다른 애플리케이션을 위한 부가 기능(예: 애플리케이션 사용량 모니터링 및 제어)도 제공합니다.

ASA CX 모듈의 기능을 십분 활용하려면 ASA CX 모듈에 보내는 트래픽에 대한 다음 지침을 참조하십시오.

- HTTP 트래픽에 대해 ASA 검사를 구성하지 마십시오.
- Cloud Web Security(ScanSafe) 검사를 구성하지 마십시오. 동일한 트래픽에 대해 ASA CX 작업과 Cloud Web Security 검사를 모두 구성하면 ASA는 ASA CX 작업만 수행합니다.
- ASA의 다른 애플리케이션 검사 기능은 ASA CX 모듈과 호환됩니다(기본 검사 포함).
- MUS(Mobile User Security) 서버를 활성화하지 마십시오. ASA CX 모듈과 호환되지 않습니다.
- ASA 클러스터링을 활성화하지 마십시오. ASA CX 모듈과 호환되지 않습니다.
- 장애 조치를 활성화할 경우, ASA 장애 조치가 일어나면 기존의 모든 ASA CX 흐름이 새로운 ASA에 전송됩니다. 그러나 ASA CX 모듈의 작업 없이 트래픽이 ASA를 통과하게 됩니다. 새로운 ASA에서 수신한 새 흐름에만 ASA CX 모듈의 작업이 수행됩니다.

모니터 전용 모드

테스트 및 데모를 위해 ASA에서 일기 전용 트래픽의 복제 스트림을 ASA CX 모듈에 보내도록 구성할 수 있으며, 이를 위해 **monitor-only** 키워드를 사용합니다. 그러면 ASA 트래픽 흐름에 영향을 주지 않으면서 모듈에서 트래픽을 어떻게 검사하는지 확인할 수 있습니다. 이 모드에서는 ASA CX 모듈이 평소와 같이 트래픽을 검사하고 정책 결정을 내리고 이벤트를 생성합니다. 그러나 패킷이 읽기 전용 복사본이므로 모듈의 작업이 실제 트래픽에 영향을 주지 않습니다. 검사가 끝나면 모듈에서는 복사본을 폐기합니다.

다음 지침을 참조하십시오.

- ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수 없습니다. 단 하나의 보안 정책 유형만 허용됩니다.
- 다음 기능은 모니터 전용 모드에서 지원되지 않습니다.
  - 거부 정책
  - 능동적 인증
  - 해독 정책
- ASA CX는 모니터 전용 모드에서 패킷 버퍼링을 수행하지 않으며, BE(best effort) 방식으로 이벤트가 생성됩니다. 예를 들어, 패킷 경계를 포괄하는 긴 URL을 가진 이벤트와 같은 일부 이벤트는 버퍼링이 지원되지 않아 영향을 받을 수 있습니다.
- ASA 정책과 ASA CX가 일치하는 모드를 갖도록 구성해야 합니다. 둘 다 모니터 전용이거나 둘 다 일반 인라인 모드여야 합니다.

예

다음 예에서는 모든 HTTP 트래픽을 ASA CX 모듈로 전환하고, ASA CX 모듈 카드에서 어떤 이유로든 오류가 발생하면 모든 HTTP 트래픽을 차단합니다.

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

다음 예에서는 10.1.1.0 네트워크 및 10.2.1.0 네트워크로 향하는 모든 IP 트래픽을 ASA CX 모듈로 전환하고, ASA CX 모듈에서 어떤 이유로든 오류가 발생하면 모든 트래픽을 허용합니다.

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

관련 명령

명령	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
class-map	프록시 맵에 사용할 트래픽을 지정합니다.
cxsc auth-proxy port	인증 프록시 포트를 설정합니다.
debug cxsc	ASA CX 디버깅 메시지를 활성화합니다.
hw-module module password-reset	모듈 비밀번호를 기본값으로 재설정합니다.
hw-module module reload	모듈을 다시 로드합니다.
hw-module module reset	재설정을 수행하고 모듈을 다시 로드합니다.
hw-module module shutdown	모듈을 종료합니다.
policy-map	정책을 구성합니다. 즉 트래픽 클래스와 하나 이상의 작업과 연결합니다.
session do get-config	모듈 컨피그레이션을 가져옵니다.
session do password-reset	모듈 비밀번호를 기본값으로 재설정합니다.
session do setup host ip	모듈 관리 주소를 구성합니다.
show asp table classify domain cxsc	ASA CX 모듈에 트래픽을 보내기 위해 생성한 NP 규칙을 표시합니다.
show asp table classify domain cxsc-auth-proxy	ASA CX 모듈의 인증 프록시를 위해 생성한 NP 규칙을 표시합니다.
show module	모듈 상태를 표시합니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.
show service-policy	서비스 정책 통계를 표시합니다.

cxsc auth-proxy port

ASA CX 모듈 트래픽을 위한 인증 프록시 포트를 설정하려면 글로벌 컨피그레이션 모드에서 **cxsc auth-proxy port** 명령을 사용합니다. 포트를 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

cxsc auth-proxy port *port*

no cxsc auth-proxy port [*port*]

구문 설명

port *port*	인증 프록시 포트를 1024보다 높은 값으로 설정합니다. 기본값은 885입니다.

명령 기본값

기본 포트는 885입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(4.1)	이 명령을 도입했습니다.
9.1(3)	컨텍스트별로 ASA CX 정책을 구성할 수 있습니다.

사용 지침

cxsc 명령을 구성할 때 인증 프록시를 활성화할 경우 이 명령으로 포트를 변경할 수 있습니다.

ASA CX에서 (ID 정책을 활용하기 위해) HTTP 사용자를 인증해야 하는 경우, ASA가 인증 프록시의 역할을 하도록 구성해야 합니다. ASA CX 모듈은 인증 요청을 ASA 인터페이스 IP 주소/프록시 포트에 리디렉션합니다. 기본적으로 port는 885입니다. ASA에서 보낸 트래픽을 ASA CX 모듈로 전환하도록 이 기능을 서비스 정책의 일부로 구성합니다. 인증 프록시를 활성화하지 않으면 수동적 인증만 가능합니다.

예

다음 예에서는 ASA CX 트래픽을 위한 인증 프록시를 활성화하고 포트를 5000으로 변경합니다.

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
ciscoasa(config)# cxsc auth-port 5000
```

관련 명령

명령	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
class-map	프록시 맵에 사용할 트래픽을 지정합니다.
cxsc	ASA CX 모듈로 트래픽을 리디렉션합니다.
debug cxsc	ASA CX 디버그 메시지를 활성화합니다.
hw-module module password-reset	모듈 비밀번호를 기본값으로 재설정합니다.
hw-module module reload	모듈을 다시 로드합니다.
hw-module module reset	재설정을 수행하고 모듈을 다시 로드합니다.
hw-module module shutdown	모듈을 종료합니다.
policy-map	정책을 구성합니다. 즉 트래픽 클래스와 하나 이상의 작업과 연결합니다.
session do get-config	모듈 컨피그레이션을 가져옵니다.
session do password-reset	모듈 비밀번호를 기본값으로 재설정합니다.
session do setup host ip	모듈 관리 주소를 구성합니다.
show asp table classify domain cxsc	ASA CX 모듈에 트래픽을 보내기 위해 생성한 NP 규칙을 표시합니다.
show asp table classify domain cxsc-auth-proxy	ASA CX 모듈의 인증 프록시를 위해 생성한 NP 규칙을 표시합니다.
show module	모듈 상태를 표시합니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.
show service-policy	서비스 정책 통계를 표시합니다.

파 트 3

D 명령

database path ~ dhcp-server 명령

database path

로컬 CA 서버 데이터베이스의 경로 또는 위치를 지정하려면 ca server 컨피그레이션 모드에서 **database** 명령을 사용합니다. 기본 설정인 플래시 메모리로 경로를 재설정하려면 이 명령의 **no** 형식을 사용합니다.

[no] database path *mount-name directory-path*

구문 설명

directory-path	CA 파일이 저장된 탑재 지점의 디렉토리 경로를 지정합니다.
mount-name	탑재 이름을 지정합니다.

기본값

기본적으로 CA 서버 데이터베이스가 플래시 메모리에 저장됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
CA 서버 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

데이터베이스에 저장된 로컬 CA 파일은 인증서 데이터베이스, 사용자 데이터베이스 파일, 임시 PKCS12 파일, 현재 CRL 파일을 포함합니다. *mount-name* 인수는 ASA의 파일 시스템을 지정하는 데 사용하는 **mount** 명령의 *name* 인수와 동일합니다.

참고 이 CA 파일은 내부에 저장되는 파일이며 수정해서는 안 됩니다.

예

다음 예에서는 CA 데이터베이스의 탑재 지점을 cifs_share로, 탑재 지점의 데이터베이스 파일 디렉토리를 ca_dir/files_dir로 정의합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# database path cifs_share ca_dir/files_dir/
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	ca server 컨피그레이션 모드 CLI 명령 집합에 대한 액세스를 제공합니다. 이를 통해 사용자는 로컬 CA를 구성하고 관리할 수 있습니다.
crypto ca server user-db write	로컬 CA 데이터베이스에 구성된 사용자 정보를 디스크에 씁니다.
debug crypto ca server	사용자가 로컬 CA 서버를 구성할 때 디버깅 메시지를 표시합니다.
mount	ASA에서 CIFS(Common Internet File System) 및/또는 FTPFS(File Transfer Protocol file systems)에 액세스할 수 있게 해줍니다.
show crypto ca server	ASA의 CA 컨피그레이션 특성을 표시합니다.
show crypto ca server cert-db	CA 서버에서 발급한 인증서를 표시합니다.

ddns

DDNS(동적 DNS) 업데이트 메서드 유형을 지정하려면 ddns-update-method 모드에서 **ddns** 명령을 사용합니다. 실행 중인 컨피그레이션에서 어떤 업데이트 메서드 유형을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ddns [both]

no ddns [both]

구문 설명

both	(선택 사항) DNS A 및 PTR RR(리소스 레코드) 모두의 업데이트를 지정합니다.

기본값

DNS A RR만 업데이트합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ddns-update-method	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

DDNS가 DNS로 관리되는 name-to-address 및 address-to-name 매핑을 업데이트합니다. ASA의 이번 릴리스에서는 DDNS 업데이트를 수행하는 2가지 메서드(RFC 2136에 의해 정의된 IETF 표준 및 일반 HTTP 메서드) 중에서 IETF 메서드를 지원합니다.

이름 및 주소 매핑은 2가지 RR 유형에 수록됩니다.

- A 리소스 레코드는 도메인 이름-IP 주소 매핑을 포함합니다.
- PTR 리소스 레코드는 IP 주소-도메인 이름 매핑을 포함합니다.

DDNS 업데이트는 DNS A 유형과 PTR RR 유형 간에 정보의 일관성을 유지하는 데 사용할 수 있습니다.

ddns-update-method 컨피그레이션 모드에서 **ddns** 명령을 실행하면 업데이트가 DNS A RR에만 적용되는지 또는 DNS A 유형과 PTR RR 유형 모두에 적용되는지 정의합니다.

예

다음 예에서는 ddns-2라는 DDNS 업데이트 메서드에서 DNS A 및 PTR RR 둘 다 업데이트하도록 구성합니다.

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# ddns both
```

관련 명령

명령	설명
ddns update	DDNS 업데이트 메서드를 ASA 인터페이스 또는 DDNS 업데이트 호스트 이름과 연결합니다.
ddns update method	DNS 리소스 레코드를 동적으로 업데이트하는 메서드를 생성합니다.
dhcp-client update dns	DHCP 클라이언트에서 DHCP 서버에 전달할 업데이트 매개변수를 구성합니다.
dhcpd update dns	DDNS 업데이트를 수행하도록 DHCP 서버를 활성화합니다.
interval maximum	DDNS 업데이트 메서드에 의한 업데이트 시도의 최대 간격을 구성합니다.

ddns update

DDNS(동적 DNS) 업데이트 메서드를 ASA 인터페이스 또는 업데이트 호스트 이름과 연결하려면 인터페이스 컨피그레이션 모드에서 **ddns update** 명령을 사용합니다. 실행 중인 컨피그레이션에서 DDNS 업데이트 메서드와 인터페이스 또는 호스트 이름의 연결을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ddns update [*method-name* | **hostname** *hostname***]**

no ddns update [*method-name* | **hostname** *hostname***]**

구문 설명

hostname	명령 문자열의 다음 용어가 호스트 이름임을 지정합니다.
hostname	업데이트에 사용할 호스트 이름을 지정합니다.
method-name	구성 중인 인터페이스와 연결할 메서드 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

DDNS 업데이트 메서드를 정의하고 ASA 인터페이스와 연결해야 DDNS 업데이트를 트리거할 수 있습니다.

호스트 이름은 FQDN(정규화된 도메인 이름)이거나 단순히 호스트 이름일 수 있습니다. 단순히 호스트 이름일 경우 ASA는 그 호스트 이름에 도메인 이름을 추가하여 FQDN을 만듭니다.

예

다음 예에서는 인터페이스 GigabitEthernet0/2를 ddns-2라는 DDNS 업데이트 메서드 및 hostname1.example.com이라는 호스트 이름과 연결합니다.

```
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname hostname1.example.com
```

관련 명령

명령	설명
ddns	생성된 DDNS 메서드에 대한 DDNS 업데이트 메서드 유형을 지정합니다.
ddns update method	DNS 리소스 레코드를 동적으로 업데이트하는 메서드를 생성합니다.
dhcp-client update dns	DHCP 클라이언트에서 DHCP 서버에 전달할 업데이트 매개변수를 구성합니다.
dhcpd update dns	DDNS 업데이트를 수행하도록 DHCP 서버를 활성화합니다.
interval maximum	DDNS 업데이트 메서드에 의한 업데이트 시도의 최대 간격을 구성합니다.

ddns update method

DNS RR을 동적으로 업데이트하는 메서드를 생성하려면 글로벌 컨피그레이션 모드에서 **ddns update method** 명령을 사용합니다. 실행 중인 컨피그레이션에서 DDNS(동적 DNS) 업데이트 메서드를 제거하려면 이 명령의 **no** 형식을 사용합니다.

ddns update method *name*

no ddns update method *name*

구문 설명

name	DNS 레코드를 동적으로 업데이트할 메서드의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

DDNS가 DNS로 관리되는 name-to-address 및 address-to-name 매핑을 업데이트합니다. **ddns update method** 명령으로 구성되는 업데이트 메서드는 어떤 DDNS 업데이트가 얼마나 자주 수행되는가를 결정합니다. ASA의 이번 릴리스에서는 DDNS 업데이트를 수행하는 2가지 메서드(RFC 2136에 의해 정의된 IETF 표준 및 일반 HTTP 메서드) 중에서 IETF 메서드를 지원합니다.

이름 및 주소 매핑은 2가지 RR 유형에 수록되어 있습니다.

- A 리소스 레코드는 도메인 이름-IP 주소 매핑을 포함합니다.
- PTR 리소스 레코드는 IP 주소-도메인 이름 매핑을 포함합니다.

DDNS 업데이트는 DNS A 유형과 PTR RR 유형 간에 정보의 일관성을 유지하는 데 사용할 수 있습니다.

참고 **ddns update method** 명령을 실행하기에 앞서 인터페이스에서 활성화된 도메인 조회와 함께 **dns** 명령을 사용하여 연결 가능한 기본 DNS 서버를 구성해야 합니다.

예

다음 예에서는 ddns-2라는 DDNS 업데이트 메서드를 구성합니다.

```
ciscoasa(config)# ddns update method ddns-2
```

관련 명령

명령	설명
ddns	생성된 DDNS 메서드에 대한 DDNS 업데이트 메서드 유형을 지정합니다.
ddns update	DDNS 업데이트 메서드를 ASA 인터페이스 또는 DDNS 업데이트 호스트 이름과 연결합니다.
dhcp-client update dns	DHCP 클라이언트에서 DHCP 서버에 전달할 업데이트 매개변수를 구성합니다.
dhcpd update dns	동적 DNS 업데이트를 수행하도록 DHCP 서버를 활성화합니다.
interval maximum	DDNS 업데이트 메서드에 의한 업데이트 시도의 최대 간격을 구성합니다.

debug

어떤 기능에 대한 디버깅 메시지를 표시하려면 특별 권한 EXEC 모드에서 **debug** 명령을 사용합니다. 디버그 메시지의 표시를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

debug *feature* **[***subfeature***] [***level***]**

no debug *feature* [*subfeature*]

구문 설명

level	(선택 사항) 디버깅 레벨을 지정합니다. 모든 기능에서 이 레벨을 사용할 수 있는 것은 아닙니다.
feature	디버깅을 활성화하려는 기능을 지정합니다. 가능한 기능을 보려면 **debug ?** 명령을 사용하여 CLI 도움말을 표시합니다.
subfeature	(선택 사항) 기능에 따라 하나 이상의 하위 기능에 대한 디버그 메시지를 활성화할 수 있습니다.

기본값

기본 디버깅 레벨은 1입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

디버깅 출력은 CPU 프로세스에서 우선순위가 높기 때문에 시스템을 사용 불가능한 상태로 만들 수 있습니다. 따라서 **debug** 명령은 구체적인 문제를 해결하거나 Cisco 기술 지원 담당자와 문제 해결 세션을 진행할 때만 사용합니다. 또한 네트워크 트래픽 및 사용자 수가 적을 때 **debug** 명령을 사용하는 것이 가장 좋습니다. 그러한 기간에 디버깅하면 **debug** 명령의 처리 오버헤드 증가로 인해 시스템 사용에 지장이 생길 가능성이 줄어듭니다.

예

다음은 **debug aaa internal** 명령 출력의 예입니다.

```
ciscoasa(config)# debug aaa internal
debug aaa internal enabled at level 1
ciscoasa(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

default(crl configure)

모든 CRL 매개변수를 시스템 기본값으로 되돌리려면 crl configure 컨피그레이션 모드에서 **default** 명령을 사용합니다.

default

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Crl configure 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령의 호출은 활성 컨피그레이션의 일부가 되지 않습니다. crl configure 컨피그레이션 모드는 crypto ca trustpoint 컨피그레이션 모드에서 액세스할 수 있습니다. 이 매개변수는 LDAP 서버에서 필요할 때만 사용됩니다.

예

다음 예에서는 ca-crl 컨피그레이션 모드를 시작하고 CRL 명령의 값을 기본값으로 되돌립니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# default
ciscoasa(ca-crl)#
```

관련 명령

명령	설명
crl configure	crl configure 컨피그레이션 모드를 시작합니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.
protocol ldap	LDAP을 CRL 검색 방법으로 지정합니다.

default(interface)

인터페이스 명령을 시스템 기본값으로 되돌리려면 인터페이스 컨피그레이션 모드에서 **default** 명령을 사용합니다.

default *command*

구문 설명

command	기본값으로 설정하려는 명령을 지정합니다. 예: **default activation key**

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 런타임 명령입니다. 이 명령을 입력하더라도 활성 컨피그레이션의 일부가 되지 않습니다.

예

다음 예에서는 인터페이스 컨피그레이션 모드를 시작하고 보안 레벨을 기본값으로 되돌립니다.

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# default security-level
```

관련 명령

명령	설명
interface	인터페이스 컨피그레이션 모드를 시작합니다.

default(OSPFv3)

OSPFv3 매개변수를 기본값으로 되돌리려면 라우터 컨피그레이션 모드에서 **default** 명령을 사용합니다.

default [area | auto-cost | default-information | default-metric | discard-route | distance | distribute-list | ignore | log-adjacency-changes | maximum-paths | passive-interface | redistribute | router-id | summary-prefix | timers]

구문 설명

area	(선택 사항) OSPFv3 영역 매개변수를 지정합니다.
auto-cost	(선택 사항) 대역폭에 따라 OSPFv3 인터페이스 비용을 지정합니다.
default-information	(선택 사항) 기본 정보를 배포합니다.
default-metric	(선택 사항) 재배포되는 경로의 메트릭을 지정합니다.
discard-route	(선택 사항) discard-route 설치를 활성화하거나 비활성화합니다.
distance	(선택 사항) 관리 영역을 지정합니다.
distribute-list	(선택 사항) 라우팅 업데이트에서 네트워크를 필터링합니다.
ignore	(선택 사항) 특정 이벤트를 무시합니다.
log-adjacency-changes	(선택 사항) 인접성 상태의 변경 사항을 기록합니다.
maximum-paths	(선택 사항) 다중 경로를 통해 패킷을 전달합니다.
passive-interface	(선택 사항) 인터페이스에서 라우팅 업데이트를 억제합니다.
redistribute	(선택 사항) 다른 라우팅 프로토콜의 IPv6 접두사를 재배포합니다.
router-id	(선택 사항) 지정된 라우팅 프로세스의 라우터 ID를 지정합니다.
summary-prefix	(선택 사항) OSPFv3 요약 접두사를 지정합니다.
timers	(선택 사항) OSPFv3 타이머를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

OSPFv3 매개변수 기본값을 재설정하는 데 이 명령을 사용합니다.

예

다음 예에서는 OSPFv3 타이머 매개변수를 기본값으로 재설정합니다.

```
ciscoasa(config-router)# default timers spf
```

관련 명령

명령	설명
distance	OSPFv3 라우팅 프로세스의 관리 영역을 지정합니다.
default-information originate	OSPFv3 라우팅 도메인에 이르는 기본 외부 경로를 생성합니다.
log-adjacency-changes	OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성합니다.

default(time-range)

absolute 및 **periodic** 명령의 기본 설정을 복원하려면 시간 범위 컨피그레이션 모드에서 **default** 명령을 사용합니다.

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

구문 설명

absolute	시간 범위가 유효한 절대 시간을 정의합니다.
days-of-the-week	이 인수의 첫 번째는 해당 시간 범위가 유효한 첫 번째 날 또는 요일을 나타냅니다. 두 번째는 해당문이 유효한 마지막 날 또는 요일을 나타냅니다. 이 인수는 Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday 중 하나이거나 이들의 조합일 수 있습니다. 다음 값도 가능합니다. • daily—Monday부터 Sunday까지 • weekdays—Monday부터 Friday까지 • weekend—Saturday, Sunday 그 주의 종료일이 시작일과 동일할 경우 생략해도 됩니다.
periodic	시간 범위 기능을 지원하는 기능에 대한 반복적(주간) 시간 범위를 지정합니다.
time	HH:MM 형식으로 시간을 지정합니다. 예를 들어, 8:00은 오전 8:00입니다. 그리고 20:00은 오후 8:00입니다.
to	"시작 시간부터 종료 시간까지"의 범위를 완성하려면 **to** 키워드를 입력해야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
시간 범위 컨피그레이션	•	•	•	•	

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

end days-of-the-week 값이 시작일 값과 동일할 경우 생략해도 됩니다.

time-range 명령에서 **absolute** 및 **periodic** 값이 모두 지정된 경우, 절대 시작 시간에 도달한 후에야 **periodic** 명령이 평가되며 절대 종료 시간에 도달하면 더 이상 평가가 이루어지지 않습니다.

시간 범위 기능은 ASA의 시스템 클록을 사용합니다. 그러나 이 기능은 NTP 동기화를 사용할 때 가장 효과적입니다.

예

다음 예에서는 **absolute** 키워드의 기본 동작을 복원하는 방법을 보여줍니다.

```
ciscoasa(config-time-range)# default absolute
```

관련 명령

명령	설명
absolute	시간 범위가 유효한 절대 시간을 정의합니다.
periodic	시간 범위 기능을 지원하는 기능에 대한 반복적(주간) 시간 범위를 지정합니다.
time-range	시간을 기준으로 한 ASA에 대한 액세스 제어를 정의합니다.

default user group

Cloud Web Security의 경우 ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없을 때 사용할 기본 사용자 이름 및/또는 그룹을 지정하려면 매개변수 컨피그레이션 모드에서 **default user group** 명령을 사용합니다. 기본 사용자 또는 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다. 먼저 **policy-map type inspect scansafe** 명령을 입력하여 매개변수 컨피그레이션 모드에 액세스할 수 있습니다.

default {[user *username*] **[group** *groupname*]}

no default [user *username*] **[group** *groupname*]

구문 설명

username	기본 사용자 이름을 지정합니다.
groupname	기본 그룹 이름을 지정합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없을 경우 기본 사용자 및/또는 그룹이 HTTP 헤더에 포함됩니다.

예

다음 예에서는 기본 이름을 "Boulder", 그룹 이름을 "Cisco"로 설정합니다.

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default name Boulder group Cisco
```

관련 명령

명령	설명
class-map type inspect scansafe	화이트리스트에 있는 사용자 및 그룹에 대한 검사 클래스 맵을 만듭니다.
http[**s**] (parameters)	검사 정책 맵의 서비스 유형을 HTTP 또는 HTTPS로 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	어떤 화이트리스트에 대해 사용자 또는 그룹을 매칭합니다.
policy-map type inspect scansafe	규칙에 대한 필수 매개변수를 구성하고 선택적으로 화이트리스트를 식별할 수 있도록 검사 정책 맵을 만듭니다.
retry-count	재시도 카운터 값을 입력합니다. 이는 ASA에서 Cloud Web Security 프록시 서버의 가용성을 확인하기 위해 폴링할 때까지 기다리는 시간입니다.
scansafe	다중 컨텍스트 모드에서 컨텍스트별 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN 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 연결할 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.

default-acl

PV(posture validation)에 실패한 NAC Framework 세션에 대한 기본 ACL로 사용할 ACL을 지정하려면 nac-policy-nac-framework 컨피그레이션 모드에서 **default-acl** 명령을 사용합니다. NAC 정책에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

[no] default-acl *acl-name*

구문 설명

acl-name	세션에 적용할 액세스 제어 목록의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Nac-policy-nac-framework 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
8.0(2)	"nac-"가 명령 이름에서 삭제되었습니다. 이 명령이 group-policy 컨피그레이션 모드에서 nac-policy-nac-framework 컨피그레이션 모드로 이동했습니다.

사용 지침

각 그룹 정책은 해당 정책에 매칭되고 NAC 기준에 부합하는 호스트에 적용될 기본 ACL을 가리킵니다. ASA는 PV에 앞서 NAC 기본 ACL을 적용합니다. ASA는 PV를 마치고 기본 ACL을 원격 호스트의 Access Control Server에서 얻은 ACL로 대체합니다. PV가 실패하면 기본 ACL을 유지합니다.

클라이언트리스 인증이 활성화된 경우(기본 설정) ASA는 NAC 기본 ACL도 적용합니다.

예

다음 예에서는 PV가 성공하기 전에 적용할 ACL로 acl-1을 지정합니다.

```
ciscoasa(config-group-policy)# default-acl acl-1
ciscoasa(config-group-policy)
```

다음 예에서는 기본 그룹 정책에서 ACL을 상속합니다.

```
ciscoasa(config-group-policy)# no default-acl
ciscoasa(config-group-policy)
```

관련 명령

명령	설명
nac-policy	Cisco NAC 정책을 생성하여 액세스하고 그 유형을 지정합니다.
nac-settings	그룹 정책에 NAC 정책을 지정합니다.
debug nac	NAC Framework 이벤트의 로깅을 활성화합니다.
show vpn-session_summary.db	IPsec, WebVPN, NAC 세션의 수를 표시합니다.
show vpn-session.db	NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.

default enrollment

모든 등록 매개변수를 시스템 기본값으로 되돌리려면 crypto ca trustpoint 컨피그레이션 모드에서 **default enrollment** 명령을 사용합니다.

default enrollment

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Crypto ca trustpoint 컨피그레이션	•	•	•	•	•

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령의 호출은 활성 컨피그레이션의 일부가 되지 않습니다.

예

다음 예에서는 trustpoint central에 대해 crypto ca trustpoint 컨피그레이션 모드를 시작하고 trustpoint central의 모든 등록 매개변수를 기본값으로 되돌립니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# default enrollment
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
clear configure crypto ca trustpoint	모든 신뢰 지점을 제거합니다.
crl configure	crl 컨피그레이션 모드를 시작합니다.
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.

default-domain

그룹 정책의 사용자에 대해 기본 도메인 이름을 설정하려면 group-policy 컨피그레이션 모드에서 **default-domain** 명령을 사용합니다. 도메인 이름을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

default-domain {value *domain-name* **| none}**

no default-domain [*domain-name***]**

구문 설명

none	기본 도메인 이름이 없음을 나타냅니다. 기본 도메인 이름을 null 값으로 설정합니다. 즉 기본 도메인 이름을 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 기본 도메인 이름을 상속할 수 없게 합니다.
value *domain-name*	그룹의 기본 도메인 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

사용자가 도메인 이름을 상속할 수 없게 하려면 **default-domain none** 명령을 사용합니다.

ASA는 기본 도메인 이름을 AnyConnect Secure Mobility Client 또는 레거시 VPN 클라이언트(IPsec/IKEv1)에 전달하여 도메인 필드가 빠진 DNS 쿼리에 추가하게 합니다. 이 도메인 이름은 터널링된 패킷에만 적용됩니다. 기본 도메인 이름이 없을 때 사용자는 기본 그룹 정책의 기본 도메인 이름을 상속합니다.

기본 도메인 이름에는 영숫자, 하이픈(-), 마침표(.)만 사용할 수 있습니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책을 위해 FirstDomain이라는 기본 도메인 이름을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# default-domain value FirstDomain
```

관련 명령

명령	설명
split-dns	스플릿 터널을 통해 확인되는 도메인 목록을 제공합니다.
split-tunnel-network-list	ASA에서 터널링이 필요한 네트워크와 그렇지 않은 네트워크를 구별하는 데 사용하는 액세스 목록을 지정합니다.
split-tunnel-policy	IPsec 클라이언트에서 조건에 따라 암호화된 형태로 IPsec 터널을 통해 또는 일반 텍스트 형태로 네트워크 인터페이스에 패킷을 전달할 수 있게 합니다.

default-group-policy

사용자가 기본적으로 상속하는 특성의 집합을 지정하려면 tunnel-group general-attributes 컨피그레이션 모드에서 **default-group-policy** 명령을 사용합니다. 기본 그룹 정책 이름을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

default-group-policy *group-name*

no default-group-policy *group-name*

구문 설명

group-name	기본 그룹의 이름을 지정합니다.

기본값

기본 그룹 이름은 DfltGrpPolicy입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

버전	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	webvpn 컨피그레이션 모드의 **default-group-policy** 명령은 더 이상 사용되지 않습니다. tunnel-group general-attributes 모드의 **default-group-policy** 명령으로 대체되었습니다.

사용 지침

버전 7.1(1)의 webvpn 컨피그레이션 모드에서 이 명령을 입력하면 tunnel-group general-attributes 모드의 동일한 명령으로 변환됩니다.

기본 그룹 정책인 DfltGrpPolicy는 ASA의 초기 컨피그레이션을 함께 제공합니다. 이 특성을 모든 터널 그룹 유형에 적용할 수 있습니다.

예

config-general 컨피그레이션 모드에서 입력되는 다음 예에서는 IPsec LAN-to-LAN 터널 그룹인 "standard-policy"에 대해 사용자가 기본적으로 상속하는 특성의 집합을 지정합니다. 이 명령 집합은 어카운팅 서버, 인증 서버, 권한 부여 서버, 주소 풀을 정의합니다.

```
ciscoasa(config)# tunnel-group standard-policy type ipsec-ra
ciscoasa(config)# tunnel-group standard-policy general-attributes
ciscoasa(config-tunnel-general)# default-group-policy first-policy
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
group-policy	그룹 정책을 만들거나 수정합니다.
show running-config tunnel group	모든 터널 그룹 또는 특정 터널 그룹의 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group general-attributes	명명된 터널 그룹의 일반 특성을 지정합니다.

default-group-policy(webvpn)

WebVPN 또는 이메일 프록시 컨피그레이션에서 그룹 정책을 지정하지 않을 때 사용할 그룹 정책의 이름을 지정하려면 여러 컨피그레이션 모드에서 **default-group-polic***y* 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

default-group-policy *groupname*

no default-group-policy

구문 설명

groupname	기본 그룹 정책으로 사용할 이미 구성된 그룹 정책을 지정합니다. 그룹 정책을 구성하려면 **group-policy** 명령을 사용합니다.

기본값

*DfltGrpPolicy*라는 기본 그룹 정책은 항상 ASA에 있습니다. 이 **default-group-polic***y* 명령을 사용하면 WebVPN 및 이메일 프록시 세션의 기본 그룹 정책으로 생성한 그룹 정책으로 대체할 수 있습니다. DfltGrpPolicy를 수정하는 방법도 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

버전	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	이 명령은 webvpn 컨피그레이션 모드에서 더 이상 사용되지 않으며 tunnel-group general-attributes 컨피그레이션 모드로 이동했습니다.

사용 지침

WebVPN, IMAP4S, POP3S, SMTPS 세션은 지정된 또는 기본 그룹 정책이 필요합니다. WebVPN에서는 webvpn 컨피그레이션 모드에서 이 명령을 사용합니다. 이메일 프록시는 해당 이메일 프록시 모드에서 이 명령을 사용합니다.

버전 7.1(1)의 webvpn 컨피그레이션 모드에서 이 명령을 입력하면 tunnel-group general-attributes 컨피그레이션 모드의 동일한 명령으로 변환됩니다.

시스템 DefaultGroupPolicy는 수정 가능하지만 삭제할 수는 없습니다. 다음 AVP가 있습니다.

특성	기본값
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn attributes	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	none

예

다음 예에서는 WebVPN을 위해 WebVPN7이라는 기본 그룹 정책을 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

WebVPN 사용자의 기본 유휴 타이머 값을 설정하려면 webvpn 컨피그레이션 모드에서 **default-idle-timeout** 명령을 사용합니다. 컨피그레이션에서 기본 유휴 타이머 값을 제거하고 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

default-idle-timeout *seconds*

no default-idle-timeout

구문 설명

seconds	유휴 타이머의 시간(초)을 지정합니다. 최소값은 60초, 최대값은 1일(86400초)입니다.

기본값

1800초(30분)

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서는 어떤 사용자에 대해 유휴 타이머가 정의되지 않은 경우, 그 값이 0인 경우 또는 그 값이 유효 범위에 속하지 않을 경우 여기에 설정한 값을 사용합니다. 기본 유휴 타이머는 오래된 세션을 차단합니다.

이 명령을 짧은 기간으로 설정하는 것이 좋습니다. 쿠키가 비활성화된 브라우저(또는 쿠키에 대한 프롬프트를 표시한 다음 쿠키를 거부하는 브라우저)에서 사용자가 연결되지 않았음에도 세션 데이터베이스에 나타나는 상황이 생길 수 있습니다. 최대 허용 연결 수가 1로 설정된 경우(**vpn-simultaneous-logins** 명령) 사용자는 다시 로그인할 수 없습니다. 데이터베이스에서 최대 연결 횟수에 도달했음을 알리기 때문입니다. 유휴 타이머를 낮게 설정하면 그러한 오류 세션이 곧 사라지므로 사용자가 다시 로그인할 수 있습니다.

예

다음 예에서는 기본 유휴 타이머를 1200초(20분)로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# default-idle-timeout 1200
```

관련 명령

명령	설명
vpn-simultaneous-logins	동시 VPN 세션의 최대 허용 횟수를 설정합니다.

default-information(EIGRP)

EIGRP 라우팅 프로세스의 후보 기본 경로 정보를 제어하려면 라우터 컨피그레이션 모드에서 **default-information** 명령을 사용합니다. 수신 또는 발신 업데이트에서 EIGRP 후보 기본 경로 정보를 억제하려면 이 명령의 **no** 형식을 사용합니다.

default-information {in | out} [*acl-name***]**

no default-information {in | out}

구문 설명

acl-name	(선택 사항) 명명된 표준 액세스 목록을 지정합니다.
in	EIGRP에서 외부 기본 라우팅 정보를 받아들이도록 구성합니다.
out	EIGRP에서 외부 라우팅 정보를 알리도록 구성합니다.

기본값

외부 경로가 승인되고 전송됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

이 명령의 **no** 형식 또는 액세스 목록이 지정된 **default-information** 명령이 실행 중인 컨피그레이션에 나타납니다. 기본적으로 후보 기본 라우팅 정보가 승인되고 전송되기 때문입니다. 이 명령의 **no** 형식은 *acl-name* 인수를 사용하지 않습니다.

예

다음 예에서는 외부 또는 후보 기본 경로 정보의 수신을 비활성화합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no default-information in
```

관련 명령

명령	설명
router eigrp	EIGRP 라우팅 프로세스를 생성하고 이 프로세스에 대한 컨피그레이션 모드로 들어갑니다.

default-information originate(BGP)

BGP(Border Gateway Protocol) 라우팅 프로세스에서 기본 경로(네트워크 0.0.0.0)를 배포하도록 구성하려면 주소군 컨피그레이션 모드에서 **default-information originate** 명령을 사용합니다. 기본 경로의 알림을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

default-information originate

no default-information originate

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

default-information originate 명령은 BGP 라우팅 프로세스에서 기본 경로(네트워크 0.0.0.0)를 알림을 발송하도록 구성하는 데 사용합니다. 이 컨피그레이션을 완료하려면 재배포문도 구성해야 합니다. 그러지 않으면 기본 경로가 광고되지 않습니다.

BGP의 **default-information originate** 명령의 컨피그레이션은 **network(BGP)** 명령의 컨피그레이션과 비슷합니다. 그러나 **default-information originate** 명령에서는 경로 0.0.0.0의 명시적 재배포가 필요합니다. **network** 명령에서는 IGP(Interior Gateway Protocol) 라우팅 테이블에 경로 0.0.0.0만 있어야 합니다. 이런 이유로 **network** 명령을 선호합니다.

참고 **default-information originate** 명령은 **neighbor default-originate** 명령이 있는 동일한 라우터에서 구성할 수 없습니다. 둘 중 하나만 구성해야 합니다.

예

다음 예제에서는 라우터가 OSPF의 기본 경로를 BGP 라우팅 프로세스에 재배포하도록 구성됩니다.

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# default-information originate
ciscoasa(config-router-af)# redistribute ospf 100
```

관련 명령

명령	설명
network	BGP 및 다중 프로토콜 BGP 라우팅 프로세스에서 광고할 네트워크를 지정합니다.
neighbor default-originate	BGP 스피커(로컬 라우터)에서 기본 경로 0.0.0.0을 인접 디바이스로 전송하도록 허용합니다.

default-information originate(OSPFv2 and OSPFv3)

OSPFv2 또는 OSPFv3 라우팅 도메인에 이르는 기본 외부 경로를 생성하려면 라우터 컨피그레이션 모드 또는 IPv6 라우터 컨피그레이션 모드에서 **default-information originate** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

default-information originate [always] [metric *value***] [metric-type {1 | 2}] [route-map** *map-name***]**

no default-information originate [[always] [metric *value***] [metric-type {1 | 2}] [route-map** *map-name***]]**

구문 설명

always	(선택 사항) 소프트웨어의 기본 경로 유무와 상관없이 항상 기본 경로를 광고합니다.
metric *value*	(선택 사항) OSPF 기본 메트릭 값을 0~16777214의 범위에서 지정합니다.
metric-type {**1** | **2**}	(선택 사항) OSPF 라우팅 도메인에 광고되는 기본 경로와 연결된 외부 링크 유형을 지정합니다. 유효한 값은 다음과 같습니다. • **1** — Type 1 외부 경로 • **2** — Type 2 외부 경로
route-map *map-name*	(선택 사항) 적용할 경로 맵의 이름을 지정합니다.

기본값

기본값은 다음과 같습니다.

- **metric** *value*는 1입니다.
- **metric-type**은 2입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
IPv6 라우터 컨피그레이션	• 예	—	• 예	—	—
라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.0(1)	OSPFv3에 대한 지원을 추가했습니다.

사용 지침

선택 사항인 키워드 및 인수와 함께 이 명령의 **no** 형식을 사용하면 선택적 정보만 명령에서 제거합니다. 예를 들어, **no default-information originate metric** *3* 명령을 입력하면 실행 중인 컨피그레이션에서 **metric** *3* 옵션이 명령에서 제거됩니다. 실행 중인 컨피그레이션에서 전체 명령을 제거하려면 어떤 옵션도 없이 이 명령의 **no** 형식, 즉 **no default-information originate**를 사용합니다.

예

다음 예에서는 **default-information originate** 명령을 선택 사항인 메트릭 및 메트릭 유형과 함께 사용하는 방법을 보여줍니다.

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
ciscoasa(config-rtr)#
```

관련 명령

명령	설명
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 OSPFv2 명령을 표시합니다.
ipv6 router ospf	IPv6 라우터 컨피그레이션 모드를 시작합니다.
show running-config ipv6 router	전역 라우터 컨피그레이션에서 OSPFv3 명령을 표시합니다.

default-information originate(RIP)

RIP에 대한 기본 경로를 생성하려면 라우터 컨피그레이션 모드에서 **default-information originate** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

default-information originate [route-map *name***]**

no default-information originate [route-map *name***]]**

구문 설명

route-map *name*	(선택 사항) 적용할 경로 맵의 이름입니다. 경로 맵이 충족되면 라우팅 프로세스에서 기본 경로를 생성합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

default-information originate 명령에서 참조한 경로 맵에서는 확장 액세스 목록을 사용할 수 없습니다. 표준 액세스 목록만 사용 가능합니다.

예

다음 예에서는 RIP에 대한 기본 경로를 생성하는 방법을 보여줍니다.

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# default-information originate
```

관련 명령

명령	설명
router rip	RIP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

default-language

클라이언트리스 SSL VPN 페이지에 표시될 기본 언어를 설정하려면 webvpn 컨피그레이션 모드에서 **default-language** 명령을 사용합니다.

default-language *language*

구문 설명

language	이전에 가져온 변환 테이블의 이름을 지정합니다.

기본값

기본 언어는 en-us(미국 영어)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ASA에서는 브라우저 기반의 클라이언트리스 SSL VPN 연결을 시작하는 사용자에게 표시되는 포털과 화면 그리고 AnyConnect VPN Client 사용자에게 표시되는 사용자 인터페이스를 위한 언어 변환을 제공합니다.

클라이언트리스 SSL VPN 사용자가 로그인하기 전에 처음으로 ASA에 연결할 때 기본 언어가 표시됩니다. 따라서 표시되는 언어는 터널 그룹 또는 그룹 정책 설정 및 참조하는 임의의 사용자 지정에 따라 달라집니다.

예

다음 예에서는 *Sales*라는 이름을 사용하여 기본 언어를 중국어로 변경합니다.

```
ciscoasa(config-webvpn)# default-language zh
```

관련 명령

명령	설명
import webvpn translation-table	변환 테이블을 가져옵니다.
revert	캐시 메모리에서 변환 테이블을 제거합니다.
show import webvpn translation-table	가져온 변환 테이블에 대한 정보를 표시합니다.

default-metric

재배포된 경로에 대한 EIGRP 메트릭을 지정하려면 라우터 컨피그레이션 모드에서 **default-metric** 명령을 사용합니다. 기본값으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

구문 설명

bandwidth	경로의 최소 대역폭이며, 단위는 초당 킬로바이트입니다. 유효한 값은 1~4294967295입니다.
delay	경로 지연 시간이며, 단위는 10마이크로초입니다. 유효한 값은 1~4294967295입니다.
loading	경로의 유효 대역폭이며, 1~255의 숫자로 표시됩니다(255는 100% 로딩).
mtu	MTU에 대해 허용되는 최소값이며, 단위는 바이트입니다. 유효한 값은 1~65535입니다.
reliability	패킷 전송의 성공률이며 0~255의 숫자로 표시됩니다. 값이 255이면 100% 신뢰성을 나타내며, 0이면 신뢰성이 없는 것입니다.

기본값

연결된 경로만 기본 메트릭 없이 재배포할 수 있습니다. 재배포된 연결된 경로의 메트릭은 0으로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

EIGRP에 프로토콜을 재배포하려면 기본 메트릭을 사용해야 합니다. 단, **metric** 키워드와 특성을 **redistribute** 명령에서 사용하는 경우는 제외합니다. 메트릭의 기본값은 다양한 네트워크에 적합하도록 신중하게 설정된 것입니다. 이 값을 변경할 때 각별히 주의하십시오. 고정 경로에서 재배포하는 경우에만 동일한 메트릭을 유지할 수 있습니다.

IPv6 활성 인터페이스에서 허용되는 최소 MTU는 1280바이트입니다. 그러나 IPsec이 인터페이스에서 활성화된 경우, IPsec 암호화의 오버헤드 때문에 MTU가 1380보다 작은 값으로 설정되어야 합니다. 1380바이트보다 낮게 인터페이스를 설정하면 패킷이 폐기될 수 있습니다.

예

다음 예에서는 재배포 RIP 경로 메트릭이 EIGRP 메트릭으로 변환되는 방법을 보여줍니다. 사용되는 값은 bandwidth = 1000, delay = 100, reliability = 250, loading = 100, MTU = 1500입니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 172.16.0.0
ciscoasa(config-router)# redistribute rip
ciscoasa(config-router)# default-metric 1000 100 250 100 1500
```

관련 명령

명령	설명
router eigrp	EIGRP 라우팅 프로세스를 생성하고 이 프로세스에 대한 라우터 컨피그레이션 모드로 들어갑니다.
redistribute (EIGRP)	EIGRP 라우팅 프로세스에 경로를 재배포합니다.

delay

인터페이스의 지연 시간 값을 설정하려면 인터페이스 컨피그레이션 모드에서 **delay** 명령을 사용합니다. 지연 시간의 기본값으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

delay *delay-time*

no delay

구문 설명

delay-time	지연 시간이며, 단위는 10마이크로초입니다. 유효한 값은 1~16777215입니다.

기본값

기본 지연 시간은 인터페이스 유형에 따라 달라집니다. 인터페이스의 지연 시간 값을 확인하려면 **show interface** 명령을 사용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

10마이크로초 단위로 값을 입력합니다. **show interface** 출력에 표시되는 지연 시간의 값은 마이크로초 단위입니다.

예

다음 예에서는 인터페이스의 지연 시간을 기본값인 1000에서 2000으로 변경합니다. 명령이 지연 시간의 값에 어떤 영향을 주는지 알아보기 위해 잘린 **show interface** 명령의 출력이 **delay** 명령의 앞뒤에 포함되었습니다. 지연 시간의 값은 **show interface** 출력의 두 번째 줄, DLY 레이블 다음에 표시됩니다.

지연 시간의 값을 2000으로 변경하기 위해 입력하는 명령은 **delay 2000**이 아니라 **delay 200**입니다. **delay** 명령과 함께 입력하는 값은 10마이크로초 단위이고, **show interface** 출력에서는 마이크로초 단위로 표시하기 때문입니다.

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# show interface Ethernet0/0
```

```
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed

ciscoasa(config-if)# delay 200
ciscoasa(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

관련 명령

명령	설명
show interface	인터페이스 통계 및 설정을 표시합니다.

delete

플래시 메모리에서 파일을 삭제하려면 특별 권한 EXEC 모드에서 **delete** 명령을 사용합니다.

delete [/noconfirm] [/recursive] [/replicate] [disk0: | disk1: | flash:] [*path/***] *filename***

구문 설명

/noconfirm	(선택 사항) 확인 프롬프트를 표시하지 않습니다.
/recursive	(선택 사항) 지정된 파일을 모든 하위 디렉토리에서 반복적으로 삭제합니다.
/replicate	(선택 사항) 지정된 파일을 대기 유닛에서 삭제합니다.
disk0:	(선택 사항) 내부 플래시 메모리를 지정합니다.
disk1:	(선택 사항) 외부 플래시 메모리 카드를 지정합니다.
filename	삭제할 파일의 이름을 지정합니다.
flash:	(선택 사항) 내부 플래시 메모리를 지정합니다. 이 키워드는 **disk0**과 동일합니다.
path/	(선택 사항) 파일의 경로를 지정합니다.

기본값

디렉토리를 지정하지 않으면 현재 작업 디렉토리가 기본적으로 사용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

경로가 지정되지 않을 경우 현재 작업 디렉토리에서 파일이 삭제됩니다. 파일 삭제 시 와일드카드를 사용할 수 있습니다. 파일을 삭제할 때 파일 이름과 함께 프롬프트가 표시되며 삭제를 확인해야 합니다.

예

다음 예에서는 현재 작업 디렉토리에서 test.cfg라는 파일을 삭제하는 방법을 보여줍니다.

```
ciscoasa# delete test.cfg
```

관련 명령

명령	설명
cd	현재 작업 디렉토리를 지정된 디렉토리로 변경합니다.
rmdir	파일 또는 디렉토리를 제거합니다.
show file	지정된 파일을 표시합니다.

deny-message

성공적으로 WebVPN에 로그인했지만 VPN 권한이 없는 원격 사용자에게 전달되는 메시지를 변경하려면 group-webvpn 컨피그레이션 모드에서 **deny-message value** 명령을 사용합니다. 원격 사용자가 메시지를 받지 않도록 문자열을 제거하려면 이 명령의 **no** 형식을 사용합니다.

deny-message value *string*

no deny-message value

구문 설명

string	특수 문자, 공백, 구두점을 포함하여 영숫자 491자까지 가능합니다.

기본값

기본 거부 메시지는 "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	이 명령은 tunnel-group webvpn 컨피그레이션 모드에서 group-webvpn 컨피그레이션 모드로 이동했습니다.

사용 지침

이 명령을 입력하기 전에 글로벌 컨피그레이션 모드에서 **group-policy** *name* **attributes** 명령을 입력하고 **webvpn** 명령을 입력해야 합니다 (이 단계에서는 정책 이름을 이미 생성했다고 가정합니다.).

no deny-message none 명령은 group-webvpn 컨피그레이션에서 특성을 제거합니다. 정책이 특성 값을 상속합니다.

deny-message value 명령에서 문자열을 입력할 때 명령이 줄바꿈하더라도 계속 입력합니다.

VPN 세션에 사용된 터널 정책과 상관없이 원격 사용자가 로그인하면 그 브라우저에 텍스트가 나타납니다.

예

다음 예에서는 group2라는 내부 그룹 정책을 생성하는 첫 번째 명령을 보여줍니다. 그 다음 명령에서는 이 정책의 거부 메시지를 수정합니다.

```
ciscoasa(config)# group-policy group2 internal
ciscoasa(config)# group-policy group2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
you have not been granted rights to use the VPN features. Contact your administrator for
more information."
ciscoasa(config-group-webvpn)
```

관련 명령

명령	설명
clear configure group-policy	모든 그룹 정책 컨피그레이션을 제거합니다.
group-policy	그룹 정책을 만듭니다.
group-policy attributes	group-policy attribute 컨피그레이션 모드를 시작합니다.
show running-config group-policy	명명된 정책에 대해 실행 중인 그룹 정책 컨피그레이션을 표시합니다.
webvpn	group-policy webvpn 컨피그레이션 모드를 시작합니다.

deny version

SNMP 트래픽의 특정 버전을 거부하려면 snmp-map 컨피그레이션 모드에서 **deny version** 명령을 사용합니다. 이 명령을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

deny version *version*

no deny version *version*

구문 설명

version	ASA에서 폐기하는 SNMP 트래픽의 버전을 지정합니다. 허용되는 값은 **1**, **2**, **2c**, **3**입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Snmp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

SNMP 트래픽을 특정 버전의 SNMP로 제한하려면 **deny version** 명령을 사용합니다. 이전 버전의 SNMP는 안전성이 떨어지므로, 보안 정책에 따라 SNMP 트래픽이 버전 2로 제한될 수 있습니다. SNMP 맵 내에서 **deny version** 명령을 사용합니다. 이 맵은 **snmp-map** 명령으로 구성하는데, 글로벌 컨피그레이션 모드에서 **snmp-map** 명령을 입력하여 액세스할 수 있습니다. SNMP 맵을 만든 다음 **inspect snmp** 명령을 사용하여 맵을 활성화한 다음 **service-policy** 명령을 사용하여 하나 이상의 인터페이스에 적용합니다.

예

다음 예에서는 SNMP 트래픽을 식별하고 SNMP 맵과 정책을 정의하고 외부 인터페이스에 정책을 적용하는 방법을 보여줍니다.

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

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
inspect snmp	SNMP 애플리케이션 검사를 활성화합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.
snmp-map	SNMP 맵을 정의하고 SNMP 맵 컨피그레이션 모드를 활성화합니다.
service-policy	하나 이상의 인터페이스에 정책 맵을 적용합니다.

description

명명된 컨피그레이션 유닛(예: 컨텍스트, 객체 그룹, DAP 레코드)에 대한 설명을 추가하려면 여러 컨피그레이션 모드에서 **description** 명령을 사용합니다. 설명을 제거하려면 이 명령의 **no** 형식을 사용합니다.

description *text*

no description

구문 설명

text	최대 200자의 텍스트 문자열로 설명을 설정합니다. 이 설명으로 해당 컨피그레이션에 유익한 정보를 추가할 수 있습니다. dynamic-access-policy-record 모드는 최대 길이가 80자입니다. 이벤트 관리자 애플릿의 경우 최대 길이는 256자입니다. 문자열에 물음표(?)를 포함하려면 **Ctrl-V**를 입력한 다음 문자열을 입력해야 CLI 도움말이 호출되지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

이 명령은 여러 컨피그레이션 모드에서 사용할 수 있습니다.

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0(2)	dynamic-access-policy-record 컨피그레이션 모드에 대한 지원을 추가했습니다.
9.2(1)	이벤트 관리자 애플릿 컨피그레이션 모드에 대한 지원을 추가했습니다.

예

다음 예에서는 "Administration" 컨텍스트 컨피그레이션에 설명을 추가합니다.

```
ciscoasa(config)# context administrator
ciscoasa(config-context)# description This is the admin context.
ciscoasa(config-context)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-context)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-context)# config-url flash://admin.cfg
```

관련 명령

명령	설명
class-map	**policy-map** 명령에서 작업을 적용할 트래픽을 지정합니다.
context	시스템 컨피그레이션에서 보안 컨텍스트를 만들고 컨텍스트 컨피그레이션 모드를 시작합니다.
gtp-map	GTP 검사 엔진의 매개변수를 제어합니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
object-group	**access-list** 명령에 포함할 트래픽을 지정합니다.
policy-map	**class-map** 명령으로 지정된 트래픽에 적용할 작업을 지정합니다.

dhcp client route distance

DHCP를 통해 습득한 경로의 관리 영역을 구성하려면 인터페이스 컨피그레이션 모드에서 **dhcp client route distance** 명령을 사용합니다. 기본 설정으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

dhcp client route distance *distance*

no dhcp client route distance *distance*

구문 설명

distance	DHCP를 통해 습득한 경로에 적용할 관리 영역입니다. 유효한 값은 1부터 255까지입니다.

기본값

DHCP를 통해 습득한 경로는 기본적으로 관리 영역 1이 지정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

dhcp client route distance 명령은 DHCP를 통해 경로가 습득된 경우에만 확인합니다. DHCP를 통해 경로를 습득한 다음에 **dhcp client route distance** 명령을 입력한 경우, 지정된 관리 영역은 이미 습득한 경로에 영향을 주지 않습니다. 명령을 입력한 다음에 습득한 경로만 지정된 관리 영역을 갖습니다.

DHCP를 통해 경로를 습득하려면 **ip address dhcp** 명령에서 **setroute** 옵션을 지정해야 합니다.

DHCP가 여러 인터페이스에서 구성된 경우 각 인터페이스에서 **dhcp client route distance** 명령을 사용하여 설치된 경로의 우선순위를 나타내야 합니다.

예

다음 예에서는 GigabitEhternet0/2에서 DHCP를 통해 기본 경로를 습득합니다. 이 경로를 추적하려면 엔트리 객체 1을 추적합니다. SLA 작업에서는 외부 인터페이스의 10.1.1.1 게이트웨이가 사용 가능한지 모니터링합니다. SLA 작업이 실패할 경우 GigabitEthernet0/3에서 DHCP를 통해 습득한 백업 경로가 사용됩니다. 백업 경로는 관리 영역 254가 지정됩니다.

```
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)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

관련 명령

명령	설명
dhcp client route track	DHCP를 통해 습득한 경로를 추적 엔트리 객체와 연결합니다.
ip address dhcp	지정된 인터페이스에 DHCP를 통해 습득한 IP 주소를 구성합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.
track rtr	SLA를 폴링할 추적 엔트리를 생성합니다.

dhcp client route track

DHCP 클라이언트에서 추가된 경로를 지정된 추적 객체 번호와 연결하도록 구성하려면 인터페이스 컨피그레이션 모드에서 **dhcp client route track** 명령을 사용합니다. DHCP 클라이언트의 경로 추적을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dhcp client route track *number*

no dhcp client route track

구문 설명

number	추적 엔트리 객체 ID입니다. 유효한 값은 1부터 500까지입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

dhcp client route track 명령은 DHCP를 통해 경로가 습득된 경우에만 확인합니다. DHCP로부터 경로를 습득한 다음에 **dhcp client route track** 명령을 입력한 경우, 이미 습득한 경로는 추적 객체와 연결되지 않습니다. 다음 두 명령을 정확한 순서로 입력해야 합니다. 반드시 **dhcp client route track** 명령을 먼저 입력한 다음 **ip address dhcp setroute** 명령을 입력합니다. **ip address dhcp setroute** 명령을 이미 입력한 경우 이 명령을 제거하고 앞서 설명한 순서대로 다시 입력합니다. 명령을 입력한 다음에 습득한 경로만 지정된 추적 객체와 연결됩니다.

DHCP를 통해 경로를 습득하려면 **ip address dhcp** 명령에서 **setroute** 옵션을 지정해야 합니다.

DHCP가 여러 인터페이스에서 구성된 경우 각 인터페이스에서 **dhcp client route distance** 명령을 사용하여 설치된 경로의 우선순위를 나타내야 합니다.

예

다음 예에서는 GigabitEhternet0/2에서 DHCP를 통해 기본 경로를 습득합니다. 이 경로를 추적하려면 엔트리 객체 1을 추적합니다. SLA 작업에서는 외부 인터페이스의 10.1.1.1 게이트웨이가 사용 가능한지 모니터링합니다. SLA 작업이 실패할 경우 GigabitEthernet0/3에서 DHCP를 통해 습득한 백업 경로가 사용됩니다. 백업 경로는 관리 영역 254가 지정됩니다.

```
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)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

관련 명령

명령	설명
dhcp client route distance	DHCP를 통해 습득한 경로에 관리 영역을 지정합니다.
ip address dhcp	지정된 인터페이스에 DHCP를 통해 습득한 IP 주소를 구성합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.
track rtr	SLA를 폴링할 추적 엔트리를 생성합니다.

dhcp-client broadcast-flag

ASA에서 DHCP 클라이언트 패킷에 브로드캐스트 플래그를 설정할 수 있게 하려면 글로벌 컨피그레이션 모드에서 **dhcp-client broadcast-flag** 명령을 사용합니다. 브로드캐스트 플래그를 허용하지 않으려면 이 명령의 **no** 형식을 사용합니다.

dhcp-client broadcast-flag

no dhcp-client broadcast-flag

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본적으로 브로드캐스트 플래그는 비활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ip address dhcp 명령을 사용하여 어떤 인터페이스에 대해 DHCP 클라이언트를 활성화할 경우, DHCP 클라이언트에서 IP 주소를 요청하는 discover를 보낼 때 DHCP 패킷 헤더의 브로드캐스트 플래그를 1로 설정하는 데 이 명령을 사용할 수 있습니다. DHCP 서버가 이 브로드캐스트 플래그를 수신하고, 플래그가 1로 설정되었으면 회신 패킷을 브로드캐스트합니다.

no dhcp-client broadcast-flag 명령을 입력한 경우, 브로드캐스트 플래그는 0으로 설정되고 DHCP 서버는 제공된 IP 주소의 클라이언트에 회신 패킷을 유니캐스트합니다.

DHCP 클라이언트는 DHCP 서버가 보낸 브로드캐스트 및 유니캐스트 제안을 모두 받을 수 있습니다.

예

다음 예에서는 브로드캐스트 플래그를 활성화합니다.

```
ciscoasa(config)# dhcp-client broadcast-flag
```

관련 명령

명령	설명
ip address dhcp	인터페이스에서 DHCP 클라이언트를 활성화합니다.
interface	IP 주소를 설정할 수 있도록 인터페이스 컨피그레이션 모드를 시작합니다.
dhcp-client client-id	인터페이스 MAC 주소를 포함하도록 DHCP 요청 패킷 옵션 61을 설정합니다.
dhcp-client update dns	DHCP 클라이언트에 대한 DNS 업데이트를 활성화합니다.

dhcp-client client-id

내부에서 생성된 기본 문자열 대신 MAC 주소를 옵션 61의 DHCP 요청 패킷 내에 저장하게 하려면 글로벌 컨피그레이션 모드에서 **dhcp-client client-id** 명령을 사용합니다. MAC 주소를 허용하지 않으려면 이 명령의 **no** 형식을 사용합니다.

dhcp-client client-id interface *interface_name*

no dhcp-client client-id interface *interface_name*

구문 설명

interface *interface_name*	옵션 61에 대해 MAC 주소를 활성화하려는 인터페이스를 지정합니다.

기본값

기본적으로 옵션 61에는 내부에서 생성된 ASCII 문자열이 사용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ip address dhcp 명령을 사용하여 어떤 인터페이스에 대해 DHCP 클라이언트를 활성화할 경우, 일부 ISP는 옵션 61이 인터페이스 MAC 주소일 것으로 예상합니다. MAC 주소가 DHCP 요청 패킷에 포함되지 않은 경우 IP 주소는 지정되지 않습니다. 옵션 61에 대해 인터페이스 MAC 주소를 포함하려면 **dhcp-client client-id** 명령을 사용합니다.

예

다음 예에서는 외부 인터페이스에 대해 옵션 61의 MAC 주소를 활성화합니다.

```
ciscoasa(config)# dhcp-client client-id interface outside
```

관련 명령

명령	설명
ip address dhcp	인터페이스에서 DHCP 클라이언트를 활성화합니다.
interface	IP 주소를 설정할 수 있도록 인터페이스 컨피그레이션 모드를 시작합니다.
dhcp-client broadcast-flag	DHCP 클라이언트 패킷에서 브로드캐스트 플래그를 설정합니다.
dhcp-client update dns	DHCP 클라이언트에 대한 DNS 업데이트를 활성화합니다.

dhcp-client update dns

DHCP 클라이언트에서 DHCP 서버에 전달하는 업데이트 매개변수를 구성하려면 글로벌 컨피그레이션 모드에서 **dhcp-client update dns** 명령을 사용합니다. DHCP 클라이언트에서 DHCP 서버에 전달하는 매개변수를 제거하려면 이 명령의 **no** 형식을 사용합니다.

dhcp-client update dns [server {both | none}]

no dhcp-client update dns [server {both | none}]

구문 설명

both	클라이언트는 DHCP 서버가 DNS A 및 PTR 리소스 레코드를 모두 업데이트하도록 요청합니다.
none	클라이언트는 DHCP 서버가 DDNS 업데이트를 수행하지 않도록 요청합니다.
server	클라이언트 요청을 수신할 DHCP 서버를 지정합니다.

기본값

기본적으로 ASA는 DHCP 서버가 PTR RR 업데이트만 수행하도록 요청합니다. 클라이언트는 서버에 FQDN 옵션을 보내지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 인터페이스 컨피그레이션 모드에서도 입력할 수 있으나, 하이픈이 사용되지 않습니다. **dhcp client update dns** 명령을 참조하십시오. 인터페이스 모드에서 **dhcp client update dns** 명령을 입력하면 글로벌 컨피그레이션 모드에서 이 명령으로 구성한 설정을 재정의합니다.

예

다음 예에서는 클라이언트가 DHCP 서버에서 A 및 PTR RR 모두 업데이트하지 않게끔 요청하도록 구성합니다.

```
ciscoasa(config)# dhcp-client update dns server none
```

다음 예에서는 클라이언트가 서버에서 A 및 PTR RR 모두 업데이트하게끔 요청하도록 구성합니다.

```
ciscoasa(config)# dhcp-client update dns server both
```

관련 명령

명령	설명
ddns	생성된 DDNS 메서드에 대한 DDNS 업데이트 메서드 유형을 지정합니다.
ddns update	DDNS 업데이트 메서드를 ASA 인터페이스 또는 DDNS 업데이트 호스트 이름과 연결합니다.
ddns update method	DNS 리소스 레코드를 동적으로 업데이트하는 메서드를 생성합니다.
dhcpd update dns	DDNS 업데이트를 수행하도록 DHCP 서버를 활성화합니다.
interval maximum	DDNS 업데이트 메서드에 의한 업데이트 시도의 최대 간격을 구성합니다.

dhcp-network-scope

ASA DHCP 서버에서 이 그룹 정책의 사용자에게 주소를 지정하는 데 사용할 IP 주소의 범위를 지정하려면 group-policy 컨피그레이션 모드에서 **dhcp-network-scope** 명령을 사용합니다. 실행 중인 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

dhcp-network-scope {*ip_address*} | **none**

no dhcp-network-scope

구문 설명

ip_address	DHCP 서버에서 이 그룹 정책의 사용자에게 IP 주소를 지정하는 데 사용할 IP 서브네트워크를 지정합니다.
none	DHCP 서브네트워크를 null 값으로 설정하여 어떤 IP 주소도 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 값을 상속할 수 없게 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Group-policy	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 다른 그룹 정책에서 값을 상속하는 것을 허용합니다. 값을 상속할 수 없게 하려면 **dhcp-network-scope none** 명령을 사용합니다.

예

다음 예에서는 First Group이라는 그룹 정책에 대해 IP 서브네트워크 10.10.85.1을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dhcp-network-scope 10.10.85.1
```

dhcp-server

VPN 터널이 설정될 때 클라이언트에 IP 주소를 지정하는 DHCP 서버에 대한 지원을 구성하려면 command in tunnel-group general-attributes 컨피그레이션 모드에서 **dhcp-server** 명령을 사용합니다. 이 명령을 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

dhcp-server [link-selection | subnet-selection] ip1 [ip2-ip10]

[no] dhcp-server [link-selection | subnet-selection] ip1 [ip2-ip10]

구문 설명

ip1	DHCP 서버의 주소
ip2-ip10	(선택 사항) 추가 DHCP 서버의 주소. 최대 10개를 동일한 명령에서 또는 여러 명령에 분산시켜 지정할 수 있습니다.
link-selection	(선택 사항) ASA에서 DHCP 하위 옵션 5를 보내도록 지정합니다. 이는 RFC 3527에 정의된 릴레이 정보 옵션 82의 링크 선택 하위 옵션입니다. 이 RFC를 지원하는 서버에서만 사용해야 합니다.
subnet-selection	(선택 사항) ASA에서 DHCP 옵션 118을 보내도록 지정합니다. 이는 RFC 3011에 정의된 IPv4 서브넷 선택 옵션입니다. 이 RFC를 지원하는 서버에서만 사용해야 합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0(5)	**link-selection** 및 **subnet-selection** 키워드를 추가했습니다.

사용 지침

원격 액세스 터널 그룹 유형에만 이 특성을 적용할 수 있습니다.

예

config-general 컨피그레이션 모드에서 다음 명령을 입력하면 3개의 DHCP 서버(dhcp1, dhcp2, dhcp3)가 IPsec 원격 액세스 터널 그룹 "remotegrp"에 추가됩니다.

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
ciscoasa(config-tunnel-general)
```

관련 명령

명령	설명
clear-configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel group	모든 터널 그룹 또는 특정 터널 그룹의 터널 그룹 컨피그레이션을 표시합니다.
tunnel-group general-attributes	명명된 터널 그룹의 일반 특성을 지정합니다.

12 장

dhcpd address ~ distribute-list out(BGP) 명령

dhcpd address

DHCP 서버에서 사용하는 IP 주소 풀을 정의하려면 글로벌 컨피그레이션 모드에서 **dhcpd address** 명령을 사용합니다. 기존 DHCP 주소 풀을 제거하려면 이 명령의 **no** 형식을 사용합니다.

dhcpd address *IP_address1*[*-IP_address2*] *interface_name*

no dhcpd address *interface_name*

구문 설명

interface_name	주소 풀이 지정되는 인터페이스입니다.
IP_address1	DHCP 주소 풀의 시작 주소입니다.
IP_address2	DHCP 주소 풀의 끝 주소입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령을 사용하려면 ASA DHCP 서버의 주소 풀이 이 서버가 활성화된 ASA 인터페이스와 동일한 서브넷에 있어야 하며, 해당 ASA 인터페이스를 *interface_name*으로 지정해야 합니다.

주소 풀의 크기는 ASA에 있는 풀당 최대 256개 주소로 제한됩니다. 주소 풀의 범위가 253개 주소보다 클 경우 ASA 인터페이스의 넷마스크는 클래스 C 주소(예: 255.255.255.0)가 될 수 없으며 그보다 더 커야 합니다(예: 255.255.254.0).

DHCP 클라이언트는 ASA DHCP 서버 인터페이스의 서브넷에 물리적으로 연결되어야 합니다.

dhcpd address 명령에서는 인터페이스 이름에 "-"(대시) 문자를 사용할 수 없습니다. 이 문자는 객체 이름의 일부가 아니라 범위 지정자로 해석되기 때문입니다.

no dhcpd address *interface_name* 명령은 지정된 인터페이스에 대해 구성한 DHCP 서버 주소 풀을 제거합니다.

ASA에서 DHCP 서버 기능을 구현하는 방법에 대한 자세한 내용은 *CLI 컨피그레이션 가이드*를 참조하십시오.

예

다음 예에서는 ASA의 DMZ 인터페이스에 있는 DHCP 클라이언트를 위해 주소 풀과 DNS 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 209.165.200.226
ciscoasa(config)# dhcpd enable dmz
```

다음 예에서는 내부 인터페이스에서 DHCP 서버를 구성하는 방법을 보여줍니다. **dhcpd address** 명령은 IP 주소 10개로 된 풀을 이 인터페이스의 DHCP 서버에 지정합니다.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
dhcpd enable	지정된 인터페이스에서 DHCP 서버를 활성화합니다.
show dhcpd	DHCP 바인딩, 통계 또는 상태 정보를 표시합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd auto_config

ASA에서 DHCP 또는 PPPoE 클라이언트를 실행 중인 인터페이스로부터 얻은 값에 따라 DHCP 서버의 DNS, WINS, 도메인 이름 값을 자동으로 구성할 수 있게 하려면 글로벌 컨피그레이션 모드에서 **dhcpd auto_config** 명령을 사용합니다. DHCP 매개변수의 자동 컨피그레이션을 중지하려면 이 명령의 **no** 형식을 사용합니다.

dhcpd auto_config *client_if_name* **[[vpnclient-wins-override] interface** *if_name***]**

no dhcpd auto_config *client_if_name* **[[vpnclient-wins-override] interface** *if_name***]**

구문 설명

client_if_name	DNS, WINS, 도메인 이름 매개변수를 제공하는 DHCP 클라이언트가 실행 중인 인터페이스를 지정합니다.
interface *if_name*	작업을 적용할 인터페이스를 지정합니다.
vpnclient-wins-override	인터페이스 DHCP 또는 PPPoE 클라이언트 WINS 매개변수를 vpnclient 매개변수로 재정의합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

CLI 명령을 사용하여 DNS, WINS 또는 도메인 이름 매개변수를 지정할 경우 CLI에서 구성된 매개변수가 자동 컨피그레이션에 의한 매개변수를 재정의합니다.

예

다음 예에서는 내부 인터페이스에서 DHCP를 구성하는 방법을 보여줍니다. **dhcpd auto_config** 명령은 외부 인터페이스의 DHCP 클라이언트에서 얻은 DNS, WINS, 도메인 정보를 내부 인터페이스의 DHCP 클라이언트에 전달하는 데 사용됩니다.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd auto_config outside
ciscoasa(config)# dhcpd enable inside
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
dhcpd enable	지정된 인터페이스에서 DHCP 서버를 활성화합니다.
show ip address dhcp server	DHCP 서버에서 DHCP 클라이언트의 역할을 하는 인터페이스에 제공하는 DHCP 옵션에 대한 세부 정보를 표시합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd dns

DHCP 클라이언트의 DNS 서버를 정의하려면 글로벌 컨피그레이션 모드에서 **dhcpd dns** 명령을 사용합니다. 정의된 서버를 지우려면 이 명령의 **no** 형식을 사용합니다.

dhcpd dns *dnsip1* **[***dnsip2***] [interface** *if_name***]**

no dhcpd dns *dnsip1* **[***dnsip2***] [interface** *if_name***]**

구문 설명

dnsip1	DHCP 클라이언트를 위한 기본 DNS 서버의 IP 주소를 지정합니다.
dnsip2	(선택 사항) DHCP 클라이언트를 위한 대체 DNS 서버의 IP 주소를 지정합니다.
interface *if_name*	서버에 입력된 값이 적용되는 인터페이스를 지정합니다. 인터페이스가 지정되지 않을 경우 값은 모든 서버에 적용됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

dhcpd dns 명령으로 DHCP 클라이언트를 위한 DNS 서버의 IP 주소를 하나 이상 지정할 수 있습니다. 2개의 DNS 서버를 지정할 수 있습니다. **no dhcpd dns** 명령을 사용하면 DNS IP 주소를 컨피그레이션에서 제거할 수 있습니다.

예

다음 예에서는 ASA의 DMZ 인터페이스에 있는 DHCP 클라이언트를 위해 주소 풀과 DNS 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 192.168.1.2
ciscoasa(config)# dhcpd enable dmz
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
dhcpd address	지정된 인터페이스에서 DHCP 서버가 사용하는 주소 풀을 지정합니다.
dhcpd enable	지정된 인터페이스에서 DHCP 서버를 활성화합니다.
dhcpd wins	DHCP 클라이언트의 WINS 서버를 정의합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd domain

DHCP 클라이언트의 DNS 도메인 이름을 정의하려면 글로벌 컨피그레이션 모드에서 **dhcpd domain** 명령을 사용합니다. DNS 도메인 이름을 지우려면 이 명령의 **no** 형식을 사용합니다.

dhcpd domain *domain_name* **[interface** *if_name***]**

no dhcpd domain [*domain_name***] [interface** *if_name***]**

구문 설명

domain_name	DNS 도메인 이름(example.com)을 지정합니다.
interface *if_name*	서버에 입력된 값이 적용되는 인터페이스를 지정합니다. 인터페이스가 지정되지 않을 경우 값은 모든 서버에 적용됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

dhcpd domain 명령을 사용하면 DHCP 클라이언트 를 위한 DNS 도메인 이름을 지정할 수 있습니다. **no dhcpd domain** 명령을 사용하면 DNS 도메인 서버를 컨피그레이션에서 제거할 수 있습니다.

예

다음 예에서는 ASA에서 DHCP 서버가 DHCP 클라이언트에 제공한 도메인 이름을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd enable

DHCP 서버를 활성화하려면 글로벌 컨피그레이션 모드에서 **dhcpd enable** 명령을 사용합니다. DHCP 서버를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dhcpd enable *interface*

no dhcpd enable *interface*

구문 설명

interface	어떤 인터페이스에서 DHCP 서버를 활성화할 것인지 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

DHCP 서버는 DHCP 클라이언트에 네트워크 컨피그레이션 매개변수를 제공합니다. DHCP 서버를 ASA 내에서 지원하므로 ASA에서 연결된 클라이언트의 컨피그레이션에 DHCP를 사용할 수 있습니다. **dhcpd enable** *interface* 명령을 사용하면 DHCP 데몬이 DHCP가 활성화된 인터페이스에서 DHCP 클라이언트 요청을 수신하게 할 수 있습니다. **no dhcpd enable** 명령은 지정된 인터페이스에서 DHCP 서버 기능을 비활성화합니다.

참고 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트가 사용하는 인터페이스(공유 VLAN)에서 DHCP 서버를 활성화할 수 없습니다.

ASA에서 DHCP 클라이언트 요청에 응답할 때, 요청이 수신된 인터페이스의 IP 주소 및 서브넷 마스크를 응답의 기본 게이트웨이의 IP 주소 및 서브넷 마스크로 사용합니다.

참고 ASA DHCP 서버 데몬은 ASA 인터페이스에 직접 연결되지 않는 클라이언트를 지원하지 않습니다.

ASA에서 DHCP 서버 기능을 구현하는 방법에 대한 자세한 내용은 *CLI 컨피그레이션 가이드*를 참조하십시오.

예

다음 예에서는 내부 인터페이스에서 DHCP 서버를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

관련 명령

명령	설명
debug dhcpd	DHCP 서버의 디버깅 정보를 표시합니다.
dhcpd address	지정된 인터페이스에서 DHCP 서버가 사용하는 주소 풀을 지정합니다.
show dhcpd	DHCP 바인딩, 통계 또는 상태 정보를 표시합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd lease

DHCP 임대 기간을 지정하려면 글로벌 컨피그레이션 모드에서 **dhcpd lease** 명령을 사용합니다. 임대의 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

dhcpd lease *lease_length* **[interface** *if_name***]**

no dhcpd lease [*lease_length***] [interface** *if_name***]**

구문 설명

interface *if_name*	서버에 입력된 값이 적용되는 인터페이스를 지정합니다. 인터페이스가 지정되지 않을 경우 값은 모든 서버에 적용됩니다.
lease_length	DHCP 서버에서 DHCP 클라이언트에 부여한 IP 주소의 임대 기간(초)을 지정합니다. 유효한 값의 범위는 300초~1048575초입니다.

기본값

기본 *lease_length*는 3600초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

dhcpd lease 명령을 사용하면 DHCP 클라이언트에 부여된 임대 기간(초)을 지정할 수 있습니다. 이 임대 기간은 DHCP 클라이언트에서 DHCP 서버로부터 받은 IP 주소를 사용할 수 있는 기간을 나타냅니다.

지정한 임대 기간을 컨피그레이션에서 제거하고 기본값인 3600초로 대체하려면 **no dhcpd lease** 명령을 사용합니다.

예

다음 예에서는 DHCP 클라이언트를 위한 DHCP 정보의 임대 기간을 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd option

DHCP 옵션을 구성하려면 글로벌 컨피그레이션 모드에서 **dhcpd option** 명령을 사용합니다. 이 옵션을 지우려면 이 명령의 **no** 형식을 사용합니다.

dhcpd option *code* {**ascii** *string*} | {**ip** *IP_address* [*IP_address*]} | {**hex** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

구문 설명

ascii *string*	옵션 매개변수가 공백 없는 ASCII 문자열임을 나타냅니다.
code	설정 중인 DHCP 옵션을 나타내는 숫자를 지정합니다. 유효한 값의 범위는 0~255이며, 몇 가지 예외가 있습니다. 지원되지 않는 DHCP 옵션 코드의 목록은 사용 지침 섹션을 참조하십시오.
hex *hex_string*	옵션 매개변수가 공백이 없고 자릿수가 짝수인 16진수 문자열임을 나타냅니다. 0x 접두사를 사용할 필요 없습니다.
interface *if_name*	서버에 입력된 값이 적용되는 인터페이스를 지정합니다. 인터페이스가 지정되지 않을 경우 값은 모든 서버에 적용됩니다.
ip	옵션 매개변수가 IP 주소임을 나타냅니다. **ip** 키워드로 최대 2개의 IP 주소를 지정할 수 있습니다.
IP_address	점으로 구분된 10진수로 IP 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

Cico IP Phone과 라우터에 TFTP 정보를 제공하는 데 **dhcpd option** 명령을 사용할 수 있습니다.

DHCP 옵션 요청이 ASA DHCP 서버에 도착하면 ASA는 클라이언트에 대한 응답에 **dhcpd option** 명령에 의해 지정된 하나 이상의 값을 포함시킵니다.

dhcpd option 66 및 **dhcpd option 150** 명령은 Cisco IP Phone과 라우터에서 컨피그레이션 파일의 다운로드에 사용할 수 있는 TFTP 서버를 지정합니다. 이 명령을 다음과 같이 사용합니다.

- **dhcpd option 66 ascii** *string* - 여기서 *string*은 TFTP 서버의 IP 주소 또는 호스트 이름입니다. 옵션 66에 대해 하나의 TFTP 서버만 지정할 수 있습니다.
- **dhcpd option 150 ip** *IP_address* [*IP_address*] - 여기서 *IP_address*는 TFTP 서버의 IP 주소입니다. 옵션 150에 대해 최대 2개의 IP 주소를 지정할 수 있습니다.

참고 **dhcpd option 66** 명령에서는 **ascii** 매개변수만, **dhcpd option 150**에서는 **ip** 매개변수만 사용할 수 있습니다.

dhcpd option 66 | 150 명령을 위해 IP 주소를 지정할 때 다음 지침을 따릅니다.

- TFTP 서버가 DHCP 서버 인터페이스에 있을 경우 TFTP 서버의 로컬 IP 주소를 사용합니다.
- TFTP 서버가 DHCP 서버 인터페이스만큼 안전하지 않은 인터페이스에 있을 경우 일반 아웃바운드 규칙을 적용합니다. DHCP 클라이언트를 위해 NAT, 전역, 액세스 목록 엔트리를 만들고 TFTP 서버의 실제 IP 주소를 사용합니다.
- TFTP 서버가 더 안전한 인터페이스에 있을 경우 일반 인바운드 규칙을 적용합니다. TFTP 서버를 위해 고정 및 액세스 목록 구문을 만들고 TFTP 서버의 전역 IP 주소를 사용합니다.

다른 DHCP 옵션에 대한 자세한 내용은 RFC 2132를 참조하십시오.

참고 ASA는 사용자가 제공하는 옵션의 유형 및 값이 RFC 2132에 정의된 옵션 코드의 예상 유형 및 값과 일치하는지 확인하지 않습니다. 이를테면 **dhcpd option 46 ascii hello** 명령을 입력할 수 있습니다. RFC 2132에 따르면 옵션 46이 1자리의 16진수 값으로 정의되지만 ASA는 이 컨피그레이션을 승인합니다.

dhcpd option 명령으로 다음 DHCP 옵션을 구성할 수 없습니다.

옵션 코드	설명
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

예

다음 예에서는 DHCP 옵션 66을 위해 TFTP 서버를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd option 66 ascii MyTftpServer
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd ping_timeout

DHCP ping의 시간 초과 기본값을 변경하려면 글로벌 컨피그레이션 모드에서 **dhcpd ping_timeout** 명령을 사용합니다. 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

dhcpd ping_timeout *number* **[interface** *if_name***]**

no dhcpd ping_timeout [**interface** *if_name*]

구문 설명

interface *if_name*	서버에 입력된 값이 적용되는 인터페이스를 지정합니다. 인터페이스가 지정되지 않을 경우 값은 모든 서버에 적용됩니다.
number	ping의 시간 초과 값이며, 단위는 밀리초입니다. 최소값은 10이고 최대 값은 10000입니다. 기본값은 50입니다.

기본값

*number*의 기본값은 50밀리초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

주소 충돌을 방지하고자 DHCP 서버는 DHCP 클라이언트에 주소를 지정하기 전에 주소에 2개의 ICMP ping 패킷을 보냅니다. ASA는 두 ICMP ping 패킷 모두 시간 초과된 후에 DHCP 클라이언트에 IP 주소를 지정합니다. 예를 들어, 기본값이 사용되는 경우 ASA는 1500밀리초(ICMP ping 패킷당 750밀리초)가 지나면 IP 주소를 지정합니다.

ping 시간 초과의 값이 크면 DHCP 서버의 성능에 불리하게 작용할 수 있습니다.

예

다음 예에서는 **dhcpd ping_timeout** 명령을 사용하여 DHCP 서버의 ping 시간 초과 값을 변경하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcpd update dns

DHCP 서버에서 DDNS 업데이트를 수행할 수 있게 하려면 글로벌 컨피그레이션 모드에서 **dhcpd update dns** 명령을 사용합니다. DHCP 서버의 DDNS 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

구문 설명

both	DHCP 서버에서 A 및 PTR DNS RR을 모두 업데이트하도록 지정합니다.
interface	DDNS 업데이트를 적용할 ASA 인터페이스를 지정합니다.
override	DHCP 서버에서 DHCP 클라이언트 요청을 재정의하도록 지정합니다.
srv_ifc_name	이 옵션을 적용할 인터페이스를 지정합니다.

기본값

기본적으로 DHCP 서버는 PTR RR 업데이트만 수행합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

DDNS가 DNS로 관리되는 name-to-address 및 address-to-name 매핑을 업데이트합니다. 업데이트는 DHCP 서버와 연계하여 이루어집니다. **dhcpd update dns** 명령은 서버에 의한 업데이트를 활성화합니다.

이름 및 주소 매핑은 2가지 RR 유형에 수록되어 있습니다.

- A 리소스 레코드는 도메인 이름-IP 주소 매핑을 포함합니다.
- PTR 리소스 레코드는 IP 주소-도메인 이름 매핑을 포함합니다.

DDNS 업데이트는 DNS A 유형과 PTR RR 유형 간에 정보의 일관성을 유지하는 데 사용할 수 있습니다.

dhcpd update dns 명령을 사용하면 DHCP 서버에서 A 및 PRT RR 업데이트 모두 또는 PTR RR 업데이트만 수행하도록 구성할 수 있습니다. DHCP 클라이언트의 업데이트 요청을 재정의하도록 구성할 수도 있습니다.

예

다음 예에서는 DDNS 서버가 A 및 PTR 업데이트를 모두 수행하고 DHCP 클라이언트의 요청을 재정의하도록 구성합니다.

```
ciscoasa(config)# dhcpd update dns both override
```

관련 명령

명령	설명
ddns	생성된 DDNS 메서드에 대한 DDNS 업데이트 메서드 유형을 지정합니다.
ddns update	DDNS 업데이트 메서드를 ASA 인터페이스 또는 DDNS 업데이트 호스트 이름과 연결합니다.
ddns update method	DNS 리소스 레코드를 동적으로 업데이트하는 메서드를 생성합니다.
dhcp-client update dns	DHCP 클라이언트에서 DHCP 서버에 전달할 업데이트 매개변수를 구성합니다.
interval maximum	DDNS 업데이트 메서드에 의한 업데이트 시도의 최대 간격을 구성합니다.

dhcpd wins

DHCP 클라이언트를 위한 WINS 서버 IP 주소를 정의하려면 글로벌 컨피그레이션 모드에서 **dhcpd wins** 명령을 사용합니다. WINS 서버 IP 주소를 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

dhcpd wins *server1* [*server2*] **[interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] **[interface** *if_name*]

구문 설명

interface *if_name*	서버에 입력된 값이 적용되는 인터페이스를 지정합니다. 인터페이스가 지정되지 않을 경우 값은 모든 서버에 적용됩니다.
server1	기본 Microsoft NetBIOS 이름 서버(WINS 서버)의 IP 주소를 지정합니다.
server2	(선택 사항) 대체 Microsoft NetBIOS 이름 서버(WINS 서버)의 IP 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

dhcpd wins 명령을 사용하면 DHCP 클라이언트를 위한 WINS 서버의 주소를 지정할 수 있습니다. **no dhcpd wins** 명령은 WINS 서버 IP 주소를 컨피그레이션에서 제거합니다.

예

다음 예에서는 DHCP 클라이언트에 보내는 WINS 서버 정보를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

관련 명령

명령	설명
clear configure dhcpd	모든 DHCP 서버 설정을 제거합니다.
dhcpd address	지정된 인터페이스에서 DHCP 서버가 사용하는 주소 풀을 지정합니다.
dhcpd dns	DHCP 클라이언트의 DNS 서버를 정의합니다.
show dhcpd	DHCP 바인딩, 통계 또는 상태 정보를 표시합니다.
show running-config dhcpd	현재 DHCP 서버 컨피그레이션을 표시합니다.

dhcprelay enable

DHCP 릴레이 서버를 활성화하려면 글로벌 컨피그레이션 모드에서 **dhcprelay enable** 명령을 사용합니다. DHCP 릴레이 에이전트를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

구문 설명

interface_name	DHCP 릴레이 에이전트가 클라이언트 요청을 수락하는 인터페이스의 이름입니다.

기본값

DHCP 릴레이 에이전트는 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

DHCP 릴레이 에이전트는 지정된 ASA 인터페이스에서 지정된 DHCP 서버로 DHCP 요청이 전달될 수 있게 합니다.

ASA에서 **dhcprelay enable** *interface_name* 명령을 사용하여 DHCP 릴레이 에이전트를 시작하려면 **dhcprelay server** 명령이 이미 컨피그레이션에 포함되어 있어야 합니다. 그렇지 않으면 ASA는 다음과 비슷한 오류 메시지를 표시합니다.

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

다음 조건에서는 DHCP 릴레이를 활성화할 수 없습니다.

- DHCP 릴레이와 DHCP 릴레이 서버를 동일한 인터페이스에서 활성화할 수 없습니다.
- DHCP 릴레이와 DHCP 서버(**dhcpd enable**)를 동일한 인터페이스에서 활성화할 수 없습니다.
- DHCP 서버가 활성화되지 않으면 DHCP 릴레이 에이전트도 활성화될 수 없습니다.
- 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트가 사용하는 인터페이스(공유 VLAN)에서 DHCP 릴레이를 활성화할 수 없습니다.

no dhcprelay enable *interface_name* 명령은 *interface_name* 인수에 의해 지정된 인터페이스의 DHCP 릴레이 에이전트 컨피그레이션만 제거합니다.

예

다음 예에서는ASA의 외부 인터페이스에 있는 IP 주소 10.1.1.1, ASA의 내부 인터페이스에 있는 클라이언트 요청, 최대 90초의 시간 초과 값을 사용하여 DHCP 서버를 위한 DHCP 릴레이 에이전트를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

다음 예에서는 DHCP 릴레이 에이전트를 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# no dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
debug dhcp relay	DHCP 릴레이 에이전트의 디버깅 정보를 표시합니다.
dhcprelay server	DHCP 릴레이 에이전트가 DHCP 요청을 전달할 DHCP 서버를 지정합니다.
dhcprelay setroute	DHCP 릴레이 에이전트가 DHCP 회신에서 기본 라우터 주소로 사용할 IP 주소를 정의합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

dhcprelay information trust-all

지정된 인터페이스를 신뢰받는 인터페이스로 구성하려면 글로벌 컨피그레이션 모드에서 **dhcprelay information trust-all** 명령을 사용합니다.

dhcprelay information trust-all

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 지정된 인터페이스를 신뢰받는 인터페이스로 구성합니다. 인터페이스의 신뢰받는 컨피그레이션을 보려면 인터페이스 컨피그레이션 모드에서 **show running-config dhcprelay interface** 명령을 사용합니다. 인터페이스 컨피그레이션 모드에서 어떤 인터페이스를 신뢰받는 인터페이스로 구성하려면 **dhcprelay information trusted** 명령을 사용합니다. 글로벌 컨피그레이션 모드에서 어떤 인터페이스를 신뢰받는 인터페이스로 표시하려면 **show running-config dhcprelay** 명령을 사용합니다.

예

다음 예에서는 글로벌 컨피그레이션 모드에서 지정된 인터페이스를 신뢰받는 인터페이스로 구성하는 방법을 보여줍니다.

```
ciscoasa(config-if)# interface vlan501
ciscoasa(config-if)# nameif inside
ciscoasa(config)# dhcprelay information trust-all
ciscoasa(config)# show running-config dhcprelay
dhcprelay information trust-all
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
dhcprelay enable	지정된 인터페이스에서 DHCP 릴레이 에이전트를 활성화합니다.
dhcprelay setroute	DHCP 릴레이 에이전트가 DHCP 회신에서 기본 라우터 주소로 사용할 IP 주소를 정의합니다.
dhcprelay timeout	DHCP 릴레이 에이전트의 시간 초과 값을 지정합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

dhcprelay information trusted

지정된 인터페이스를 신뢰받는 인터페이스로 구성하려면 인터페이스 컨피그레이션 모드에서 **dhcprelay information trusted** 명령을 사용합니다.

dhcprelay information trusted

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 지정된 인터페이스를 신뢰받는 인터페이스로 구성합니다. 인터페이스의 신뢰받는 컨피그레이션을 보려면 인터페이스 컨피그레이션 모드에서 **show running-config dhcprelay interface** 명령을 사용합니다. 글로벌 컨피그레이션 모드에서 어떤 인터페이스를 신뢰받는 인터페이스로 구성하려면 **dhcprelay information trust-all** 명령을 사용합니다. 글로벌 컨피그레이션 모드에서 어떤 인터페이스를 신뢰받는 인터페이스로 표시하려면 **show running-config dhcprelay** 명령을 사용합니다.

예

다음 예에서는 지정된 인터페이스를 신뢰받는 인터페이스로 구성하는 방법을 보여줍니다.

```
ciscoasa(config-if)# interface gigabitEthernet 0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay information trusted
ciscoasa(config)# show running-config dhcprelay
interface gigabitEthernet 0/0
nameif inside
dhcprelay information trusted
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
dhcprelay enable	지정된 인터페이스에서 DHCP 릴레이 에이전트를 활성화합니다.
dhcprelay setroute	DHCP 릴레이 에이전트가 DHCP 회신에서 기본 라우터 주소로 사용할 IP 주소를 정의합니다.
dhcprelay timeout	DHCP 릴레이 에이전트의 시간 초과 값을 지정합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

dhcprelay server(global)

DHCP 요청이 전달되는 DHCP 서버를 지정하려면 글로벌 컨피그레이션 모드에서 **dhcpreplay server** 명령을 사용합니다. DHCP 서버를 DHCP 릴레이 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

dhcprelay server [*interface_name***]**

no dhcprelay server [*interface_name***]**

구문 설명

interface_name	DHCP 서비스가 상주하는 ASA 인터페이스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

DHCP 릴레이 에이전트는 지정된 ASA 인터페이스에서 지정된 DHCP 서버로 DHCP 요청이 전달될 수 있게 합니다. 인터페이스당 최대 10개의 DHCP 릴레이 서버를 추가할 수 있습니다. **dhcprelay enable** 명령을 입력하려면 먼저 하나 이상의 **dhcprelay server** 명령을 ASA 컨피그레이션에 추가해야 합니다. DHCP 릴레이 서버가 구성된 인터페이스에서 DHCP 클라이언트를 구성할 수 없습니다.

dhcprelay enable 명령이 컨피그레이션에 추가되는 즉시 **dhcprelay server** 명령이 지정된 인터페이스에서 UDP 포트 67을 열고 DHCP 릴레이 작업을 시작합니다.

예

다음 예에서는ASA의 외부 인터페이스에 있는 IP 주소 10.1.1.1, ASA의 내부 인터페이스에 있는 클라이언트 요청, 최대 90초의 시간 초과 값을 사용하여 DHCP 서버를 위한 DHCP 릴레이 에이전트를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
dhcprelay enable	지정된 인터페이스에서 DHCP 릴레이 에이전트를 활성화합니다.
dhcprelay setroute	DHCP 릴레이 에이전트가 DHCP 회신에서 기본 라우터 주소로 사용할 IP 주소를 정의합니다.
dhcprelay timeout	DHCP 릴레이 에이전트의 시간 초과 값을 지정합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

dhcprelay server(interface)(9.1(2) 이상)

DHCP 요청이 전달되는 DHCP 릴레이 인터페이스 서버를 지정하려면 인터페이스 컨피그레이션 모드에서 **dhcpreplay server** 명령을 사용합니다. DHCP 릴레이 인터페이스 서버를 DHCP 릴레이 컨피그레이션에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

dhcprelay server *ip_address*

no dhcprelay server *ip_address*

구문 설명

ip_address	DHCP 릴레이 에이전트가 클라이언트 DHCP 요청을 전달할 DHCP 릴레이 인터페이스 서버의 IP 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

사용 지침

DHCP 릴레이 에이전트는 지정된 ASA 인터페이스에서 지정된 DHCP 서버로 DHCP 요청이 전달될 수 있게 합니다. 인터페이스당 최대 4개의 DHCP 릴레이 서버를 추가할 수 있습니다. **dhcprelay enable** 명령을 입력하려면 먼저 하나 이상의 **dhcprelay server** 명령을 ASA 컨피그레이션에 추가해야 합니다. DHCP 릴레이 서버가 구성된 인터페이스에서 DHCP 클라이언트를 구성할 수 없습니다.

dhcprelay enable 명령이 컨피그레이션에 추가되는 즉시 **dhcprelay server** 명령이 지정된 인터페이스에서 UDP 포트 67을 열고 DHCP 릴레이 작업을 시작합니다.

인터페이스 컨피그레이션 모드에서 **dhcprelay server** *ip_address* 명령을 사용하여 인터페이스별로 DHCP 릴레이 서버(헬퍼라고 함) 주소를 구성할 수 있습니다. 그러면 인터페이스에서 수신한 DHCP 요청에 헬퍼 주소가 구성되었으면 그 요청은 해당 서버로만 전달됩니다.

no dhcprelay server *ip_address* 명령을 사용하면 인터페이스에서는 더 이상 해당 서버에 DHCP 패킷을 전달하지 않고 *ip_address* 인수에 의해 지정된 DHCP 서버의 DHCP 릴레이 에이전트 컨피그레이션만 제거합니다.

이 명령은 글로벌 컨피그레이션 모드에서 구성된 DHCP 릴레이 서버보다 우선적으로 적용됩니다. 즉 DHCP 릴레이 에이전트는 먼저 DHCP 릴레이 인터페이스 서버에 클라이언트 검색 메시지를 전달한 다음 DHCP 전역 릴레이 서버에 전달합니다.

예

다음 예에서는ASA의 외부 인터페이스에 있는 IP 주소 10.1.1.1, ASA의 내부 인터페이스에 있는 클라이언트 요청, 최대 90초의 시간 초과 값을 사용하여 DHCP 릴레이 인터페이스 서버를 위한 DHCP 릴레이 에이전트를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# interface vlan 10
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay server 10.1.1.1
ciscoasa(config-if)# exit
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay enable inside
dhcprelay timeout 90

interface vlan 10
nameif inside
dhcprelay server 10.1.1.1
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
dhcprelay enable	지정된 인터페이스에서 DHCP 릴레이 에이전트를 활성화합니다.
dhcprelay setroute	DHCP 릴레이 에이전트가 DHCP 회신에서 기본 라우터 주소로 사용할 IP 주소를 정의합니다.
dhcprelay timeout	DHCP 릴레이 에이전트의 시간 초과 값을 지정합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

dhcprelay setroute

DHCP 회신에서 기본 게이트웨이 주소를 설정하려면 글로벌 컨피그레이션 모드에서 **dhcprelay setroute** 명령을 사용합니다. 기본 라우터를 제거하려면 이 명령의 **no** 형식을 사용합니다.

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

구문 설명

interface	DHCP 릴레이 에이전트에서 첫 번째 기본 IP 주소(DHCP 서버에서 보낸 패킷에 있음)를 *interface*의 주소로 변경하도록 구성합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령을 실행하면 DHCP 회신의 기본 IP 주소가 지정된 ASA 인터페이스의 주소를 대체합니다. **dhcprelay setroute** *interface* 명령을 사용하면 DHCP 릴레이 에이전트가 첫 번째 기본 라우터 주소(DHCP 서버에서 보낸 패킷에 있음)를 *interface*의 주소로 변경합니다.

패킷에 기본 라우터 옵션이 없을 경우 ASA에서는 *interface*의 주소를 포함하는 것으로 추가합니다. 그러면 클라이언트에서 기본 경로가 ASA를 가리키도록 설정할 수 있습니다.

dhcprelay setroute *interface* 명령을 구성하지 않을 경우 (그리고 패킷에 기본 라우터 옵션이 있다면) 라우터 주소를 변경하지 않고 ASA를 통과합니다.

예

다음 예에서는 외부 DHCP 서버가 보낸 DHCP 회신의 기본 게이트웨이를 ASA의 내부 인터페이스로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay setroute inside
ciscoasa(config)# dhcprelay enable inside
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
dhcprelay enable	지정된 인터페이스에서 DHCP 릴레이 에이전트를 활성화합니다.
dhcprelay server	DHCP 릴레이 에이전트가 DHCP 요청을 전달할 DHCP 서버를 지정합니다.
dhcprelay timeout	DHCP 릴레이 에이전트의 시간 초과 값을 지정합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

dhcprelay timeout

DHCP 릴레이 에이전트 시간 초과 값을 설정하려면 글로벌 컨피그레이션 모드에서 **dhcprelay timeout** 명령을 사용합니다. 시간 초과 값을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

dhcprelay timeout *seconds*

no dhcprelay timeout

구문 설명

seconds	DHCP 릴레이 에이전트 협상에 허용된 시간(초)을 지정합니다.

기본값

DHCP 릴레이 시간 초과의 기본값은 60초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

dhcprelay timeout 명령을 사용하면 DHCP 서버가 릴레이 바인딩 구조를 통해 DHCP 클라이언트에 전달할 응답에 허용되는 시간을 초 단위로 설정할 수 있습니다.

예

다음 예에서는ASA의 외부 인터페이스에 있는 IP 주소 10.1.1.1, ASA의 내부 인터페이스에 있는 클라이언트 요청, 최대 90초의 시간 초과 값을 사용하여 DHCP 서버를 위한 DHCP 릴레이 에이전트를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

관련 명령

명령	설명
clear configure dhcprelay	모든 DHCP 릴레이 에이전트 설정을 제거합니다.
dhcprelay enable	지정된 인터페이스에서 DHCP 릴레이 에이전트를 활성화합니다.
dhcprelay server	DHCP 릴레이 에이전트가 DHCP 요청을 전달할 DHCP 서버를 지정합니다.
dhcprelay setroute	DHCP 릴레이 에이전트가 DHCP 회신에서 기본 라우터 주소로 사용할 IP 주소를 정의합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

dialog

WebVPN 사용자에게 표시되는 대화 상자 메시지를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **dialog** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

dialog {**title** | **message** | **border**} **style** *value*

no dialog {**title** | **message** | **border**} **style** *value*

구문 설명

border	경계선의 변경 사항을 지정합니다.
message	메시지의 변경 사항을 지정합니다.
style	스타일의 변경 사항을 지정합니다.
title	제목의 변경 사항을 지정합니다.
value	표시할 실제 텍스트 또는 CSS 매개변수입니다(최대 256자).

기본값

기본 제목 스타일은 background-color:#669999;color:white입니다.

기본 메시지 스타일은 background-color:#99CCCC;color:black입니다.

기본 경계선 스타일은 border:1px solid black;border-collapse:collapse입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

style 옵션은 임의의 유효한 CSS 매개변수로 표시됩니다. 이 매개변수에 대한 설명은 본 설명서의 범위에 속하지 않습니다. CSS 매개변수에 대한 자세한 내용은 World Wide Web Consortium 웹 사이트(www.w3.org)의 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F는 편리한 CSS 매개변수 목록을 포함하고 있으며 www.w3.org/TR/CSS21/propidx.html에서 이용할 수 있습니다.

WebVPN 페이지 - 페이지 색상의 가장 대표적인 변경 방법에 대한 몇 가지 팁을 소개합니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 (HTML에서 인식된다면) 색상의 이름을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며, 각 색상(빨강, 녹색, 파랑)을 나타내는 0~255 범위의 10진수입니다. 쉼표로 구분하여 입력한 값은 해당 강도의 각 색상이 나머지 색상과 조합되는 것을 의미합니다.
- HTML 형식은 #000000이며, 6자리의 16진수입니다. 1번째와 2번째 자리는 빨강을, 3번째와 4번째 자리는 녹색을, 5번째와 6번째는 파랑을 나타냅니다.

참고 손쉽게 WebVPN 페이지를 사용자 지정하려면 ASDM을 사용하는 것이 좋습니다. 색 견본, 미리 보기 등 스타일 요소를 편리하게 구성할 수 있는 기능을 제공합니다.

예

다음 예에서는 대화 상자 메시지를 사용자 지정하는데, 전경색을 파랑으로 변경합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# dialog message style color:blue
```

관련 명령

명령	설명
application-access	WebVPN Home 페이지의 Application Access 상자를 사용자 지정합니다.
browse-networks	WebVPN Home 페이지의 Browse Networks 상자를 사용자 지정합니다.
web-bookmarks	WebVPN Home 페이지의 Web Bookmarks 제목 또는 링크를 사용자 지정합니다.
file-bookmarks	WebVPN Home 페이지의 File Bookmarks 제목 또는 링크를 사용자 지정합니다.

dir

디렉토리 내용을 표시하려면 특별 권한 EXEC 모드에서 **dir** 명령을 사용합니다.

dir [/all] [all-filesystems] [/recursive] [disk0: | disk1: | flash: | system:] [*path***]**

구문 설명

/all	(선택 사항) 모든 파일을 표시합니다.
/recursive	(선택 사항) 디렉토리의 내용을 순환하여 표시합니다.
all-filesystems	(선택 사항) 모든 파일 시스템의 파일을 표시합니다.
disk0:	(선택 사항) 내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다.
disk1:	(선택 사항) 외부 플래시 메모리 카드를 지정하고 그 다음에 콜론을 표시합니다.
flash:	(선택 사항) 기본 플래시 파티션의 디렉토리 내용을 표시합니다.
path	(선택 사항) 특정 경로를 지정합니다.
system:	(선택 사항) 파일 시스템의 디렉토리 내용을 표시합니다.

기본값

디렉토리를 지정하지 않으면 현재 작업 디렉토리가 기본적으로 사용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

키워드 또는 인수 없이 **dir** 명령을 사용하면 현재 디렉토리의 디렉토리 내용을 표시합니다.

예

다음 예에서는 디렉토리 내용을 표시하는 방법을 보여줍니다.

```
ciscoasa# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

다음 예에서는 전체 파일 시스템의 내용을 순환하여 표시하는 방법을 보여줍니다.

```
ciscoasa# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

다음 예에서는 플래시 파티션의 내용을 표시하는 방법을 보여줍니다.

```
ciscoasa# dir flash:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

관련 명령

명령	설명
cd	현재 작업 디렉토리를 지정된 디렉토리로 변경합니다.
pwd	현재 작업 디렉토리를 표시합니다.
mkdir	디렉토리를 만듭니다.
rmdir	디렉토리를 제거합니다.

disable

특별 권한 EXEC 모드를 종료하고 일반 EXEC 모드로 돌아가려면 특별 권한 EXEC 모드에서 **disable** 명령을 사용합니다.

disable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

특별 권한 모드를 시작하려면 **enable** 명령을 사용합니다. **disable** 명령을 사용하면 특별 권한 모드를 종료하고 일반 모드로 돌아갈 수 있습니다.

예

다음 예에서는 특별 권한 모드를 시작하는 방법을 보여줍니다.

```
ciscoasa> enable
ciscoasa#
```

다음 예에서는 특별 권한 모드를 종료하는 방법을 보여줍니다.

```
ciscoasa# disable
ciscoasa>
```

관련 명령

명령	설명
enable	특별 권한 EXEC 모드를 활성화합니다.

disable(cache)

WebVPN을 위한 캐싱을 비활성화하려면 캐시 컨피그레이션 모드에서 **disable** 명령을 사용합니다. 캐싱을 다시 활성화하려면 이 명령의 **no** 버전을 사용합니다.

disable

no disable

기본값

각 캐시 특성의 기본 설정과 함께 캐싱이 활성화됩니다.

명령 모드

다음 표는 명령을 입력하는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
캐시 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

캐싱은 자주 재사용되는 객체를 시스템 캐시에 저장합니다. 그러면 콘텐츠 다시 쓰기 및 압축을 반복할 필요성이 줄어듭니다. WebVPN과 원격 서버 및 최종 사용자 브라우저 간의 트래픽을 줄이므로 많은 애플리케이션이 훨씬 더 효율적으로 실행될 수 있습니다.

예

다음 예에서는 캐싱을 비활성화했다가 다시 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# disable
ciscoasa(config-webvpn-cache)# no disable
ciscoasa(config-webvpn-cache)#
```

관련 명령

명령	설명
cache	webvpn 캐시 컨피그레이션 모드를 시작합니다.
cache-compressed	WebVPN 캐시 압축을 구성합니다.
expiry-time	캐싱 객체의 유효성을 재검사하지 않고 그 만료 시간을 구성합니다.
lmfactor	last-modified 타임스탬프만 있는 캐싱 객체에 대해 유효성 재검사 정책을 설정합니다.
max-object-size	캐싱할 객체의 최대 크기를 정의합니다.
min-object-size	캐싱할 객체의 최소 크기를 정의합니다.

disable service-settings

전화 프록시 기능을 사용할 때 IP 전화기의 서비스 설정을 비활성화하려면 phone-proxy 컨피그레이션 모드에서 **disable service-settings** 명령을 사용합니다. IP 전화기의 설정을 유지하려면 이 명령의 **no** 형식을 사용합니다.

disable service-settings

no disable service-settings

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

서비스 설정은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
전화 프록시 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

기본적으로 다음 설정이 IP 전화기에서 비활성화되어 있습니다.

- PC Port
- Gratuitous ARP
- Voice VLAN access
- Web Access
- Span to PC Port

구성된 각 IP 전화기에 대해 CUCM에 구성된 설정을 유지하려면 **no disable service-settings** 명령을 구성합니다.

예

다음 예에서는 ASA의 전화 프록시 기능을 사용하는 IP 전화기의 설정을 유지하는 방법을 보여줍니다.

```
ciscoasa(config-phone-proxy)# no disable service-settings
```

관련 명령

명령	설명
phone-proxy	전화 프록시 인스턴스를 구성합니다.
show phone-proxy	전화 프록시 관련 정보를 표시합니다.

display

ASA에서 DAP 특성 데이터베이스에 기록하는 특성 값 쌍을 표시하려면 dap 테스트 특성 모드에서 **display** 명령을 입력합니다.

display

명령 기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Dap 테스트 특성	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

일반적으로 ASA는 AAA 서버에서 사용자 권한 부여 특성을 검색하고 Cisco Secure Desktop, Host Scan, CNA 또는 NAC에서 엔드포인트 특성을 검색합니다. 이 특성 모드에서 테스트 명령에 대해 사용자 권한 부여 및 엔드포인트 특성을 지정합니다. ASA에서는 DAP 레코드에 대한 AAA 선택 특성 및 엔드포인트 선택 특성을 평가할 때 DAP 하위 시스템에서 참조하는 특성 데이터베이스에 이를 기록합니다. **display** 명령을 사용하면 이 특성을 콘솔에 표시할 수 있습니다.

관련 명령

명령	설명
attributes	특성 값 쌍을 설정할 수 있는 특성 컨피그레이션 모드를 시작합니다.
dynamic-access-policy-record	DAP 레코드를 생성합니다.
test dynamic-access-policy attributes	특성 하위 모드를 시작합니다.
test dynamic-access-policy execute	DAP를 생성하고 그 결과 액세스 정책을 콘솔에 표시하는 로직을 실행합니다.

distance bgp

BGP 경로에 대한 관리 거리를 구성하려면 주소군 컨피그레이션 모드에서 **distance bgp** 명령을 사용합니다. 관리 거리를 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다**.**

distance bgp *external-distance internal-distance local-distance*

no distance bgp

구문 설명

external-distance	외부 BGP 경로에 대한 관리 거리입니다. 외부 자동 시스템에서 학습한 경로는 외부 경로입니다. 이 인수의 값 범위는 1부터 255까지입니다.
internal-distance	내부 BGP 경로에 대한 관리 거리입니다. 로컬 자동 시스템의 피어에서 학습한 경로는 내부 경로입니다. 이 인수의 값 범위는 1부터 255까지입니다.
local-distance	로컬 BGP 경로에 대한 관리 거리입니다. 로컬 경로는 **네트워크** 라우터 컨피그레이션 명령을 실행하면 나열되는 네트워크입니다. 다른 프로세스에서 재배포되는 라우터나 네트워크에 대해 주로 백도어의 역할을 합니다. 이 인수의 값 범위는 1부터 255까지입니다.

기본값

이 명령이 구성되지 않았거나 no 형식이 입력되지 않을 경우 다음 값을 사용합니다.

external-distance: 20
internal-distance: 200
local-distance: 200

참고 영역이 255인 경로는 라우팅 테이블에 설치되지 않았습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

distance bgp 명령은 라우팅 정보 소스(예: 개별 라우터, 가우터 그룹)의 신뢰 등급을 구성하는 데 사용합니다. 관리 거리의 값은 1부터 255까지의 양의 정수입니다.

일반적으로 이 값이 클수록 신뢰 등급이 낮습니다. 관리 거리가 255라면 이 라우팅 정보 소스는 전혀 신뢰할 수 없으므로 무시해야 합니다. 다른 프로토콜이 eBGP(외부 BGP)를 통해 학습하는 것보다 우수한 노드 경로를 확실히 제공할 수 있거나 BGP가 일부 내부 경로를 우선적으로 사용해야 할 경우 이 명령을 사용합니다.

주의 내부 BGP 경로의 관리 거리를 변경하는 것은 위험하므로 권장되지 않습니다. 잘못된 컨피그레이션 때문에 라우팅 테이블이 일관성을 잃고 라우팅이 중단될 수 있습니다.

distance bgp 명령이 **distance mbgp** 명령을 대체합니다.

예 다음 예에서는 외부 영역이 10으로, 내부 영역이 50으로, 로컬 영역이 100으로 설정됩니다.

```
ciscoasa(config)# router bgp 50000
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)# distance bgp 10 50 100
ciscoasa(config-router-af)# end
```

distance eigrp

내부 및 외부 EIGRP 경로의 관리 거리를 구성하려면 라우터 컨피그레이션 모드에서 **distance eigrp** 명령을 사용합니다. 기본값으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

distance eigrp *internal-distance external-distance*

no distance eigrp

구문 설명

external-distance	EIGRP 외부 경로에 대한 관리 거리입니다. 외부 경로는 자동 시스템의 외부에 있는 네이버로부터 최상의 경로를 학습하는 것입니다. 유효한 값은 1부터 255까지입니다.
internal-distance	EIGRP 내부 경로에 대한 관리 거리입니다. 내부 경로는 동일한 자동 시스템 내의 다른 엔티티로부터 학습한 것입니다. 유효한 값은 1부터 255까지입니다.

기본값

기본값은 다음과 같습니다.

- *external-distance* is 170
- *internal-distance* is 90

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

각 라우팅 프로토콜이 다른 라우팅 프로토콜과 다른 알고리즘을 기반으로 한 메트릭을 가지므로, 서로 다른 라우팅 프로토콜에 의해 생성된 동일한 목적지의 경로 2개 중 "최적의 경로"를 결정하지 못할 수도 있습니다. 관리 거리는 서로 다른 두 라우팅 프로토콜에 의해 동일한 목적지에 대한 각기 다른 경로가 2개 이상 있을 경우 최적의 경로를 선택하기 위해 ASA에서 사용하는 경로 매개변수입니다.

둘 이상의 라우팅 프로토콜이 ASA에서 실행 중일 경우, **distance eigrp** 명령을 사용하면 EIGRP 라우팅 프로토콜에 의해 검색된 경로의 기본 관리 거리를 나머지 라우팅 프로토콜과 비교하여 조정할 수 있습니다. 표 12-1에서는 ASA에서 지원하는 라우팅 프로토콜의 기본 관리 거리를 나열합니다.

표 12-1 기본 관리 거리

경로 소스	기본 관리 거리
연결된 인터페이스	0
고정 경로	1
EIGRP 요약 경로	5
내부 EIGRP	90
OSPF	110
RIP	120
EIGRP 외부 경로	170
알 수 없음	255

이 명령의 **no** 형식은 키워드나 인수가 없습니다. 이 명령의 **no** 형식을 사용하면 내부 및 외부 EIGRP 경로 모두의 기본 관리 거리가 복원됩니다.

예

다음 예에서는 **distance eigrp** 명령을 사용하여 모든 EIGRP 내부 경로의 관리 거리를 80으로, 모든 EIGRP 외부 경로의 관리 거리를 115로 설정합니다. EIGRP 외부 경로의 관리 거리를 115로 설정하면, 특정 목적지에 대해 EIGRP에 의해 검색된 경로가 OSPF가 아닌 RIP에 의해 검색된 동일한 경로보다 우선적으로 적용됩니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.7.0
ciscoasa(config-router)# network 172.16.0.0
ciscoasa(config-router)# distance eigrp 90 115
```

관련 명령

명령	설명
router eigrp	EIGRP 라우팅 프로세스를 생성하고 이 프로세스에 대한 컨피그레이션 모드로 들어갑니다.

distance(OSPFv3)

경로 유형에 따라 OSPFv3 경로 관리 거리를 정의하려면 IPv6 라우터 컨피그레이션 모드에서 **distance** 명령을 사용합니다. 기본값으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

distance [ospf {external | intra-area | inter-area}] *distance*

no distance [**ospf** {**external | intra-area | inter-area**}] *distance*

구문 설명

distance	관리 거리를 지정합니다. 유효한 값은 10부터 254까지입니다.
external	(선택 사항) OSPFv3 경로에 대해 외부 type 5 및 type 7 경로를 지정합니다.
inter-area	(선택 사항) OSPFv3 경로에 대해 영역 간(inter-area) 경로를 지정합니다.
intra-area	(선택 사항) OSPFv3 경로에 대해 영역 내(intra-area) 경로를 지정합니다.
ospf	(선택 사항) OSPFv3 경로에 대해 관리 거리를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
IPv6 라우터 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

OSPFv3 경로의 관리 거리를 설정하는 데 이 명령을 사용합니다.

예

다음 예에서는 OSPFv3의 외부 type 5 및 type 7 경로에 대한 관리 거리를 200으로 설정합니다.

```
ciscoasa(config-if)# ipv6 router ospf
ciscoasa(config-router)# distance ospf external 200
```

관련 명령

명령	설명
default-information originate	OSPFv3 라우팅 도메인에 이르는 기본 외부 경로를 생성합니다.
redistribute	한 라우팅 도메인의 IPv6 경로를 다른 라우팅 도메인에 재배포합니다.

distance ospf(OSPFv2)

경로 유형에 따라 OSPFv2 경로 관리 거리를 정의하려면 라우터 컨피그레이션 모드에서 **distance ospf** 명령을 사용합니다. 기본값으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

distance ospf [intra-area *d1***] [inter-area** *d2***] [external** *d3***]**

no distance ospf

구문 설명

d1, *d2*, and *d3*	각 경로 유형에 대한 영역을 지정합니다. 유효한 값의 범위는 1~255입니다.
external	(선택 사항) 다른 경로 도메인으로부터 재배포를 통해 학습한 경로에 대한 영역을 설정합니다.
inter-area	(선택 사항) 어떤 영역에서 다른 영역으로 가는 모든 경로의 관리 거리를 설정합니다.
intra-area	(선택 사항) 어떤 영역 내에 있는 모든 경로의 관리 거리를 설정합니다.

기본값

d1, *d2*, *d3*의 기본값은 110입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

하나 이상의 키워드 및 인수를 지정해야 합니다. 관리 거리의 각 유형에 대해 개별적으로 명령을 입력할 수 있습니다. 그러나 컨피그레이션에서는 하나의 명령으로 나타납니다. 관리 거리를 재입력할 경우 해당 경로 유형의 관리 거리만 변경됩니다. 나머지 경로 유형의 관리 거리는 그대로 유지됩니다.

이 명령의 **no** 형식은 키워드나 인수가 없습니다. 이 명령의 **no** 형식을 사용하면 모든 경로 유형에서 기본 관리 거리를 복원합니다. 여러 경로 유형이 구성된 상태에서 어느 한 경로 유형에 대해 기본 관리 거리를 복원하려는 경우 다음 중 하나를 수행하면 됩니다.

- 그 경로 유형을 기본값으로 직접 설정합니다.
- 이 명령의 **no** 형식을 사용하여 전체 컨피그레이션을 제거한 다음 유지하려는 경로 유형의 컨피그레이션을 재입력합니다.

예

다음 예에서는 외부 경로의 관리 거리를 150으로 설정합니다.

```
ciscoasa(config-router)# distance ospf external 105
ciscoasa(config-router)#
```

다음 예에서는 각 경로 유형에 대해 개별적으로 명령을 입력할 경우 라우터 컨피그레이션에서 어떻게 하나의 명령으로 나타나는지 보여줍니다.

```
ciscoasa(config-rtr)# distance ospf intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf intra-area 105
ciscoasa(config-rtr)# distance ospf external 105
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
ciscoasa(config)#
```

다음 예에서는 각 관리 거리를 105로 설정한 다음 외부 관리 거리만 150으로 변경하는 방법을 보여줍니다. **show running-config router ospf** 명령은 어떻게 외부 경로 유형의 값만 바뀌고 나머지 경로 유형에서는 이전에 설정된 값이 유지되는지 보여줍니다.

```
ciscoasa(config-rtr)# distance ospf external 105 intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf external 150
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
ciscoasa(config)#
```

관련 명령

명령	설명
router ospf	OSPFv2의 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 OSPFv2 명령을 표시합니다.

distribute-list

OSPF(Open Shortest Path First) 업데이트에서 수신했거나 발신한 네트워크를 필터링하려면 라우터 컨피그레이션 모드에서 **distribute-list** 명령을 사용합니다. 필터를 변경하거나 취소하려면 이 명령의 no 형식을 사용합니다.

distribute-list *access-list name* **[in |out] [interface** *if_name***]**

no distribute-list *access-list name* **[in |out]**

구문 설명

access-list name	표준 IP 액세스 목록 이름입니다. 이 목록에서는 라우팅 업데이트에서 수신하고 억제할 네트워크를 정의합니다.
in	수신 라우팅 업데이트에 액세스 목록 또는 경로-정책을 적용합니다.
out	발신 라우팅 업데이트에 액세스 목록 또는 경로-정책을 적용합니다. **out** 키워드는 라우터 컨피그레이션 모드에서만 사용할 수 있습니다.
interface *if_name*	(선택 사항) 라우팅 업데이트를 적용할 인터페이스입니다. 인터페이스를 지정하면 그 인터페이스에서 수신한 라우팅 업데이트에만 액세스 목록이 적용됩니다.

기본값

네트워크는 필터링되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

어떤 인터페이스도 지정하지 않을 경우 액세스 목록은 모든 수신 업데이트에 적용됩니다.

예

다음 예에서는 외부 인터페이스에서 수신한 OSPF 라우팅 업데이트를 필터링합니다. 10.0.0.0 네트워크의 경로를 승인하고 다른 경로는 모두 삭제합니다.

```
ciscoasa(config)# access-list ospf_filter permit 10.0.0.0
ciscoasa(config)# access-list ospf_filter deny any
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ospf_filter in interface outside
```

관련 명령

명령	설명
distribute-list in	수신 라우팅 업데이트를 필터링합니다.
router ospf	OSPF 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

distribute-list in

수신 라우팅 업데이트를 필터링하려면 라우터 컨피그레이션 모드에서 **distribute-list in** 명령을 사용합니다. 필터링을 제거하려면 이 명령의 **no** 형식을 사용합니다.

distribute-list *acl* **in [interface** *if_name***]**

no distribute-list *acl* **in [interface** *if_name*]

구문 설명

acl	표준 액세스 목록의 이름입니다.
interface *if_name*	(선택 사항) 수신 라우팅 업데이트를 적용할 인터페이스입니다. 인터페이스를 지정하면 그 인터페이스에서 수신한 라우팅 업데이트에만 액세스 목록이 적용됩니다.

기본값

수신 업데이트에서 네트워크는 필터링되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

어떤 인터페이스도 지정하지 않을 경우 액세스 목록은 모든 수신 업데이트에 적용됩니다.

예

다음 예에서는 외부 인터페이스에서 수신한 RIP 라우팅 업데이트를 필터링합니다. 10.0.0.0 네트워크의 경로를 승인하고 다른 경로는 모두 삭제합니다.

```
ciscoasa(config)# access-list ripfilter permit 10.0.0.0
ciscoasa(config)# access-list ripfilter deny any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter in interface outside
```

다음 예에서는 외부 인터페이스에서 수신한 EIGRP 라우팅 업데이트를 필터링합니다. 10.0.0.0 네트워크의 경로를 승인하고 다른 경로는 모두 삭제합니다.

```
ciscoasa(config)# access-list eigrp_filter permit 10.0.0.0
ciscoasa(config)# access-list eigrp_filter deny any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter in interface outside
```

관련 명령

명령	설명
distribute-list out	발신 라우팅 업데이트를 필터링합니다.
router eigrp	EIGRP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
router rip	RIP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

distribute-list in(BGP)

수신 BGP(Border Gateway Protocol) 업데이트에서 수신한 경로 또는 네트워크를 필터링하려면 주소군 컨피그레이션 모드에서 **distribute-list in** 명령을 사용합니다. 배포 목록을 삭제하고 실행 중인 컨피그레이션 파일에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

distribute-list {*acl-name* | *prefix list-name*} **in**

no distribute-list {*acl-name* | *prefix list-name*} **in**

구문 설명

acl-name	IP 액세스 목록 이름입니다. 이 액세스 목록에서는 라우팅 업데이트에서 수신하고 억제할 네트워크를 정의합니다.
prefix *list-name*	접두사 목록의 이름입니다. 이 접두사 목록에서는 일치하는 접두사에 따라 라우팅 업데이트에서 수신하고 억제할 네트워크를 정의합니다.

기본값

이 명령이 미리 정의된 액세스 목록 또는 접두사 목록 없이 구성된 경우 배포 목록은 기본적으로 모든 트래픽을 허용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

distribute-list in 명령은 수신 BGP 업데이트를 필터링하는 데 사용합니다. 이 명령을 구성하기 전에 액세스 목록 또는 접두사 목록이 정의되어 있어야 합니다. 표준 및 확장 액세스 목록이 지원됩니다. IP 접두사 목록은 접두사의 비트 길이에 따라 필터링할 때 사용합니다. 전체 네트워크, 서브넷, 수퍼넷 또는 단일 호스트 경로를 지정할 수 있습니다. 배포 목록을 구성할 때 접두사 목록 컨피그레이션과 액세스 목록 컨피그레이션을 함께 사용할 수 없습니다. 배포 목록이 적용되기 전에 **clear bgp** 명령을 사용하여 세션을 재설정해야 합니다.

참고

- 사용 중인 Cisco IOS 소프트웨어의 버전에 따라 인터페이스 유형 및 번호 인수가 CLI에 표시될 수 있습니다. 그러나 이 인터페이스 인수는 어떤 Cisco IOS 소프트웨어 릴리스에서도 지원되지 않습니다.
- 배포 목록 대신 IP 접두사 목록(글로벌 컨피그레이션 모드에서 **ip prefix-list** 명령으로 구성)을 사용하는 것이 좋습니다. IP 접두사 목록이 성능 면에서 더 우수할 뿐 아니라 더 간단하게 구성할 수 있습니다. 배포 목록 컨피그레이션은 향후 CLI에서 삭제될 것입니다.

예

다음 예에서는 네트워크 10.1.1.0/24, 네트워크 192.168.1.0, 네트워크 10.108.0.0에서 보낸 트래픽만 받도록 BGP 라우팅 프로세스를 구성하기 위해 접두사 목록과 배포 목록을 정의합니다. 배포 목록을 활성화하기 위해 인바운드 경로의 새로 고침이 수행됩니다.

```
ciscoasa(config)# ip prefix-list RED permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list RED permit 10.108.0.0/16
ciscoasa(config)# ip prefix-list RED permit 192.168.1.0/24
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list prefix RED in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

다음 예에서는 네트워크 192.168.1.0 및 네트워크 10.108.0.0에서 보낸 트래픽만 받도록 BGP 라우팅 프로세스를 구성하기 위해 액세스 목록과 배포 목록을 정의합니다. 배포 목록을 활성화하기 위해 인바운드 경로의 새로 고침이 수행됩니다.

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.1.0
ciscoasa(config)# access-list distribute-list-acl permit 10.108.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list distribute-list-acl in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

관련 명령

명령	설명
clear bgp	하드 또는 소프트 리컨피그레이션을 사용하여 BGP 연결을 재설정합니다.
ip prefix-list	접두사 목록을 생성하거나 접두사 목록 엔트리를 추가합니다.

distribute-list out

발신 라우팅 업데이트를 필터링하려면 라우터 컨피그레이션 모드에서 **distribute-list out** 명령을 사용합니다. 필터링을 제거하려면 이 명령의 **no** 형식을 사용합니다.

distribute-list *acl* **out [interface** *if_name*] **[eigrp** *as_number* **| rip | ospf** *pid* **| static | connected]**

no distribute-list *acl* **out [interface** *if_name*] [**eigrp** *as_number* **| rip | ospf** *pid* **| static | connected]**

구문 설명

acl	표준 액세스 목록의 이름입니다.
connected	(선택 사항) 연결된 경로만 필터링합니다.
eigrp *as_number*	(선택 사항) 지정된 자동 시스템 번호에서 EIGRP 경로만 필터링합니다. *as_number* 인수는 ASA EIGRP 라우팅 프로세스의 자동 시스템 번호입니다.
interface *if_name*	(선택 사항) 발신 라우팅 업데이트를 적용할 인터페이스입니다. 인터페이스를 지정하면 그 인터페이스에서 수신한 라우팅 업데이트에만 액세스 목록이 적용됩니다.
ospf *pid*	(선택 사항) 지정된 OSPF 프로세스에 의해 검색된 OSPF 경로만 필터링합니다.
rip	(선택 사항) RIP 경로만 필터링합니다.
static	(선택 사항) 고정 경로만 필터링합니다.

기본값

발신 업데이트에서 네트워크는 필터링되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
8.0(2)	**eigrp** 키워드를 추가했습니다.

사용 지침

어떤 인터페이스도 지정하지 않을 경우 액세스 목록은 모든 발신 업데이트에 적용됩니다.

예

다음 예에서는 어떤 인터페이스에서 보내는 RIP 업데이트에서도 10.0.0.0 네트워크를 광고하지 않게 합니다.

```
ciscoasa(config)# access-list ripfilter deny 10.0.0.0
ciscoasa(config)# access-list ripfilter permit any
ciscoasa(config)# router rip
```

```
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter out
```

다음 예에서는 EIGRP 라우팅 프로세스가 외부 인터페이스에서 10.0.0.0 네트워크를 광고할 수 없게 합니다.

```
ciscoasa(config)# access-list eigrp_filter deny 10.0.0.0
ciscoasa(config)# access-list eigrp_filter permit any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter out interface outside
```

관련 명령

명령	설명
distribute-list in	수신 라우팅 업데이트를 필터링합니다.
router eigrp	EIGRP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
router rip	RIP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

distribute-list out(BGP)

아웃바운드 BGP 업데이트에서 네트워크를 광고하는 것을 억제하려면 라우터 컨피그레이션 모드에서 **distribute-list out** 명령을 사용합니다. 배포 목록을 삭제하고 실행 중인 컨피그레이션 파일에서 제거하려면 이 명령의 **no** 형식을 사용합니다.

distribute-list {*acl-name* | *prefix list-name*} **out** [*protocol process-number* | *connected* | **static**]

no distribute-list {*acl-name* | *prefix list-name*} **out** [*protocol process-number* | *connected* | **static**]

구문 설명

acl-name	IP 액세스 목록 이름입니다. 이 액세스 목록에서는 라우팅 업데이트에서 수신하고 억제할 네트워크를 정의합니다.
prefix *list-name*	접두사 목록의 이름입니다. 이 접두사 목록에서는 일치하는 접두사에 따라 라우팅 업데이트에서 수신하고 억제할 네트워크를 정의합니다.
protocol process-number	배포 목록을 적용할 라우팅 프로토콜을 지정합니다. BGP, EIGRP, OSPF, RIP가 지원됩니다. RIP를 제외한 모든 라우팅 프로토콜에서 프로세스 번호가 입력됩니다. 프로세스 번호의 값 범위는 1부터 65까지입니다.
connected	연결된 경로를 통해 학습된 피어와 네트워크를 지정합니다.
static	고정 경로를 통해 학습된 피어와 네트워크를 지정합니다.

기본값

이 명령이 미리 정의된 액세스 목록 또는 접두사 목록 없이 구성된 경우 배포 목록은 기본적으로 모든 트래픽을 허용합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
주소군 컨피그레이션	• 예	—	• 예	• 예	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

distribute-list out 명령은 아웃바운드 BGP 업데이트를 필터링하는 데 사용합니다. 이 명령을 구성하기 전에 액세스 목록 또는 접두사 목록이 정의되어 있어야 합니다. 표준 액세스 목록만 지원됩니다.

IP 접두사 목록은 접두사의 비트 길이에 따라 필터링할 때 사용합니다. 전체 네트워크, 서브넷, 수퍼넷 또는 단일 호스트 경로를 지정할 수 있습니다. 배포 목록을 구성할 때 접두사 목록 컨피그레이션과 액세스 목록 컨피그레이션을 함께 사용할 수 없습니다. 배포 목록이 적용되기 전에 **clear bgp** 명령을 사용하여 세션을 재설정해야 합니다.

참고

- 사용 중인 Cisco IOS 소프트웨어의 버전에 따라 인터페이스 유형 및 번호 인수가 CLI에 표시될 수 있습니다. 그러나 이 인터페이스 인수는 어떤 Cisco IOS 소프트웨어 릴리스에서도 지원되지 않습니다.
- 배포 목록 대신 IP 접두사 목록(글로벌 컨피그레이션 모드에서 **ip prefix-list** 명령으로 구성)을 사용하는 것이 좋습니다. IP 접두사 목록이 성능 면에서 더 우수할 뿐 아니라 더 간단하게 구성할 수 있습니다. 배포 목록 컨피그레이션은 향후 CLI에서 삭제될 것입니다.

protocol 및/또는 *process-number* 인수를 입력하면, 지정된 라우팅 프로세스에서 나온 경로에만 배포 목록이 적용됩니다. 이 배포 목록 명령에서 지정되지 않은 주소는 배포 목록이 구성된 후 발신 라우팅 업데이트에서 광고되지 않습니다.

인바운드 업데이트에서 네트워크 또는 경로의 수신을 억제하려면 **distribute-list in** 명령을 사용합니다.

예

다음 예에서는 BGP 라우팅 프로세스에서 네트워크 192.168.0.0만 광고하도록 구성하기 위해 접두사 목록과 배포 목록을 정의합니다. 배포 목록을 활성화하기 위해 아웃바운드 경로의 새로 고침이 수행됩니다.

```
ciscoasa(config)# ip prefix-list BLUE permit 192.168.0.0/16
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list prefix BLUE out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

다음 예에서는 BGP 라우팅 프로세스에서 네트워크 192.168.0.0만 광고하도록 구성하기 위해 액세스 목록과 배포 목록을 정의합니다. 배포 목록을 활성화하기 위해 아웃바운드 경로의 새로 고침이 수행됩니다.

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.0.0 0.0.255.255
ciscoasa(config)# access-list distribute-list-acl deny 0.0.0.0 255.255.255.255
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list distribute-list-acl out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

관련 명령

명령	설명
clear bgp	하드 또는 소프트 리컨피그레이션을 사용하여 BGP 연결을 재설정합니다.
ip prefix-list	접두사 목록을 생성하거나 접두사 목록 엔트리를 추가합니다.

13 장

dns domain-lookup ~ dynamic-filter whitelist 명령

dns domain-lookup

ASA가 DNS 서버에 DNS 요청을 보내 지원되는 명령의 이름을 조회하도록 하려면 글로벌 컨피그레이션 모드에서 **dns domain-lookup** 명령을 사용합니다. DNS 요청을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

구문 설명

interface_name	구성된 인터페이스의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.

예

다음 예에서는 DNS 서버에 DNS 요청을 보내 ASA에서 지원되는 명령의 이름을 조회하도록 합니다.

```
ciscoasa(config)# dns domain-lookup inside
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns-server-group 모드를 시작합니다. 여기서 DNS 서버 그룹을 구성할 수 있습니다.
show running-config dns-server group	기존 DNS 서버 그룹 컨피그레이션 중 하나 또는 전체를 표시합니다.

dns expire-entry-timer

확인된 FQDN(fully qualified domain name)의 TTL이 만료된 후 해당 IP 주소를 제거하려면 글로벌 컨피그레이션 모드에서 **dns expire-entry-timer** 명령을 사용합니다. 타이머를 제거하려면 이 명령의 **no** 형식을 사용합니다.

dns expire-entry-timer minutes *minutes*

no dns expire-entry-timer minutes *minutes*

구문 설명

minutes *minutes* 타이머 시간을 분 단위로 지정합니다. 유효한 값의 범위는 1분~65535분입니다.

기본값

기본적으로 DNS expire-entry-timer 값은 1분입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 확인된 FQDN의 TTL이 만료된 후 IP 주소를 제거하는 데 소요하는 시간을 지정합니다. IP 주소가 제거되면 ASA는 tmatch 조회 테이블을 다시 컴파일합니다.

이 명령은 DNS에 대해 연결된 네트워크 객체가 활성화된 경우에만 효력을 발휘합니다.

DNS expire-entry-timer의 기본값은 1분입니다. 그러면 DNS 엔트리의 TTL이 만료되고 1분 후에 IP 주소가 제거됩니다.

참고 기본값으로 설정 시, www.sample.com과 같이 일반 FQDN 호스트의 확인된 TTL의 기간이 짧은 경우 tmatch 조회 테이블의 재컴파일 빈도가 높을 수 있습니다. 보안을 유지하면서 tmatch 조회 테이블이 재컴파일되는 빈도를 줄이기 위해 DNS expire-entry-timer 값을 길게 지정할 수 있습니다.

예

다음 예에서는 240분이 지나면 확인된 엔트리를 제거합니다.

```
ciscoasa(config)# dns expire-entry-timer minutes 240
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns-server-group 모드를 시작합니다. 여기서 DNS 서버 그룹을 구성할 수 있습니다.
show running-config dns-server group	기존 DNS 서버 그룹 컨피그레이션 중 하나 또는 전체를 표시합니다.

dns name-server

ASA에 대해 DNS 서버를 구성하려면 글로벌 컨피그레이션 모드에서 **dns name-server** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

dns name-server *ipv4_addr* | *ipv6_addr*

no dns name-server *ipv4_addr* | *ipv6_addr*

구문 설명

ipv4_addr	DNS 서버의 IPv4 주소를 지정합니다.
ipv6_addr	DNS 서버의 IPv6 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.
9.0(1)	IPv6 주소 지원을 추가했습니다.

사용 지침

ASA의 DNS 서버 주소를 식별할 때 이 명령을 사용합니다. ASA는 DNS 서버의 IPv4 주소와 IPv6 주소를 모두 지원합니다.

예

다음 예에서는 IPv6 주소로 DNS 서버를 구성합니다.

```
ciscoasa(config)# dns domain-lookup
ciscoasa(config)# dns name-server 8080:1:2::2
ciscoasa(config)# dns retries 4
ciscoasa(config)# dns timeout 10
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns-server-group 모드를 시작합니다. 여기서 DNS 서버 그룹을 구성할 수 있습니다.
show running-config dns-server group	기존 DNS 서버 그룹 컨피그레이션 중 하나 또는 전체를 표시합니다.

dns poll-timer

ASA가 네트워크 객체 그룹에 정의된 FQDN의 확인을 위해 DNS 서버를 쿼리하는 시간의 타이머를 지정하려면 글로벌 컨피그레이션 모드에서 **dns poll-timer** 명령을 사용합니다. 타이머를 제거하려면 이 명령의 **no** 형식을 사용합니다.

dns poll-timer minutes *minutes*

no dns poll-timer minutes *minutes*

구문 설명

minutes *minutes*	타이머를 분 단위로 지정합니다. 유효한 값의 범위는 1분~65535분입니다.

기본값

기본적으로 DNS 타이머는 240분, 즉 4시간입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 ASA가 네트워크 객체 그룹에 정의된 FQDN의 확인을 위해 DNS 서버를 쿼리하는 시간의 타이머를 지정합니다. FQDN은 폴 DNS 타이머가 만료된 때와 확인된 IP 엔트리의 TTL이 만료된 때 중 더 빠른 시점에 정기적으로 확인됩니다.

이 명령은 하나 이상의 네트워크 객체 그룹이 활성화된 경우에만 효력을 발휘합니다.

예

다음 예에서는 DNS 폴 타이머를 240분으로 설정합니다.

```
ciscoasa(config)# dns poll-timer minutes 240
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns-server-group 모드를 시작합니다. 여기서 DNS 서버 그룹을 구성할 수 있습니다.
show running-config dns-server group	기존 DNS 서버 그룹 컨피그레이션 중 하나 또는 전체를 표시합니다.

dns update

DNS 폴 타이머가 만료될 때까지 기다리지 않고 DNS 조회를 시작하여 지정된 호스트 이름을 확인하려면 특별 권한 EXEC 모드에서 **dns update** 명령을 사용합니다.

dns update [host *fqdn_name***] [timeout seconds** *seconds***]**

구문 설명

host *fqdn_name*	DNS 업데이트를 수행할 호스트의 FQDN을 지정합니다.
timeout seconds *seconds*	시간 초과를 초 단위로 지정합니다.

기본값

기본적으로 시간 초과는 30초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 DNS 폴 타이머가 만료될 때까지 기다리지 않고 지정된 호스트 이름을 확인하기 위해 DNS 조회를 즉시 시작합니다. 옵션을 지정하지 않고 DNS 업데이트를 실행하면 모든 활성화된 호스트 그룹과 FQDN 호스트가 DNS 조회를 위해 선택됩니다. 이 명령의 실행이 종료되면 ASA에서는 명령 프롬프트에 [Done]을 표시하고 syslog 메시지를 생성합니다.

업데이트 작업이 시작되면 업데이트 시작 로그가 생성됩니다. 업데이트 작업이 끝나거나 타이머 만료로 중단되면 또 다른 syslog 메시지가 생성됩니다. 하나의 미처리 DNS 업데이트 작업만이 허용됩니다. 명령을 재실행할 경우 오류 메시지가 나타납니다.

예

다음 예에서는 DNS 업데이트를 수행합니다.

```
ciscoasa# dns update
ciscoasa# …
ciscoasa# [Done] dns update
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns-server-group 모드를 시작합니다. 여기서 DNS 서버 그룹을 구성할 수 있습니다.
show running-config dns-server group	기존 DNS 서버 그룹 컨피그레이션 중 하나 또는 전체를 표시합니다.

dns-group

WebVPN 터널 그룹을 위해 사용할 DNS 서버를 지정하려면 tunnel-group webvpn 컨피그레이션 모드에서 **dns-group** 명령을 사용합니다. 기본 DNS 그룹을 복원하려면 이 명령의 **no** 형식을 사용합니다.

dns-group *name*

no dns-group

구문 설명

name	터널 그룹을 위해 사용할 DNS 서버 그룹 컨피그레이션의 이름을 지정합니다.

기본값

기본값은 DefaultDNS입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

이 이름으로 어떤 DNS 그룹도 지정할 수 있습니다. **dns-group** 명령은 터널 그룹에 적합한 DNS 서버의 호스트 이름을 확인합니다.

dns server-group 명령을 사용하여 DNS 그룹을 구성합니다.

예

다음 예에서는 이름이 "dnsgroup1"인 DNS 그룹의 사용을 지정하는 사용자 지정 명령을 보여줍니다.

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# dns-group dnsgroup1
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns-server-group 모드를 시작합니다. 여기서 DNS 서버 그룹을 구성할 수 있습니다.
show running-config dns-server group	기존 DNS 서버 그룹 컨피그레이션 중 하나 또는 전체를 표시합니다.
tunnel-group webvpn-attributes	WebVPN 터널 그룹 특성을 구성하기 위해 config-webvpn 모드를 시작합니다.

dns-guard

각 쿼리에 대해 반드시 하나의 DNS 응답을 보내는 DNS Guard 기능을 활성화하려면 파라미터 컨피그레이션 모드에서 **dns-guard** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dns-guard

no dns-guard

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

DNS Guard는 기본적으로 사용됩니다. **inspect dns** 명령이 구성되었다면, **policy-map type inspect dns** 명령이 정의되지 않았더라도 이 기능을 활성화할 수 있습니다. 비활성화하려면 정책 맵 구성에서 **no dns-guard** 명령을 명시적으로 지정해야 합니다. **inspect dns** 명령이 구성되지 않을 경우 **global dns-guard** 명령에 의해 동작이 결정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	컨텍스트	시스템
파라미터 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

DNS 헤더의 식별 필드를 사용하여 DNS 응답과 DNS 헤더를 매칭합니다. ASA에서 쿼리당 하나의 응답이 허용됩니다.

예

다음 예에서는 DNS 검사 정책 맵에서 DNS Guard를 활성화하는 방법을 보여줍니다.

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

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 구성을 모두 표시합니다.

dns-server

기본 및 보조 DNS 서버의 IP 주소를 설정하려면 group-policy 컨피그레이션 모드에서 **dns-server** 명령을 사용합니다. 실행 중인 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

dns-server {**value** *ip_address* [*ip_address*] | **none**}

no dns-server

구문 설명

none	**dns-server** 명령을 null 값으로 설정합니다. 즉 어떤 DNS 서버도 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 값을 상속할 수 없게 합니다.
value *ip_address*	기본 및 보조 DNS 서버의 IP 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 다른 그룹 정책에서 DNS 서버를 상속하는 것을 허용합니다. 서버를 상속할 수 없게 하려면 **dns-server none** 명령을 사용합니다.

dns-server 명령을 실행할 때마다 기존 설정을 덮어씁니다. 예를 들어 DNS 서버 x.x.x.x를 구성한 다음 DNS 서버 y.y.y.y를 구성할 경우, 두 번째 명령이 첫 번째 명령을 덮어쓰므로 y.y.y.y가 유일한 DNS 서버가 됩니다. 다중 서버의 경우도 마찬가지입니다. 이전에 구성된 서버를 덮어쓰지 않고 DNS 서버를 추가하려면 이 명령을 입력할 때 모든 DNS 서버의 IP 주소를 포함시킵니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 IP 주소 10.10.10.15와 10.10.10.45로 DNS 서버를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dns-server value 10.10.10.15 10.10.10.45
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
show running-config dns server-group	현재 실행 중인 DNS 서버 그룹 컨피그레이션을 보여줍니다.

dns server-group

터널 그룹에 사용할 DNS 서버에 대해 도메인 이름, 이름 서버, 재시도 횟수, 시간 초과 값을 지정하려면 글로벌 컨피그레이션 모드에서 **dns server-group** 명령을 사용합니다. 특정 DNS 서버 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

dns server -group *name*

no dns server-group

구문 설명

name	터널 그룹을 위해 사용할 DNS 서버 그룹 컨피그레이션의 이름을 지정합니다.

기본값

기본값은 DefaultDNS입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

이 이름으로 어떤 DNS 그룹도 지정할 수 있습니다. **dns server-group** 명령을 사용하여 DNS 그룹을 구성합니다.

예

다음 예에서는 이름이 "eval"인 DNS 서버 그룹을 구성합니다.

```
ciscoasa(config)# dns server-group eval
ciscoasa(config-dns-server-group)# domain-name cisco.com
ciscoasa(config-dns-server-group)# name-server 192.168.10.10
ciscoasa(config-dns-server-group)# retries 5
ciscoasa(config-dns-server-group)# timeout 7
ciscoasa(config-dns-server-group)#
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
show running-config dns server-group	현재 실행 중인 DNS 서버 그룹 컨피그레이션을 보여줍니다.

domain-name

기본 도메인 이름을 설정하려면 글로벌 컨피그레이션 모드에서 **domain-name** 명령을 사용합니다. 도메인 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다.

domain-name *name*

no domain-name [*name*]

구문 설명

name	최대 63자로 도메인 이름을 설정합니다.

기본값

기본 도메인 이름은 default.domain.invalid입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서는 부적격한 이름일 경우, 해당 이름 뒤에 도메인 이름을 추가합니다. 예를 들면 도메인 이름을 "example.com"으로 설정하고 부적격한 이름인 "jupiter"로 syslog 서버를 지정할 경우, ASA에서는 그 이름을 "jupiter.example.com"으로 바꾸어 표기합니다. 다중 컨텍스트 모드라면 시스템 실행 영역에서뿐 아니라 각 컨텍스트에 대해 도메인 이름을 설정할 수 있습니다.

예

다음 예에서는 도메인을 example.com으로 설정합니다.

```
ciscoasa(config)# domain-name example.com
```

관련 명령

명령	설명
dns domain-lookup	ASA에서 이름 조회를 할 수 있게 합니다.
dns name-server	ASA에 대한 DNS 서버를 식별합니다.
hostname	ASA 호스트 이름을 설정합니다.
show running-config domain-name	도메인 이름 컨피그레이션을 표시합니다.

domain-name(dns server-group)

기본 도메인 이름을 설정하려면 dns server-group 컨피그레이션 모드에서 **domain-name** 명령을 사용합니다. 도메인 이름을 제거하려면 이 명령의 **no** 형식을 사용합니다.

domain-name *name*

no domain-name [*name*]

구문 설명

name	최대 63자로 도메인 이름을 설정합니다.

기본값

기본 도메인 이름은 default.domain.invalid입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	컨텍스트	시스템
Dns server-group 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.1(1)	이 명령은 사용 중단된 **dns domain-lookup** 명령을 대체합니다.

사용 지침

ASA에서는 부적격한 이름일 경우, 해당 이름 뒤에 도메인 이름을 추가합니다. 예를 들면 도메인 이름을 "example.com"으로 설정하고 부적격한 이름인 "jupiter"로 syslog 서버를 지정할 경우, ASA에서는 그 이름을 "jupiter.example.com"으로 바꾸어 표기합니다. 다중 컨텍스트 모드라면 시스템 실행 영역에서뿐 아니라 각 컨텍스트에 대해 도메인 이름을 설정할 수 있습니다.

예

다음 예에서는 "dnsgroup1"을 위해 도메인을 "example.com"으로 설정합니다.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# domain-name example.com
```

관련 명령

명령	설명
clear configure dns	모든 DNS 명령을 제거합니다.
dns server-group	dns-server-group 컨피그레이션 모드를 시작합니다. 여기서 DNS 서버 그룹을 구성할 수 있습니다.
domain-name	전역에서 기본 도메인 이름을 설정합니다.
show running-config dns-server group	현재 DNS 서버 그룹 컨피그레이션 중 하나 또는 전체를 표시합니다.

downgrade

소프트웨어 버전을 다운그레이드하려면 글로벌 컨피그레이션 모드에서 **downgrade** 명령을 사용합니다.

downgrade [/noconfirm] *old_image_url old_config_url* **[activation-key** *old_key***]**

구문 설명

activation-key *old_key*	(선택 사항) 활성화 키를 되돌려야 하는 경우 기존 활성화 키를 입력하면 됩니다.
old_config_url	저장된 마이그레이션 이전의 컨피그레이션(기본적으로 disk0에 저장되어 있음)으로 경로를 지정합니다.
old_image_url	disk0, disk1, tftp, ftp 또는 smb에 있는 기존 이미지로 경로를 지정합니다.
/noconfirm	(선택 사항) 프롬프트 없이 다운그레이드합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 다음 기능을 완료하기 위한 바로가기입니다.

1. 부트 이미지 컨피그레이션 삭제(**clear configure boot**)
2. 부트 이미지를 기존 이미지로 설정(**boot system**)
3. (선택 사항) 새 활성화 키 입력(**activation-key**)
4. 실행 중인 컨피그레이션을 startup에 저장(**write memory**) 이는 BOOT 환경 변수를 기존 이미지로 설정합니다. 따라서 다시 로드할 때 기존 이미지가 로드됩니다.
5. 기존 컨피그레이션을 startup 컨피그레이션에 복사(**copy** *old_config_url* **startup-config**)
6. 다시 로드(**reload**)

예

다음 예에서는 확인 없이 다운그레이드합니다.

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

관련 명령

명령	설명
activation-key	활성화 키를 입력합니다.
boot system	부팅할 이미지를 설정합니다.
clear configure boot	부트 이미지 컨피그레이션을 지웁니다.
copy startup-config	컨피그레이션을 startup 컨피그레이션에 복사합니다.

download-max-size

다운로드할 객체에 대해 허용되는 최대 크기를 지정하려면 group-policy webvpn 컨피그레이션 모드에서 **download-max-size** 명령을 사용합니다. 이 객체를 컨피그레이션에서 제거하려면 이 명령의 **no** 버전을 사용합니다.

download-max-size *size*

no download-max-size

구문 설명

size	다운로드 객체에 허용되는 최대 크기를 지정합니다. 범위는 0부터 2147483647까지입니다.

기본값

기본 크기는 2147483647입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

크기를 0으로 설정하면 객체 다운로드가 허용되지 않습니다.

예

다음 예에서는 다운로드 객체의 최대 크기를 1500바이트로 설정합니다.

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# download-max-size 1500
```

관련 명령

명령	설명
post-max-size	게시할 객체의 최대 크기를 지정합니다.
upload-max-size	업로드할 객체의 최대 크기를 지정합니다.
webvpn	group-policy 컨피그레이션 모드 또는 username 컨피그레이션 모드에서 사용합니다. 그룹 정책 또는 사용자 이름에 적용되는 파라미터의 구성을 위해 webvpn 구성 모드를 시작할 수 있습니다.
webvpn	글로벌 컨피그레이션 모드에서 사용합니다. WebVPN을 위한 전역 설정을 구성할 수 있습니다.

drop

match 명령 또는 **class** 명령과 매치하는 모든 패킷을 삭제하려면 match 또는 class 컨피그레이션 모드에서 **drop** 명령을 사용합니다. 이 작업을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

drop [send-protocol-error] [log]

no drop [send-protocol-error] [log]

구문 설명

log	매치를 로깅합니다. syslog 메시지 번호는 애플리케이션에 따라 달라집니다.
send-protocol-error	프로토콜 오류 메시지를 보냅니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	컨텍스트	시스템
match 및 class 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

Modular Policy Framework를 사용할 경우, match 또는 class 컨피그레이션 모드에서 **drop** 명령을 사용하여 **match** 명령 또는 클래스 맵과 매치하는 패킷을 삭제합니다. 이 삭제 작업은 애플리케이션 트래픽의 검사 정책 맵에서 사용할 수 있습니다(**policy-map type inspect** 명령). 그러나 모든 애플리케이션이 이 작업을 허용하는 것은 아닙니다.

검사 정책 맵은 하나 이상의 **match** 및 **class** 명령으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 명령은 애플리케이션에 따라 다릅니다. 애플리케이션 트래픽을 식별하기 위해 **match** 또는 **class** 명령을 입력한 다음(**class** 명령에서 참조하는 기존 **class-map type inspect** 명령은 **match** 명령을 포함하고 있음) **drop** 명령을 입력하여 **match** 명령 또는 **class** 명령과 매치하는 모든 패킷을 삭제할 수 있습니다.

패킷을 삭제할 경우 검사 정책 맵에서 추가 작업이 수행되지 않습니다. 예를 들어, 첫 번째 작업에서 패킷을 삭제하면 더 이상 어떤 **match** 또는 **class** 명령과도 매칭하지 않습니다. 첫 번째 작업에서 패킷을 로깅하면 패킷 삭제와 같은 두 번째 작업이 발생할 수 있습니다. 동일한 **match** 또는 **class** 명령에 대해 **drop** 작업과 **log** 작업을 모두 구성할 수 있습니다. 그러면 패킷이 어떤 매치를 위해 삭제되기 전에 로깅됩니다.

레이어 3/4 정책 맵에서 **inspect** 명령을 사용하여 애플리케이션 검사를 활성화하면(**policy-map** 명령), 이 작업을 포함하는 검사 정책 맵을 활성화할 수 있습니다. 이를테면 http_policy_map이 이름인 검사 정책 맵에서 **inspect http http_policy_map** 명령을 입력합니다.

예

다음 예에서는 HTTP 트래픽 클래스 맵과 매칭할 때 패킷을 삭제하고 로그를 보냅니다. 동일한 패킷이 2번째 **match** 명령과도 매칭할 경우, 이미 삭제되었으므로 처리되지 않습니다.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop 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	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
policy-map type inspect	애플리케이션 검사를 위한 특별한 작업을 정의합니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

drop-connection

Modular Policy Framework를 사용할 경우, **match** 명령 또는 클래스 맵과 매칭하는 트래픽에 대해 match 또는 class 컨피그레이션 모드에서 **drop-connection** 명령을 사용하여 패킷을 삭제하고 연결을 종료합니다. 이 작업을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

drop-connection [send-protocol-error] [log]

no drop-connection [send-protocol-error] [log]

구문 설명

send-protocol-error	프로토콜 오류 메시지를 보냅니다.
log	매치를 로깅합니다. 시스템 로그 메시지 번호는 애플리케이션에 따라 달라집니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	컨텍스트	시스템
match 및 class 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

연결이 ASA의 연결 데이터베이스에서 제거됩니다. 이후에 이 삭제된 연결을 위해 ASA에 들어오는 패킷은 폐기됩니다. 이 연결 삭제 작업은 애플리케이션 트래픽의 검사 정책 맵에서 사용할 수 있습니다(**policy-map type inspect** 명령). 그러나 모든 애플리케이션이 이 작업을 허용하는 것은 아닙니다. 검사 정책 맵은 하나 이상의 **match** 및 **class** 명령으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 명령은 애플리케이션에 따라 다릅니다. 애플리케이션 트래픽을 식별하기 위해 **match** 또는 **class** 명령을 입력한 다음(**class** 명령에서 참조하는 기존 **class-map type inspect** 명령은 **match** 명령을 포함하고 있음) **match** 명령 또는 **class** 명령과 매칭하는 트래픽에 대해 **drop-connection** 명령을 입력하여 패킷을 삭제하고 연결을 종료할 수 있습니다.

패킷을 삭제하거나 연결을 종료할 경우 검사 정책 맵에서 추가 작업이 수행되지 않습니다. 예를 들어, 첫 번째 작업에서 패킷을 삭제하고 연결을 종료하면 더 이상 어떤 **match** 또는 **class** 명령과도 매칭하지 않습니다. 첫 번째 작업에서 패킷을 로깅하면 패킷 삭제와 같은 두 번째 작업이 발생할 수 있습니다. 동일한 **match** 또는 **class** 명령에 대해 **drop-connection** 작업과 **log** 작업을 모두 구성할 수 있습니다. 그러면 패킷이 어떤 매칭에 대해 삭제되기 전에 로깅됩니다.

레이어 3/4 정책 맵에서 **inspect** 명령을 사용하여 애플리케이션 검사를 활성화하면(**policy-map** 명령) 이 작업을 포함하는 검사 정책 맵을 활성화할 수 있습니다. 이를테면 이름이 http_policy_map인 검사 정책 맵에서 **inspect http http_policy_map** 명령을 입력합니다.

예

다음 예에서는 http-traffic 클래스 맵과 매칭할 때 패킷을 삭제하고 연결을 종료하며 로그를 보냅니다. 동일한 패킷이 2번째 **match** 명령과도 매칭할 경우, 이미 삭제되었으므로 처리되지 않습니다.

```
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
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
policy-map type inspect	애플리케이션 검사를 위한 특별한 작업을 정의합니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

dtls port

DTLS 연결을 위해 포트를 지정하려면 webvpn 컨피그레이션 모드에서 **dtls port** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

dtls port *number*

no dtls port *number*

구문 설명

number	UDP 포트 번호이며, 값의 범위는 1부터 65535까지입니다.

기본값

기본 포트 번호는 443입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 DTLS를 사용하는 SSL VPN 연결에 쓰일 UDP 포트를 지정합니다.

DTLS는 일부 SSL 연결에서 발생하는 레이턴시 및 대역폭 문제를 방지하고 패킷 지연에 민감한 실시간 애플리케이션의 성능을 높입니다.

예

다음 예에서는 webvpn 컨피그레이션 모드를 시작하고 DTLS를 위해 포트 444를 지정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# dtls port 444
```

관련 명령

명령	설명
dtls enable	인터페이스에서 DTLS를 활성화합니다.
svc dtls	SSL VPN 연결을 설정하는 그룹 또는 사용자를 위해 DTLS를 활성화합니다.
vpn-tunnel-protocol	SSL을 비롯하여 ASA에서 원격 액세스에 허용하는 VPN 프로토콜을 지정합니다.

duplex

구리(RJ-45) 이더넷 인터페이스의 듀플렉스를 설정하려면 인터페이스 컨피그레이션 모드에서 **duplex** 명령을 사용합니다. 듀플렉스 설정을 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

duplex {auto | full | half}

no duplex

구문 설명

auto	듀플렉스 모드를 자동으로 감지합니다.
full	듀플렉스 모드를 풀(full) 듀플렉스로 설정합니다.
half	듀플렉스 모드를 하프(half) 듀플렉스로 설정합니다.

기본값

기본 설정은 자동 감지입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령은 **interface** 명령의 키워드에서 인터페이스 구성 모드 명령으로 이동했습니다.

사용 지침

물리적 인터페이스에서만 듀플렉스 모드를 설정합니다.

파이버 미디어에서는 **duplex** 명령을 사용할 수 없습니다.

네트워크에서 자동 감지를 지원하지 않을 경우 듀플렉스 모드를 특정 값으로 설정합니다.

ASA 5500 시리즈의 RJ-45 인터페이스에서는 기본 자동 협상 설정에 Auto-MDI/MDIX 기능도 포함되어 있습니다. Auto-MDI/MDIX 기능을 사용하면 자동 협상 단계에서 직선형 케이블이 감지될 경우 내부 crossover를 수행하게 되므로 crossover 케이블을 연결할 필요가 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 듀플렉스가 자동 협상으로 설정되어야 합니다. 속도 및 듀플렉스를 고정된 값으로 설정할 경우 두 설정 모두에서 자동 협상이 비활성화되므로 Auto-MDI/MDIX도 비활성화됩니다.

PoE 포트가 있을 때 듀플렉스를 **auto** 이외의 값으로 설정할 경우, IEEE 802.3af를 지원하지 않는 Cisco IP Phone과 Cisco 무선 액세스 포인트는 감지되지 않아 전원도 공급되지 않습니다.

예

다음 예에서는 듀플렉스 모드를 풀 듀플렉스로 설정합니다.

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

관련 명령

명령	설명
clear configure interface	인터페이스에 대한 모든 컨피그레이션을 지웁니다.
interface	인터페이스를 구성하고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show running-config interface	인터페이스 컨피그레이션을 표시합니다.
speed	인터페이스 속도를 설정합니다.

dynamic-access-policy-config

DAP 레코드를 구성하고 관련된 정책 특성에 액세스하려면 글로벌 컨피그레이션 모드에서 **dynamic-access-policy-config** 명령을 사용합니다. 기존 DAP 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-access-policy-config *name* | *activate*

no dynamic-access-policy-config

구문 설명

activate	DAP 선택 컨피그레이션 파일을 활성화합니다.
name	DAP 레코드의 이름을 지정합니다. 이 이름은 최대 64자까지 허용되며, 공백을 포함할 수 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중 모드	
명령 모드	라우팅 모드	투명 모드	단일 모드	컨텍스트	시스템
글로벌 컨피그레이션(name)	• 예	• 예	• 예	• 예	—
특별 권한 EXEC(activate)	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

하나 이상의 DAP 레코드를 생성하려면 글로벌 컨피그레이션 모드에서 **dynamic-access-policy-config** 명령을 사용합니다. DAP 선택 컨피그레이션 파일을 활성화하려면 **dynamic-access-policy-config** 명령을 *activate* 인수와 함께 사용합니다.

이 명령을 사용할 때 dynamic-access-policy-record 모드를 시작합니다. 여기서 명명된 DAP 레코드의 특성을 설정할 수 있습니다. dynamic-access-policy-record 모드에서 다음과 같은 명령을 사용할 수 있습니다.

- **action**
- **description**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

예

다음 예에서는 user1이라는 DAP 레코드를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# dynamic-access-policy-config user1
ciscoasa(config-dynamic-access-policy-record)#
```

관련 명령

명령	설명
dynamic-access-policy-record	DAP 레코드에 액세스 정책 특성을 채웁니다.
show running-config dynamic-access-policy-record	모든 DAP 레코드 또는 명명된 DAP 레코드에 대해 실행 중인 컨피그레이션을 표시합니다.

dynamic-access-policy-record

DAP 레코드를 생성하고 이를 액세스 정책 특성으로 채우려면 글로벌 컨피그레이션 모드에서 **dynamic-access-policy-record** 명령을 사용합니다. 기존 DAP 레코드를 제거하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-access-policy-record *name*

no dynamic-access-policy-record *name*

구문 설명

name	DAP 레코드의 이름을 지정합니다. 이 이름은 최대 64자까지 허용되며, 공백을 포함할 수 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

하나 이상의 DAP 레코드를 생성하려면 글로벌 컨피그레이션 모드에서 **dynamic-access-policy-record** 명령을 사용합니다. 이 명령을 사용할 때 dynamic-access-policy-record 모드를 시작합니다. 여기서 명명된 DAP 레코드의 특성을 설정할 수 있습니다. dynamic-access-policy-record 모드에서 다음과 같은 명령을 사용할 수 있습니다.

- **action** (**continue**, **terminate**, or **quarantine**)
- **description**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

예

다음 예에서는 Finance라는 DAP 레코드를 만드는 방법을 보여줍니다.

```
ciscoasa(config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)#
```

관련 명령

명령	설명
clear config dynamic-access-policy-record	모든 DAP 레코드 또는 명명된 DAP 레코드를 제거합니다.
dynamic-access-policy-config url	DAP 선택 컨피그레이션 파일을 구성합니다.
show running-config dynamic-access-policy-record	모든 DAP 레코드 또는 명명된 DAP 레코드에 대해 실행 중인 컨피그레이션을 표시합니다.

dynamic-authorization

AAA 서버 그룹에 대해 RADIUS 동적 권한(권한의 변경) 서비스를 활성화하려면 aaa-server host 컨피그레이션 모드에서 **dynamic-authorization** 명령을 사용합니다. 동적 권한 부여를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-authorization port *number*

no dynamic-authorization port *number*

구문 설명

port *port_number*	(선택 사항) ASA에서 동적 권한 포트를 지정합니다. 범위는 1부터 65535까지입니다.

기본값

기본 RADIUS 포트는 1645입니다. 기본적으로 동적 권한 부여는 활성화되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

사용 지침

일단 정의되면 해당 RADIUS 서버 그룹이 CoA 알림에 등록되고 ASA는 ISE에서 보내는 CoA 정책 업데이트를 포트에서 수신합니다.

다음 예에서는 단일 서버로 하나의 RADIUS 그룹을 추가하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

다음 예에서는 권한 부여 전용으로, 동적 권한 부여(CoA) 업데이트와 시간별 어카운팅을 위해 ISE 서버 객체를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
```

다음 예에서는 ISE와의 비밀번호 인증을 위해 터널 그룹을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

다음 예에서는 ISE와의 로컬 인증서 검증 및 권한 부여를 위해 터널 그룹을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

관련 명령

명령	설명
authorize-only	RADIUS 서버 그룹에 대해 권한 부여 전용 모드를 활성화합니다.
interim-accounting-update	RADIUS interim-accounting-update 메시지를 생성할 수 있게 합니다.
without-csd	특정 터널-그룹과의 연결에 대해 호스트 스캔 처리를 끕니다.

dynamic-filter ambiguous-is-black

Botnet Traffic Filter의 그레이리스트 트래픽을 삭제 목적의 블랙리스트 트래픽으로 처리하려면 글로벌 컨피그레이션 모드에서 **dynamic-filter ambiguous-is-black** 명령을 사용합니다. 그레이리스트 트래픽을 허용하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-filter ambiguous-is-black

no dynamic-filter ambiguous-is-black

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

dynamic-filter enable 명령과 **dynamic-filter drop blacklist** 명령을 차례로 구성한 경우, 이 명령은 그레이리스트 트래픽을 삭제 목적의 블랙리스트 트래픽으로 간주합니다. 이 명령을 활성화하지 않을 경우 그레이리스트 트래픽은 삭제되지 않습니다.

모호한 주소는 여러 도메인 이름과 연결된 것이지만, 이 도메인 이름 모두가 블랙리스트에 있는 것은 아닙니다. 이 주소는 그레이리스트에 있습니다.

예

다음 예에서는 외부 인터페이스에서 모든 포트 80 트래픽을 모니터링하고 위협 레벨이 보통 이상인 블랙리스트 및 그레이리스트 트래픽을 삭제합니다.

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
ciscoasa(config)# dynamic-filter ambiguous-is-black
```

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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령의 이름을 조회하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 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 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter blacklist

Botnet Traffic Filter 블랙리스트를 수정하려면 글로벌 컨피그레이션 모드에서 **dynamic-filter blacklist** 명령을 사용합니다. 블랙리스트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-filter blacklist

no dynamic-filter blacklist

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

dynamic-filter 블랙리스트 컨피그레이션 모드를 시작한 다음 **address** 및 **name** 명령을 사용하여 블랙리스트에 악성으로 표시할 도메인 이름 또는 IP 주소(호스트 또는 서브넷)를 직접 입력할 수 있습니다. 이름 또는 IP 주소를 화이트리스트에도 추가할 수 있습니다(**dynamic-filter whitelist** 명령 참조). 그러면 동적 블랙리스트와 화이트리스트 모두에 나타나는 이름 또는 주소가 syslog 메시지와 보고서에서만 화이트리스트 주소로 식별됩니다. 화이트리스트의 주소는 동적 블랙리스트에 없더라도 syslog 메시지가 표시됩니다.

고정 블랙리스트 엔트리는 항상 위협 레벨이 매우 높음으로 표시됩니다.

도메인 이름을 고정 데이터베이스에 추가하면, ASA에서 1분간 기다렸다가 그 도메인 이름에 대한 DNS 요청을 보내고 도메인 이름/IP 주소 쌍을 *DNS 호스트 캐시*에 추가합니다. (이 작업은 백그라운드 프로세스이므로 ASA 컨피그레이션을 계속하는 데 영향을 주지 않습니다.) 또한 DNS 패킷 검사를 Botnet Traffic Filter 스누핑과 함께 활성화하는 것이 좋습니다(**inspect dns dynamic-filter-snooping** 명령 참조). ASA는 다음과 같은 경우에 고정 블랙리스트 도메인 이름을 확인하는 데 일반 DNS 조회가 아닌 Botnet Traffic Filter 스누핑을 사용합니다.

- ASA DNS 서버를 사용할 수 없습니다.
- ASA에서 일반 DNS 요청을 보내기 전에 1분간 대기하는 동안 연결이 시작됩니다.

DNS 스누핑이 사용될 경우, 감염된 호스트가 고정 데이터베이스에 있는 이름에 대해 DNS 요청을 보내면 ASA는 DNS 패킷 내부에서 그 도메인 이름과 해당 IP 주소를 찾고 그 이름과 IP 주소를 DNS 역방향 조회 캐시에 추가합니다.

고정 데이터베이스를 사용하면 블랙리스트에 추가할 도메인 이름 또는 IP 주소로 동적 데이터베이스를 확장할 수 있습니다.

Botnet Traffic Filter 스누핑을 활성화하지 않을 경우, 위와 같은 상황 중 하나가 발생하면 그 트래픽은 Botnet Traffic Filter에서 모니터링하지 않습니다.

참고 이 명령을 실행하려면 ASA에서 DNS 서버를 사용해야 합니다. **dns domain-lookup** 및 **dns server-group** 명령을 참조하십시오.

예

다음 예에서는 블랙리스트 및 화이트리스트의 엔트리를 생성합니다.

```
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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 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 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.

명령	설명
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter database fetch

Botnet Traffic Filter를 위해 동적 데이터베이스의 다운로드를 테스트하려면 특별 권한 EXEC 모드에서 **dynamic-filter database fetch** 명령을 사용합니다.

dynamic-filter database fetch

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

실제 데이터베이스는 ASA에 저장되지 않습니다. 다운로드되었다가 삭제됩니다. 이 명령은 테스트 목적으로만 사용합니다.

예

다음 예에서는 동적 데이터베이스의 다운로드를 테스트합니다.

```
ciscoasa# dynamic-filter database fetch
```

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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.

명령	설명
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 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 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매칭하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter database find

도메인 이름 또는 IP 주소가 Botnet Traffic Filter를 위한 동적 데이터베이스에 포함되었는지 확인하려면 특별 권한 EXEC 모드에서 **dynamic-filter database find** 명령을 사용합니다.

dynamic-filter database find *string*

구문 설명

string	*string*은 완전한 도메인 이름 또는 IP 주소일 수 있습니다. 또는 이름 또는 주소 중 3자 이상을 입력하고 검색할 수 있습니다. 정규식은 데이터베이스 검색에서 지원되지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

일치하는 항목이 여러 개일 경우 처음 2개가 표시됩니다. 세부 검색으로 특정 매치를 찾으려면 더 긴 문자열로 입력합니다.

예

다음 예에서는 "example.com"이라는 문자열로 검색하여 1개의 항목을 찾습니다.

```
ciscoasa# dynamic-filter database find bad.example.com

   bad.example.com
Found 1 matches
```

다음 예에서는 "bad"라는 문자열로 검색하여 3개 이상의 항목을 찾습니다.

```
ciscoasa# dynamic-filter database find bad

   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

관련 명령

명령	설명
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령의 이름을 조회하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 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 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter database purge

실행 중인 메모리에서 Botnet Traffic Filter 동적 데이터베이스를 수동으로 삭제하려면 특별 권한 EXEC 모드에서 **dynamic-filter database purge** 명령을 사용합니다.

dynamic-filter database purge

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

데이터베이스 파일은 실행 중인 메모리에 저장됩니다. 플래시 메모리에 저장되지 않습니다. 데이터베이스를 삭제해야 할 경우 **dynamic-filter database purge** 명령을 사용합니다.

데이터베이스 파일을 삭제하기 전에 **no dynamic-filter use-database** 명령을 사용하여 데이터베이스 사용을 비활성화합니다.

예

다음 예에서는 데이터베이스 사용을 비활성화한 다음 데이터베이스를 삭제합니다.

```
ciscoasa(config)# no dynamic-filter use-database
ciscoasa(config)# dynamic-filter database purge
```

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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령의 이름을 조회하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 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 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter drop blacklist

Botnet Traffic Filter를 사용하여 블랙리스트 트래픽을 자동으로 삭제하려면 글로벌 컨피그레이션 모드에서 **dynamic-filter drop blacklist** 명령을 사용합니다. 자동 삭제를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-filter drop blacklist [interface *name***] [action-classify-list** *subset_access_list***] [threat-level {eq** *level* **| range** *min max***}]**

no dynamic-filter drop blacklist [interface *name***] [action-classify-list** *subset_access_list***] [threat-level {eq** *level* **| range** *min max***}]**

구문 설명

action-classify-list *sub_access_list*	(선택 사항) 삭제할 트래픽의 하위 집합을 식별합니다. 액세스 목록을 만들려면 **access-list extended** 명령을 참조하십시오. 삭제된 트래픽은 반드시 **dynamic-filter enable** 명령에 의해 식별되는 모니터링 대상 트래픽과 같거나 그 하위 집합이어야 합니다. 이를테면 **dynamic-filter enable** 명령에 대해 액세스 목록을 지정할 때 이 명령에서 **action-classify-list**를 지정할 경우, 이는 **dynamic-filter enable** 액세스 목록의 하위 집합이어야 합니다.
interface *name*	(선택 사항) 모니터링을 특정 인터페이스로 제한합니다. 삭제된 트래픽은 반드시 **dynamic-filter enable** 명령에 의해 식별되는 모니터링 대상 트래픽과 같거나 그 하위 집합이어야 합니다. 인터페이스 관련 명령이 글로벌 명령에 우선합니다.
threat-level {*eq level* | *range min max*}	(선택 사항) 위협 레벨을 설정하여 삭제되는 트래픽을 제한합니다. 명시적으로 위협 레벨을 설정하지 않을 경우 사용되는 레벨은 **threat-level range moderate very-high**입니다. **참고** 불가피한 이유로 설정을 변경해야 하는 경우가 아니라면 기본 설정을 사용하는 것이 좋습니다 . *level*, *min*, *max* 옵션은 다음과 같습니다. • **very-low** • **low** • **moderate** • **high** • **very-high** **참고** 고정 블랙리스트 엔트리는 항상 위협 레벨이 매우 높음으로 표시됩니다 .

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

기본 위협 레벨은 **threat-level range moderate very-high**입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

어떤 트래픽을 삭제하더라도 먼저 **dynamic-filter enable** 명령을 구성해야 합니다. 삭제된 트래픽은 반드시 모니터링 대상 트래픽과 같거나 그 하위 집합이어야 합니다.

각 인터페이스 및 글로벌 정책에 대해 이 명령을 여러 번 입력할 수 있습니다. 인터페이스/글로벌 정책에 대한 복수의 명령에서 트래픽을 중복하여 지정해서는 안 됩니다. 명령이 매치되는 정확한 순서를 제어할 수 없으므로, 트래픽이 중복되면 어떤 명령이 매치되는지 알 수 없게 됩니다. 예를 들어, 모든 트래픽과 매치하는 명령(**action-classify-list** 키워드 없음)과 특정 인터페이스에 대한 **action-classify-list** 키워드가 있는 명령을 함께 지정하지 마십시오. 그러면 트래픽이 **action-classify-list** 키워드가 있는 명령과 절대 매치하지 않을 수도 있습니다. 또한 **action-classify-list** 키워드를 갖는 명령을 여러 개 지정할 경우, 각 액세스 목록이 고유해야 하며 네트워크가 중복되지 않아야 합니다.

예

다음 예에서는 외부 인터페이스에서 모든 포트 80 트래픽을 모니터링하고 위협 레벨이 보통 이상인 트래픽을 삭제합니다.

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령의 이름을 조회하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.

명령	설명
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 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 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter enable

Botnet Traffic Filter를 활성화하려면 글로벌 컨피그레이션 모드에서 **dynamic-filter enable** 명령을 사용합니다. Botnet Traffic Filter를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-filter enable [interface *name***] [classify-list** *access_list***]**

no dynamic-filter enable [interface *name***] [classify-list** *access_list***]**

구문 설명

classify-list *access_list*	확장 액세스 목록을 사용하여 모니터링할 트래픽을 식별합니다(**access-list extended** 명령 참조). 액세스 목록을 만들지 않을 경우 기본적으로 모든 트래픽을 모니터링합니다.
interface *name*	모니터링을 특정 인터페이스로 제한합니다.

기본값

Botnet Traffic Filter는 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

Botnet Traffic Filter는 각 초기 연결 패킷의 소스 및 목적지 IP 주소를 동적 데이터베이스, 고정 데이터베이스, DNS 역방향 조회 캐시, DNS 호스트 캐시에 있는 IP 주소와 비교하고 syslog 메시지를 전송하거나 매치하는 트래픽을 삭제합니다.

악성코드는 알려지지 않은 호스트에 설치되는 악성 소프트웨어입니다. 악성코드가 알려진 악성 IP 주소에 연결을 시작하면, Botnet Traffic Filter에서는 개인 데이터(비밀번호, 신용카드 번호, 키 스트로크, 독점 데이터) 전송 같은 네트워크 활동을 시도하는 악성코드를 감지할 수 있습니다. Botnet Traffic Filter에서는 알려진 악성 도메인 이름 및 IP 주소로 구성된 동적 데이터베이스를 참조하여 들어오고 나가는 연결을 검사한 다음 모든 의심스러운 활동을 기록합니다. 로컬 "블랙리스트" 또는 "화이트리스트"에 IP 주소나 도메인 이름을 입력하여 만든 고정 데이터베이스로 동적 데이터베이스를 보완할 수도 있습니다.

DNS 스누핑은 별도로 활성화됩니다(**inspect dns dynamic-filter-snoop** 명령 참조). 일반적으로 Botnet Traffic Filter를 최대한 활용하려면 DNS 스누핑을 활성화해야 합니다. 하지만 원한다면 Botnet Traffic Filter 로깅을 독립적으로 사용할 수 있습니다. 동적 데이터베이스에 대한 DNS 스누핑을 사용하지 않을 경우, Botnet Traffic Filter는 고정 데이터베이스 엔트리와 동적 데이터베이스에 있는 IP 주소만 사용합니다. 동적 데이터베이스에 있는 도메인 이름은 사용하지 않습니다.

Botnet Traffic Filter 주소 범주

Botnet Traffic Filter는 다음과 같은 주소를 모니터링합니다.

- 확인된 악성코드 주소—이 주소는 "블랙리스트"에 있습니다.
- 확인된 허용 주소—이 주소는 "화이트리스트"에 있습니다.
- 모호한 주소—이 주소는 여러 도메인 이름과 연결되어 있으나, 그 모든 도메인 이름이 블랙리스트에 있는 것은 아닙니다. 이 주소는 "그레이리스트"에 있습니다.
- 목록에 없는 주소—이 주소는 미확인 상태이며 어떤 목록에도 포함되지 않았습니다.

확인된 주소에 대해 Botnet Traffic Filter 가 수행하는 작업

dynamic-filter enable 명령을 사용하여 Botnet Traffic Filter가 의심스러운 활동을 로깅하게 할 수 있습니다. 또한 **dynamic-filter drop blacklist** 명령을 사용하여 의심스러운 트래픽을 자동으로 차단하도록 구성할 수도 있습니다.

목록에 없는 주소는 어떤 syslog 메시지도 생성하지 않습니다. 그러나 블랙리스트, 화이트리스트, 그레이리스트의 주소는 유형에 따라 다른 syslog 메시지를 생성합니다. Botnet Traffic Filter는 번호가 338*nnn*인 상세한 syslog 메시지를 생성합니다. 들어오고 나가는 연결, 블랙리스트, 화이트리스트, 그레이리스트 주소, 기타 여러 변수에 따라 메시지가 달라집니다. 그레이리스트에는 여러 도메인 이름과 연결되는 주소가 포함되어 있으나, 그 모든 도메인 이름이 블랙리스트에 있는 것은 아닙니다.

syslog 메시지에 대한 자세한 내용은 syslog 메시지 가이드를 참조하십시오.

예

다음 예에서는 외부 인터페이스에서 모든 포트 80 트래픽을 모니터링하고 위협 레벨이 보통 이상인 트래픽을 삭제합니다.

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령의 이름을 조회하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.

명령	설명
dynamic-filter updater-client enable	동적 데이터베이스의 다운로드를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스의 사용을 활성화합니다.
dynamic-filter whitelist	Botnet Traffic Filter 화이트리스트를 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매칭하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter updater-client enable

Botnet Traffic Filter를 위한 동적 데이터베이스를 Cisco 업데이트 서버에서 다운로드하게 하려면 글로벌 컨피그레이션 모드에서 **dynamic-filter updater-client enable** 명령을 사용합니다. 동적 데이터베이스의 다운로드를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-filter updater-client enable

no dynamic-filter updater-client enable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

다운로드는 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

데이터베이스가 ASA에 설치되어 있지 않은 경우 약 2분 후에 데이터베이스를 다운로드합니다. 업데이트 서버가 향후 업데이트를 위해 ASA에서 서버를 폴링할 빈도를 결정합니다. 대개는 1시간마다 폴링합니다.

Botnet Traffic Filter는 정기적으로 Cisco 업데이트 서버에서 동적 데이터베이스의 업데이트를 받을 수 있습니다.

이 데이터베이스는 확인된 악성 도메인 이름 및 IP 주소 수천 개를 포함합니다. DNS 회신의 도메인 이름이 동적 데이터베이스의 어떤 이름과 일치할 경우 Botnet Traffic Filter는 그 이름과 IP 주소를 *DNS 역방향 조회 캐시*에 추가합니다. 감염된 호스트가 악성코드 사이트의 IP 주소와의 연결을 시작하면 ASA는 의심스러운 활동을 알리는 syslog 메시지를 보냅니다.

이 데이터베이스를 사용하려면 URL에 액세스할 수 있도록 ASA의 도메인 이름 서버를 구성해야 합니다. 동적 데이터베이스에서 도메인 이름을 사용하려면 DNS 패킷 검사와 Botnet Traffic Filter 스누핑을 함께 활성화해야 합니다. ASA는 DNS 패킷 내부에 도메인 이름 및 해당 IP 주소가 있는지 찾습니다.

어떤 경우에는 IP 주소 자체가 동적 데이터베이스에서 제공되며, Botnet Traffic Filter는 DNS 요청을 검사할 필요 없이 그 IP 주소로 가는 모든 트래픽을 로깅합니다.

데이터베이스 파일은 실행 중인 메모리에 저장됩니다. 플래시 메모리에 저장되지 않습니다. 데이터베이스를 삭제해야 할 경우 **dynamic-filter database purge** 명령을 사용합니다.

참고 이 명령을 실행하려면 ASA에서 DNS 서버를 사용해야 합니다. **dns domain-lookup** 및 **dns server-group** 명령을 참조하십시오.

예

다음 다중 모드 예에서는 동적 데이터베이스의 다운로드를 활성화하고 context1 및 context2에서 데이터베이스의 사용을 활성화합니다.

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

다음 단일 모드 예에서는 동적 데이터베이스의 다운로드를 활성화하고 데이터베이스의 사용을 활성화합니다.

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령에 대해 이름 조회를 수행하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns name-server	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 클래스 또는 모든 트래픽에 대해 Botnet Traffic Filter를 활성화합니다.
dynamic-filter use-database	동적 데이터베이스의 사용을 활성화합니다.
dynamic-filter whitelist	Botnet Traffic Filter 화이트리스트를 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.

명령	설명
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter use-database

Botnet Traffic Filter를 위한 동적 데이터베이스를 활성화하려면 글로벌 컨피그레이션 모드에서 **dynamic-filter use-database** 명령을 사용합니다. 동적 데이터베이스의 사용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-filter use-database

no dynamic-filter use-database

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

데이터베이스의 사용은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

다운로드한 데이터베이스의 사용을 비활성화하는 기능은 다중 컨텍스트 모드에서 유용합니다. 즉 컨텍스트별로 데이터베이스의 사용을 구성할 수 있습니다. 동적 데이터베이스의 다운로드를 활성화하려면 **dynamic-filter updater-client enable** 명령을 참조하십시오.

예

다음 다중 모드 예에서는 동적 데이터베이스의 다운로드를 활성화하고 context1 및 context2에서 데이터베이스의 사용을 활성화합니다.

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

다음 단일 모드 예에서는 동적 데이터베이스의 다운로드를 활성화하고 데이터베이스의 사용을 활성화합니다.

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령의 이름을 조회하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 클래스 또는 모든 트래픽에 대해 Botnet Traffic Filter를 활성화합니다.
dynamic-filter updater-client enable	동적 데이터베이스의 다운로드를 활성화합니다.
dynamic-filter whitelist	Botnet Traffic Filter 화이트리스트를 수정합니다.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매치하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

dynamic-filter whitelist

Botnet Traffic Filter 화이트리스트를 수정하려면 글로벌 컨피그레이션 모드에서 **dynamic-filter whitelist** 명령을 사용합니다. 화이트리스트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

dynamic-filter whitelist

no dynamic-filter whitelist

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

고정 데이터베이스를 사용하면 화이트리스트에 넣을 도메인 이름 또는 IP 주소로 동적 데이터베이스를 확장할 수 있습니다. dynamic-filter 화이트리스트 컨피그레이션 모드를 시작한 다음 **address** 및 **name** 명령을 사용하여 화이트리스트에 정상으로 표시할 도메인 이름 또는 IP 주소(호스트 또는 서브넷)를 직접 입력할 수 있습니다. 동적 블랙리스트와 고정 화이트리스트에 모두 표시되는 이름이나 주소는 syslog 메시지 및 보고서에서는 화이트리스트 주소로만 식별됩니다. 화이트리스트의 주소는 동적 블랙리스트에 없더라도 syslog 메시지가 표시됩니다. **dynamic-filter blacklist** 명령을 사용하여 고정 블랙리스트에 이름 또는 IP 주소를 입력할 수 있습니다.

도메인 이름을 고정 데이터베이스에 추가하면, ASA에서 1분간 기다렸다가 그 도메인 이름에 대한 DNS 요청을 보내고 도메인 이름/IP 주소 쌍을 *DNS 호스트 캐시*에 추가합니다. 이 작업은 백그라운드 프로세스이므로 ASA 컨피그레이션을 계속하는 데 영향을 주지 않습니다. 또한 Botnet Traffic Filter 스누핑으로 DNS 패킷 검사를 활성화하는 것이 좋습니다(**inspect dns dynamic-filter-snooping** 명령 참조). ASA는 다음과 같은 경우에 고정 블랙리스트 도메인 이름을 확인하는 데 일반 DNS 조회가 아닌 Botnet Traffic Filter 스누핑을 사용합니다.

- ASA DNS 서버를 사용할 수 없습니다.
- ASA에서 일반 DNS 요청을 보내기 전에 1분간 대기하는 동안 연결이 시작됩니다.

DNS 스누핑이 사용될 경우, 감염된 호스트가 고정 데이터베이스에 있는 이름에 대해 DNS 요청을 보내면 ASA는 DNS 패킷 내부에서 그 도메인 이름과 해당 IP 주소를 찾고 그 이름과 IP 주소를 DNS 역방향 조회 캐시에 추가합니다.

Botnet Traffic Filter 스누핑을 활성화하지 않을 경우, 위와 같은 상황 중 하나가 발생하면 그 트래픽은 Botnet Traffic Filter에서 모니터링하지 않습니다.

참고 이 명령을 실행하려면 ASA에서 DNS 서버를 사용해야 합니다. **dns domain-lookup** 및 **dns server-group** 명령을 참조하십시오.

예

다음 예에서는 블랙리스트 및 화이트리스트의 엔트리를 생성합니다.

```
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 보고 데이터를 지웁니다.
clear dynamic-filter statistics	Botnet Traffic Filter 통계를 지웁니다.
dns domain-lookup	이 명령을 사용하면 ASA에서 지원되는 명령의 이름을 조회하도록 DNS 서버에 DNS 요청을 보낼 수 있습니다.
dns server-group	ASA에 대한 DNS 서버를 식별합니다.
dynamic-filter ambiguous-is-black	작업을 위해 그레이리스트 트래픽을 블랙리스트 트래픽으로 처리합니다.
dynamic-filter blacklist	Botnet Traffic Filter 블랙리스트를 수정합니다.
dynamic-filter database fetch	Botnet Traffic Filter 동적 데이터베이스를 직접 검색합니다.
dynamic-filter database find	동적 데이터베이스에서 도메인 이름 또는 IP 주소를 검색합니다.
dynamic-filter database purge	Botnet Traffic Filter 동적 데이터베이스를 직접 삭제합니다.
dynamic-filter drop blacklist	블랙리스트 트래픽을 자동으로 삭제합니다.
dynamic-filter enable	액세스 목록을 지정하지 않으면 특정 트래픽 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.
inspect dns dynamic-filter-snoop	Botnet Traffic Filter 스누핑으로 DNS 검사를 활성화합니다.
name	블랙리스트 또는 화이트리스트에 이름을 추가합니다.
show asp table dynamic-filter	가속 보안 경로에 설치된 Botnet Traffic Filter 규칙을 표시합니다.

명령	설명
show dynamic-filter data	동적 데이터베이스에 대한 정보를 표시합니다. 여기에는 동적 데이터베이스가 마지막으로 다운로드된 시점, 데이터베이스의 버전, 데이터베이스에 포함된 엔트리 수, 10개의 샘플 엔트리 등이 포함됩니다.
show dynamic-filter dns-snoop	Botnet Traffic Filter DNS 스누핑 요약을 표시합니다. 또는 **detail** 키워드를 사용하면 실제 IP 주소와 이름을 표시합니다.
show dynamic-filter reports	최상위 10개 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서를 생성합니다.
show dynamic-filter statistics	Botnet Traffic Filter로 모니터링한 연결 수, 그중에서 화이트리스트, 블랙리스트, 그레이리스트와 매칭하는 연결 수를 표시합니다.
show dynamic-filter updater-client	updater 서버에 대한 정보를 표시합니다. 여기에는 서버 IP 주소, 다음에 ASA가 서버와 연결할 시점, 마지막으로 설치된 데이터베이스 버전이 포함됩니다.
show running-config dynamic-filter	컨피그레이션을 실행중인 Botnet Traffic Filter를 표시합니다.

파 트 4

E ~ H 명령

14 장

eigrp log-neighbor-changes ~ export webvpn webcontent 명령

eigrp log-neighbor-changes

EIGRP 네이버 인접성 변경 사항의 로깅을 활성화하려면 라우터 컨피그레이션 모드에서 **eigrp log-neighbor-changes** 명령을 사용합니다. 이 기능을 끌려면 이 명령의 **no** 형식을 사용합니다.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

eigrp log-neighbor-changes 명령은 기본적으로 활성화되어 있습니다. 이 명령의 **no** 형식만 실행 중인 컨피그레이션에 나타납니다.

예

다음 예에서는 EIGRP 네이버 변경의 로깅을 비활성화합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-changes
```

관련 명령

명령	설명
eigrp log-neighbor-warnings	네이버 경고 메시지의 로깅을 활성화합니다.
router eigrp	EIGRP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

eigrp log-neighbor-warnings

EIGRP 네이버 경고 메시지의 로깅을 활성화하려면 라우터 컨피그레이션 모드에서 **eigrp log-neighbor-warnings** 명령을 사용합니다. 이 기능을 끌려면 이 명령의 **no** 형식을 사용합니다.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

구문 설명

seconds	(선택 사항) 반복되는 네이버 경고 메시지의 시간 간격(초)입니다. 유효한 값은 1~65535입니다. 반복 경고가 이 간격에 발생할 경우 로깅되지 않습니다.

기본값

이 명령은 기본적으로 활성화되어 있습니다. 모든 네이버 경고 메시지가 로깅됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

eigrp log-neighbor-warnings 명령은 기본적으로 활성화되어 있습니다. 이 명령의 **no** 형식만 실행 중인 컨피그레이션에 나타납니다.

예

다음 예에서는 EIGRP 네이버 경고 메시지의 로깅을 비활성화합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-warnings
```

다음 예에서는 EIGRP 네이버 경고 메시지를 로깅하고 5분(300초) 간격으로 경고 메시지를 반복합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp log-neighbor-warnings 300
```

관련 명령

명령	설명
eigrp log-neighbor-messages	EIGRP 네이버 인접성의 변경 사항 로깅을 활성화합니다.
router eigrp	EIGRP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

eigrp router-id

EIGRP 라우팅 프로세스에서 사용하는 라우터 ID를 지정하려면 라우터 컨피그레이션 모드에서 **eigrp router-id** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

구문 설명

ip-addr	IP 주소(점으로 구분된 10진수) 형식의 라우터 ID. 0.0.0.0 또는 255.255.255.255를 라우터 ID로 사용할 수 없습니다.

기본값

지정되지 않으면 ASA의 최상위 IP 주소가 라우터 ID로 사용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

eigrp router-id 명령이 구성되지 않을 경우 EIGRP는 ASA의 최상위 IP 주소를 자동으로 선택하여 EIGRP 프로세스 시작 시 라우터 ID로 사용합니다. **no router eigrp** 명령을 사용하여 EIGRP 프로세스를 제거하지 않는 한 또는 **eigrp router-id** 명령을 사용하여 라우터 ID를 수동으로 구성하지 않는 한 라우터 ID는 바뀌지 않습니다.

라우터 ID는 외부 경로의 발신 라우터를 식별하는 데 사용합니다. 외부 경로가 로컬 라우터 ID와 함께 수신될 경우 그 경로는 무시됩니다. 이를 방지하려면 **eigrp router-id** 명령을 사용하여 라우터 ID에 대한 전역 주소를 지정합니다.

각 EIGRP 라우터에 고유한 값이 구성되어야 합니다.

예

다음 예에서는 172.16.1.3을 EIGRP 라우팅 프로세스의 고정 라우터 ID로 구성합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp router-id 172.16.1.3
```

관련 명령

명령	설명
router eigrp	EIGRP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드를 시작합니다.
show running-config router	전역 라우터 컨피그레이션에서 명령을 표시합니다.

eigrp stub

EIGRP 라우팅 프로세스를 stub 라우팅 프로세스로 구성하려면 라우터 컨피그레이션 모드에서 **eigrp stub** 명령을 사용합니다. EIGRP stub 라우팅을 제거하려면 이 명령의 **no** 형식을 사용합니다.

eigrp stub [receive-only] | {[connected] [redistributed] [static] [summary]}

no eigrp stub [receive-only] | {[connected] [redistributed] [static] [summary]}

구문 설명

connected	(선택 사항) 연결된 경로를 광고합니다.
receive-only	(선택 사항) ASA를 수신 전용 네이버로 설정합니다.
redistributed	(선택 사항) 다른 라우팅 프로토콜에서 재배포된 경로를 광고합니다.
static	(선택 사항) 고정 경로를 광고합니다.
summary	(선택 사항) 요약 경로를 광고합니다.

기본값

Stub 라우팅은 활성화되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

eigrp stub 명령을 사용하여 ASA를 stub로 구성합니다. 그러면 ASA는 모든 IP 트래픽을 배포 라우터로 보냅니다.

receive-only 키워드를 사용하면 ASA가 임의의 경로를 자동 시스템의 다른 어떤 라우터와도 공유할 수 없습니다. ASA는 EIGRP 네이버에서만 업데이트를 받습니다. 다른 어떤 키워드도 **receive-only** 키워드와 함께 사용할 수 없습니다.

connected, **static**, **summary**, **redistributed** 키워드 중 하나 이상 지정할 수 있습니다. 이 키워드 중 하나를 **eigrp stub** 명령과 함께 사용하면 해당 키워드에 의해 지정된 경로 유형만 전송됩니다.

connected 키워드는 EIGRP stub 라우팅 프로세스에서 연결된 경로를 보내는 것을 허용합니다. 연결된 경로가 **network** 문에 포함되지 않을 경우 EIGRP 프로세스에서 **redistribute** 명령을 사용하여 연결된 경로를 재배포하는 것이 필요할 수 있습니다.

static 키워드는 EIGRP stub 라우팅 프로세스에서 고정 경로를 보내는 것을 허용합니다. 이 옵션이 구성되지 않으면 EIGRP는 일반적으로 자동으로 재배포되는 내부 고정 경로를 비롯한 어떤 고정 경로도 보내지 않습니다. 역시 **redistribute static** 명령을 사용하여 고정 경로를 재배포해야 합니다.

summary 키워드는 EIGRP stub 라우팅 프로세스에서 요약 경로를 보내는 것을 허용합니다. **summary-address eigrp** 명령을 사용하여 요약 경로를 수동으로 만들 수 있습니다. 또는 **auto-summary** 명령이 활성화되면 요약 경로가 자동으로 만들어집니다(이 명령은 기본적으로 활성화되어 있음).

redistributed 키워드는 EIGRP stub 라우팅 프로세스에서 EIGRP 라우팅 프로세스에 재배포되었던, 다른 라우팅 프로토콜의 경로를 보낼 수 있게 합니다. 이 옵션을 구성하지 않으면 EIGRP는 재배포된 경로를 광고하지 않습니다.

예

다음 예에서는 **eigrp stub** 명령을 사용하여 ASA를 EIGRP stub로 구성하고 연결 경로와 요약 경로를 광고하게 합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected summary
```

다음 예에서는 **eigrp stub** 명령을 사용하여 ASA를 EIGRP stub로 구성하고 연결 경로와 고정 경로를 광고하게 합니다. 요약 경로 전송은 허용되지 않습니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected static
```

다음 예에서는 **eigrp stub** 명령을 사용하여 ASA를 EIGRP stub로 구성하고 EIGRP 업데이트만 수신하게 합니다. 연결 경로, 요약 경로, 고정 경로 정보는 전송되지 않습니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 eigrp
ciscoasa(config-router)# eigrp stub receive-only
```

다음 예에서는 **eigrp stub** 명령을 사용하여 ASA를 EIGRP stub로 구성하고 다른 라우팅 프로토콜에서 EIGRP에 재배포된 경로를 광고하게 합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub redistributed
```

다음 예에서는 선택 사항인 인수 없이 **eigrp stub** 명령을 사용합니다. 인수 없이 **eigrp stub** 명령을 사용하면 기본적으로 연결 경로와 고정 경로를 광고합니다.

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub
```

관련 명령

명령	설명
router eigrp	실행 중인 컨피그레이션에서 EIGRP 라우터 컨피그레이션 모드 명령을 지웁니다.
show running-config router eigrp	실행 중인 컨피그레이션의 EIGRP 라우터 컨피그레이션 모드 명령을 표시합니다.

eject

ASA 외부 Compact Flash 디바이스의 제거를 지원하려면 사용자 EXEC 모드에서 **eject** 명령을 사용합니다.

eject [/noconfirm] *disk1:*

구문 설명

disk1:	꺼낼 디바이스를 지정합니다.
/noconfirm	ASA에서 물리적으로 외부 플래시 디바이스를 제거하기 전에 디바이스 제거 확인 메시지를 표시하지 않도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

eject 명령을 사용하면 ASA 5500 시리즈에서 Compact Flash 디바이스를 안전하게 제거할 수 있습니다.

다음 예에서는 ASA에서 *disk1*을 물리적으로 제거하기 전에 **eject** 명령을 사용하여 이 디바이스를 정상적으로 종료하는 방법을 보여줍니다.

```
ciscoasa# eject /noconfig disk1:
It is now safe to remove disk1:
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

관련 명령

명령	설명
show version	운영 체제 소프트웨어에 대한 정보를 표시합니다.

email

등록 과정에서 인증서의 SAN(Subject Alternative Name) 확장에 지정된 이메일 주소를 포함시키려면 crypto ca-trustpoint 컨피그레이션 모드에서 **email** 명령을 사용합니다. 기본 설정으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

email *address*

no email

구문 설명

address	이메일 주소를 지정합니다. 최대 길이는 64자입니다.

기본값

기본적으로 설정되지 않습니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 trustpoint central의 crypto ca-trustpoint 컨피그레이션 모드를 시작하고 trustpoint central에 대한 등록 요청에 이메일 주소 user1@user.net을 포함시킵니다.

```
ciscoasa(config)# crypto ca-trustpoint central
ciscoasa(ca-trustpoint)# email user1@user.net
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca-trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.

enable

특별 권한 EXEC 모드를 시작하려면 사용자 EXEC 모드에서 **enable** 명령을 사용합니다.

enable [*level***]**

구문 설명

level	(선택 사항) 0~15의 권한 레벨. enable 인증(**aaa authentication enable console** 명령)과 함께 사용하지 않습니다.

기본값

enable 인증(**aaa authentication enable console** 명령)을 사용하지 않는 한 권한 레벨 15를 입력합니다. enable 인증을 사용하는 경우에는 사용자 이름에 대해 구성된 레벨에 따라 기본 레벨이 결정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

기본적으로 enable 비밀번호는 비어 있습니다. 비밀번호를 설정하려면 **enable password** 명령을 참조하십시오.

enable 인증을 사용하지 않을 경우 **enable** 명령을 입력하면 사용자 이름이 enable_*level*로 바뀝니다. 여기서 기본 레벨은 15입니다. enable 인증(**aaa authentication enable console** 명령)을 사용할 경우 사용자 이름과 그 레벨이 유지됩니다. 사용자 이름을 유지하는 것은 명령 권한 부여(**aaa authorization command** 명령, 로컬 또는 TACACS+ 사용)에 중요합니다.

레벨 2 이상이면 특별 권한 EXEC 모드가 시작됩니다. 레벨 0과 1은 사용자 EXEC 모드가 시작됩니다. 그 사이의 레벨을 사용하려면 로컬 명령 권한 부여(**aaa authorization command LOCAL** 명령)를 활성화하고 **privilege** 명령을 통해 이 명령을 다른 권한 레벨로 설정합니다. TACACS+ 명령 권한 부여에서는 ASA에 구성된 권한 레벨을 사용하지 않습니다.

현재 권한 레벨을 보려면 **show curpriv** 명령을 참조하십시오.

특별 권한 EXEC 모드를 종료하려면 **disable** 명령을 입력합니다.

예

다음 예에서는 특별 권한 EXEC 모드를 시작합니다.

```
ciscoasa> enable
Password: Pa$$w0rd
ciscoasa#
```

다음 예에서는 레벨 10에 대해 특별 권한 EXEC 모드를 시작합니다.

```
ciscoasa> enable 10
Password: Pa$$w0rd10
ciscoasa#
```

관련 명령

명령	설명
enable password	enable 비밀번호를 설정합니다.
disable	특별 권한 EXEC 모드를 종료합니다.
aaa authorization command	명령 권한 부여를 구성합니다.
privilege	로컬 명령 권한 부여를 위해 명령 권한 레벨을 설정합니다.
show curpriv	현재 로그인한 사용자 이름과 사용자 권한 레벨을 표시합니다.

enable(webvpn, e-mail proxy, config-mdm-proxy)

이전에 구성된 인터페이스에서 WebVPN, MDM proxy 또는 이메일 프록시 액세스를 활성화하려면 **enable** 명령을 사용합니다. WebVPN에서는 webvpn 컨피그레이션 모드에서 이 명령을 사용합니다. 이메일 프록시(IMAP4S, POP3S, SMTPS)의 경우 해당 이메일 프록시 컨피그레이션 모드에서 이 명령을 사용합니다. MDM 프록시는 config-mdm-proxy 모드에서 이 명령을 사용합니다. 인터페이스에서 WebVPN을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

enable *ifname*

no enable

구문 설명

ifname	이전에 구성된 인터페이스를 식별합니다. 인터페이스를 구성하려면 **nameif** 명령을 사용합니다.

기본값

WebVPN은 기본적으로 비활성화되어 있습니다. MDM 프록시는 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Imap4s 컨피그레이션	• 예	—	• 예	—	—
Pop3s 컨피그레이션	• 예	—	• 예	—	—
Smtps 컨피그레이션	• 예	—	• 예	—	—
Webvpn 컨피그레이션	• 예	—	• 예	—	—
config-mdm-proxy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
9.3(1)	이 명령은 이제 config-mdm-proxy 모드에서 사용할 수 있습니다.

예

다음 예에서는 Outside라는 인터페이스에서 WebVPN을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable Outside
```

다음 예에서는 Outside라는 인터페이스에서 POP3S 이메일 프록시를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# enable Outside
```

다음 예에서는 Outside라는 인터페이스에서 MDM 프록시를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# mdm-proxy
ciscoasa(config-mdm-proxy)# enable Outside
```

enable(cluster group)

클러스터링을 활성화하려면 클러스터 그룹 컨피그레이션 모드에서 **enable** 명령을 사용합니다. 클러스터링을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

enable [as-slave | noconfirm]

no enable

구문 설명

as-slave	(선택 사항) 실행 중인 컨피그레이션에 비호환 명령이 있는지 확인하지 않고 클러스터링을 활성화하며, 슬레이브가 현재의 어떤 선택에서도 마스터가 될 가능성 없이 클러스터에 참여하게 합니다. 이 컨피그레이션은 마스터 유닛에서 동기화된 컨피그레이션이 덮어씁니다.
noconfirm	(선택 사항) **enable** 명령을 입력하면 ASA는 실행 중인 컨피그레이션을 검사하여 클러스터링에서 지원되지 않는 기능을 위한 비호환 명령이 있는지 확인합니다. 여기에는 기본 컨피그레이션에 포함되었을 명령도 포함됩니다. 비호환 명령을 삭제할지 묻습니다. **No**를 선택하면 클러스터링이 활성화되지 않습니다. 확인을 건너뛰고 비호환 명령을 자동으로 삭제하려면 **noconfirm** 키워드를 사용합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

활성화된 1번째 유닛에서 마스터 유닛 선택이 일어납니다. 1번째 유닛이 지금까지는 클러스터의 유일한 멤버이므로 마스터 유닛이 됩니다. 이 기간에는 어떤 컨피그레이션 변경도 하지 마십시오.

이미 마스터 유닛이 있는 상태에서 클러스터에 슬레이브 유닛을 추가하는 경우, **enable as-slave** 명령을 사용하여 만일의 컨피그레이션 비호환성(대개는 아직 클러스터링이 구성되지 않은 인터페이스가 있는 경우)도 방지할 수 있습니다.

클러스터링을 비활성화하려면 **no enable** 명령을 입력합니다.

참고 클러스터링을 비활성화할 경우 모든 데이터 인터페이스가 종료되고 관리 인터페이스만 활성 상태가 됩니다 . 해당 유닛을 클러스터링에서 완전히 제거하려면 (이로써 활성 데이터 인터페이스를 갖기 위해서는) 전체 클러스터 그룹 컨피그레이션을 제거해야 합니다 .

예

다음 예에서는 클러스터링을 활성화하고 비호환 컨피그레이션을 제거합니다.

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용하면 ASA에서는 cLACP를 통해 네이버 스위치와 EtherChannel을 협상합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드를 시작합니다.
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.
health-check	클러스터 상태 검사 기능을 활성화합니다. 여기에는 유닛 상태 모니터링 및 인터페이스 상태 모니터링이 포함됩니다.
key	클러스터 제어 링크의 제어 트래픽에 대해 인증 키를 설정합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스를 위한 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택에서 이 유닛의 우선 순위를 설정합니다.

enable gprs

RADIUS 어카운팅으로 GPRS를 활성화하려면 radius-accounting 매개변수 컨피그레이션 모드에서 **enable gprs** 명령을 사용합니다. 이 명령을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

enable gprs

no enable gprs

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Radius-accounting 매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 **inspect radius-accounting** 명령을 통해 액세스합니다. ASA는 보조 PDP 컨텍스트를 제대로 처리하기 위해 Accounting-Request Stop 메시지에서 3GPP VSA 26-10415를 확인합니다. 이 옵션은 기본적으로 비활성화되어 있습니다. 이 기능을 활성화하려면 GTP 라이센스가 필요합니다.

예

다음 예에서는 RADIUS 어카운팅으로 GPRS를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# enable gprs
```

관련 명령

명령	설명
inspect radius-accounting	RADIUS 어카운팅에 대한 검사를 설정합니다.
parameters	검사 정책 맵에 대한 매개변수를 설정합니다.

enable password

특별 권한 EXEC 모드를 위한 enable 비밀번호를 설정하려면 글로벌 컨피그레이션 모드에서 **enable password** 명령을 사용합니다. 15 이외의 레벨에서 비밀번호를 제거하려면 이 명령의 **no** 형식을 사용합니다.

enable password *password* **[level** *level***] [encrypted]**

no enable password level *level*

구문 설명

encrypted	(선택 사항) 비밀번호가 암호화된 형식임을 나타냅니다. 비밀번호는 암호화된 형식으로 컨피그레이션에 저장됩니다. 따라서 입력한 후에 원래의 비밀번호를 볼 수 없습니다. 어떤 이유로 다른 ASA에 비밀번호를 복사해야 하는데 원래의 비밀번호를 모른다면, 암호화된 비밀번호 및 이 키워드와 함께 **enable password** 명령을 입력하면 됩니다. 일반적으로 이 키워드는 **show running-config enable** 명령을 입력할 때만 나타납니다.
level *level*	(선택 사항) 0~15의 권한 레벨에 대해 비밀번호를 설정합니다.
password	비밀번호는 대/소문자를 구분하고 영숫자와 특수 문자로 구성된 3자~32자의 문자열입니다. 물음표와 공백을 제외한 어떤 문자도 비밀번호에 사용할 수 있습니다.

기본값

기본적으로 비밀번호는 비어 있습니다. 기본 레벨은 15입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

enable 레벨 15(기본 레벨)의 기본 비밀번호는 비어 있습니다. 빈 비밀번호로 재설정하려면 *password* 인수에 어떤 텍스트도 입력하지 않습니다. 레벨 15 비밀번호는 제거할 수 없습니다.

다중 컨텍스트 모드의 경우 시스템 컨피그레이션뿐 아니라 각 컨텍스트를 위해 enable 비밀번호를 만들 수 있습니다.

기본 설정인 15가 아닌 권한 레벨을 사용하려면 로컬 명령 권한 부여(**aaa authorization command** 명령 참조, **LOCAL** 키워드 지정)를 구성하고 **privilege** 명령을 사용하여 명령을 각기 다른 권한 레벨로 설정합니다. 로컬 명령 권한 부여를 구성하지 않을 경우, enable 레벨이 무시되며 설정된 레벨과 상관없이 레벨 15에 액세스할 수 있습니다. 현재 권한 레벨을 보려면 **show curpriv** 명령을 참조하십시오.

레벨 2 이상이면 특별 권한 EXEC 모드가 시작됩니다. 레벨 0과 1은 사용자 EXEC 모드가 시작됩니다.

예

다음 예에서는 enable 비밀번호를 Pa$$w0rd로 설정합니다.

```
ciscoasa(config)# enable password Pa$$w0rd
```

다음 예에서는 레벨 10을 위해 enable 비밀번호를 Pa$$w0rd10로 설정합니다.

```
ciscoasa(config)# enable password Pa$$w0rd10 level 10
```

다음 예에서는 다른 ASA에서 복사한 암호화된 비밀번호로 enable 비밀번호를 설정합니다.

```
ciscoasa(config)# enable password jMorNbK0514fadBh encrypted
```

관련 명령

명령	설명
aaa authorization command	명령 권한 부여를 구성합니다.
enable	특별 권한 EXEC 모드를 시작합니다.
privilege	로컬 명령 권한 부여를 위해 명령 권한 레벨을 설정합니다.
show curpriv	현재 로그인한 사용자 이름과 사용자 권한 레벨을 표시합니다.
show running-config enable	enable 비밀번호를 암호화된 형식으로 표시합니다.

encryption

AnyConnect IPsec 연결을 위해 IKEv2 SA(보안 연결)에 암호화 알고리즘을 지정하려면 ikev2 정책 컨피그레이션 모드에서 **encryption** 명령을 사용합니다. 이 명령을 제거하고 기본 설정을 사용하려면 이 명령의 **no** 형식을 사용합니다.

encryption [des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null]

no encryption [des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null]

구문 설명

des	ESP용 56비트 DES-CBC 암호화를 지정합니다.
3des	(기본) ESP용 Triple DES 암호화 알고리즘을 지정합니다.
aes	ESP용 128비트 키 암호화의 AES를 지정합니다.
aes-192	ESP용 192비트 키 암호화의 AES를 지정합니다.
aes-256	ESP용 256비트 키 암호화의 AES를 지정합니다.
aes-gcm	IKEv2 암호화용 AES-GCM 알고리즘을 지정합니다.
aes-gcm-192	IKEv2 암호화용 AES-GCM 알고리즘을 지정합니다.
aes-gcm-256	IKEv2 암호화용 AES-GCM 알고리즘을 지정합니다.
null	AES-GCM/GMAC가 암호화 알고리즘으로 구성된 경우 null 무결성 알고리즘을 선택합니다.

기본값

기본값은 3DES입니다.

사용 지침

IKEv2 SA는 1단계에서 사용되는 키로서 IKEv2 피어가 2단계에서 안전하게 통신할 수 있게 합니다. **crypto ikev2 policy** 명령을 입력한 다음 **encryption** 명령을 사용하여 SA 암호화 알고리즘을 설정할 수 있습니다.

OSPFv3 암호화가 인터페이스에서 활성화된 경우 IPsec 터널이 구성된 상태에서 인접성을 설정하면 지연이 발생합니다. **show crypto sockets**, **show ipsec policy**, **show ipsec sa** 명령을 사용하여 기본 IPsec 터널 상태를 확인하고 처리가 진행 중임을 확인합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ikev2-policy 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 추가됩니다.
9.0(1)	IKEv2 암호화에 사용할 AES-GCM 알고리즘을 추가했습니다.

예

다음 예에서는 ikev2-policy 컨피그레이션 모드를 시작하고 암호화를 AES-256으로 설정합니다.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# encryption aes-256
```

관련 명령

명령	설명
group	AnyConnect IPsec 연결을 위해 IKEv2 SA에서 Diffie-Hellman 그룹을 지정합니다.
integrity	AnyConnect IPsec 연결을 위해 IKEv2 SA에서 ESP 무결성 알고리즘을 지정합니다.
prf	AnyConnect IPsec 연결을 위해 IKEv2 SA에서 pseudo-random 기능을 지정합니다.
lifetime	AnyConnect IPsec 연결을 위해 IKEv2 SA의 SA 수명을 지정합니다.

endpoint

H.323 프로토콜 검사를 위해 HSI 그룹에 엔드포인트를 추가할 때 hsi 그룹 컨피그레이션 모드에서 **endpoint** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

구문 설명

if_name	엔드포인트가 ASA에 연결될 때 거치는 인터페이스.
ip_address	추가할 엔드포인트의 IP 주소. HSI 그룹당 최대 10개의 엔드포인트가 허용됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Hsi-group 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 H.323 검사 정책 맵에서 HSI 그룹에 엔드포인트를 추가하는 방법을 보여줍니다.

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

관련 명령

명령	설명
class-map	레이어 3/4 클래스 맵을 만듭니다.
hsi-group	HSI 그룹을 만듭니다.
hsi	HSI 그룹에 HSI를 추가합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

endpoint-mapper

DCERPC 검사를 위한 엔드포인트 매퍼 옵션을 구성하려면 매개변수 컨피그레이션 모드에서 **endpoint-mapper** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

구문 설명

epm-service-only	바인딩 과정에서 엔드포인트 매퍼 서비스를 적용하도록 지정합니다.
lookup-operation	엔드포인트 매퍼 서비스의 조회 작업을 활성화하도록 지정합니다.
timeout *value*	조회 작업의 핀홀 시간 초과를 지정합니다. 범위는 0:0:1부터 1193:0:0까지입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 DCERPC 정책 맵에서 엔드포인트 매퍼를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# endpoint-mapper epm-service-only
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

enforcenextupdate

NextUpdate CRL 필드를 처리하는 방법을 지정하려면 ca-crl 컨피그레이션 모드에서 **enforcenextupdate** 명령을 사용합니다. 경과된 또는 누락된 NextUpdate 필드를 허용하려면 이 명령의 **no** 형식을 사용합니다.

enforcenextupdate

no enforcenextupdate

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 설정은 enforced (on)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ca-crl 컨피그레이션	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

설정된 경우 이 명령에서 아직 경과하지 않은 NextUpdate 필드를 가지려면 CRL이 필요합니다. 사용하지 않으면 ASA에서는 CRL에서 누락되거나 경과된 NextUpdate 필드를 허용합니다.

예

다음 예에서는 crypto ca-crl 컨피그레이션 모드를 시작하고 CRL에서 trustpoint central에 대해 아직 만료되지 않은 NextUpdate 필드를 갖게 합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# enforcenextupdate
ciscoasa(ca-crl)#
```

관련 명령

명령	설명
cache-time	캐시 갱신 시간(분)을 지정합니다.
crl configure	ca-crl 컨피그레이션 모드를 시작합니다.
crypto ca trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.

enrollment-retrieval

등록된 사용자가 PKCS12 등록 파일을 검색할 수 있는 시간(단위: 시간)을 지정하려면 로컬 crypto ca-server 컨피그레이션 모드에서 **enrollment-retrieval** 명령을 사용합니다. 이 시간을 기본값인 24시간으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

enrollment-retrieval *timeout*

no enrollment-retrieval

구문 설명

timeout	사용자가 로컬 CA 등록 웹 페이지에서 발급된 인증서를 검색해야 하는 시간을 지정하며, 단위는 시간입니다. 유효한 시간 초과 값의 범위는 1시간부터 720시간까지입니다.

기본값

기본적으로 PKCS12 등록 파일이 저장되고 24시간 동안 검색 가능합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

PKCS12 등록 파일은 발급된 인증서와 키 쌍을 포함합니다. 이 파일은 로컬 CA 서버에 저장되며, **enrollment-retrieval** 명령으로 지정된 기간 동안 등록 웹 페이지에서 검색 가능합니다.

사용자가 등록 가능으로 표시되면 그 사용자는 **otp expiration** 명령으로 지정된 기간 동안 해당 비밀번호를 사용하여 등록할 수 있습니다. 사용자가 성공적으로 등록되면 PKCS12 파일이 생성되어 저장되고 그 사본이 등록 웹 페이지를 통해 반환됩니다. 사용자는 **enrollment-retrieval** 명령으로 지정된 명령 기간 동안 어떤 이유로든(예: 등록하는 중에 다운로드에 실패한 경우) 파일의 또 다른 사본을 반환할 수 있습니다.

참고 이 시간은 OTP 만료 기간과 상관없습니다.

예

다음 예에서는 인증서 발급 후 48시간 동안 로컬 CA 서버에서 PKCS12 등록 파일을 검색할 수 있도록 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# enrollment-retrieval 48
ciscoasa(config-ca-server)#
```

다음 예에서는 검색 시간을 기본값인 24시간으로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no enrollment-retrieval
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	ca-server 컨피그레이션 모드 명령에 대한 액세스를 제공합니다. 그러면 로컬 CA를 구성하고 관리할 수 있습니다.
OTP expiration	CA 등록 페이지를 위해 발급된 일회용 비밀번호의 유효 기간을 지정합니다. 단위는 시간입니다.
smtp from-address	CA 서버로부터 생성되는 모든 이메일에서 E-mail From: 필드에 사용할 이메일 주소를 지정합니다.
smtp subject	로컬 CA 서버로부터 생성되는 모든 이메일의 제목 필드에 표시할 텍스트를 지정합니다.
subject-name-default	CA 서버로부터 발급된 모든 사용자 인증서에서 사용자 이름과 함께 사용할 일반 주체-이름 DN을 지정합니다.

enrollment retry count

재시도 횟수를 지정하려면 crypto ca-trustpoint 컨피그레이션 모드에서 **enrollment retry count** 명령을 사용합니다. 재시도 횟수의 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

enrollment retry count *number*

no enrollment retry count

구문 설명

number	등록 요청 보내기 시도의 최대 횟수. 유효한 값은 0, 1회~100회입니다.

기본값

number 인수의 기본 설정은 0(무제한)입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

인증서를 요청한 다음 ASA는 CA로부터 인증서를 받을 때까지 기다립니다. ASA에서 구성된 재시도 기간 내에 인증서를 받지 못하면 또 다른 인증서 요청을 보냅니다. ASA는 응답을 받을 때까지 아니면 구성된 재시도 기간이 끝날 때까지 요청을 반복합니다. 이 명령은 선택 사항이며, 자동 등록이 구성된 경우에만 적용됩니다.

예

다음 예에서는 trustpoint central을 위해 crypto ca-trustpoint 컨피그레이션 모드를 시작하고 trustpoint central 내에서 등록 재시도 횟수를 20회로 구성합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry count 20
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.
default enrollment	등록 매개변수를 기본값으로 되돌립니다.
enrollment retry period	등록 요청을 재전송하기 전에 기다리는 시간(분)을 지정합니다.

enrollment retry period

재시도 기간을 지정하려면 crypto ca-trustpoint 컨피그레이션 모드에서 **enrollment retry period** 명령을 사용합니다. 재시도 기간의 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

enrollment retry period *minutes*

no enrollment retry period

구문 설명

minutes	등록 요청 보내기 시도의 간격(분). 유효한 값의 범위는 1분~60분입니다.

기본값

기본 설정은 1분입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

인증서를 요청한 다음 ASA는 CA로부터 인증서를 받을 때까지 기다립니다. ASA에서 지정된 재시도 기간 내에 인증서를 받지 못하면 또 다른 인증서 요청을 보냅니다. 이 명령은 선택 사항이며, 자동 등록이 구성된 경우에만 적용됩니다.

예

다음 예에서는 trustpoint central을 위해 crypto ca-trustpoint 컨피그레이션 모드를 시작하고 trustpoint central 내에서 등록 재시도 기간을 10분으로 구성합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry period 10
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.
default enrollment	모든 등록 매개변수를 시스템 기본값으로 되돌립니다.
enrollment retry count	등록 요청 재시도 횟수를 정의합니다.

enrollment terminal

이 신뢰 지점의 잘라내기/붙여넣기 등록을 지정하려면(수동 등록이라고도 함) crypto ca-trustpoint 컨피그레이션 모드에서 **enrollment terminal** 명령을 사용합니다. 명령의 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

enrollment terminal

no enrollment terminal

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 설정은 off입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 trustpoint central의 crypto ca-trustpoint 컨피그레이션 모드를 시작하고 trustpoint central에 대해 CA 등록의 잘라내기/붙여넣기(cut-and-paste) 방법을 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.
default enrollment	등록 매개변수를 기본값으로 되돌립니다.
enrollment retry count	등록 요청 보내기의 재시도 횟수를 지정합니다.
enrollment retry period	등록 요청을 재전송하기 전에 기다리는 시간(분)을 지정합니다.
enrollment url	이 신뢰 지점에 자동 등록(SCEP)을 지정하고 URL을 구성합니다.

enrollment url

이 신뢰 지점에 등록하고 등록 URL을 구성하기 위해 자동 등록(SCEP)을 지정하려면 crypto ca-trustpoint 컨피그레이션 모드에서 **enrollment url** 명령을 사용합니다. 명령의 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

enrollment url *url*

no enrollment url

구문 설명

url	자동 등록을 위한 URL 이름을 지정합니다. 최대 길이는 1,000자입니다(사실상 제한 없음).

기본값

기본 설정은 off입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 trustpoint central의 crypto ca-trustpoint 컨피그레이션 모드를 시작하고 URL https://enrollsite for trustpoint central에서 SCEP 등록을 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url https://enrollsite
ciscoasa(ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.
default enrollment	등록 매개변수를 기본값으로 되돌립니다.
enrollment retry count	등록 요청 보내기의 재시도 횟수를 지정합니다.
enrollment retry period	등록 요청을 재전송하기 전에 기다리는 시간(분)을 지정합니다.
enrollment terminal	이 신뢰 지점에 잘라내기/붙여넣기 등록을 지정합니다.

enrollment-retrieval

등록된 사용자가 PKCS12 등록 파일을 검색할 수 있는 시간(단위: 시간)을 지정하려면 로컬 ca-server 컨피그레이션 모드에서 **enrollment-retrieval** 명령을 사용합니다. 이 시간을 기본값인 24시간으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

enrollment-retrieval *timeout*

no enrollment-retrieval

구문 설명

timeout	사용자가 로컬 CA 등록 웹 페이지에서 발급된 인증서를 검색해야 하는 시간을 지정하며, 단위는 시간입니다. 유효한 시간 초과 값의 범위는 1시간부터 720시간까지입니다.

기본값

기본적으로 PKCS12 등록 파일이 저장되고 24시간 동안 검색 가능합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ca-server 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

PKCS12 등록 파일은 발급된 인증서와 키 쌍을 포함합니다. 이 파일은 로컬 CA 서버에 저장되며, **enrollment-retrieval** 명령으로 지정된 기간 동안 등록 웹 페이지에서 검색 가능합니다.

사용자가 등록 가능으로 표시되면 그 사용자는 **otp expiration** 명령으로 지정된 기간 동안 해당 비밀번호를 사용하여 등록할 수 있습니다. 사용자가 성공적으로 등록되면 PKCS12 파일이 생성되어 저장되고 그 사본이 등록 웹 페이지를 통해 반환됩니다. 사용자는 **enrollment-retrieval** 명령으로 지정된 기간 동안 어떤 이유로든(예: 등록하는 중에 다운로드에 실패한 경우) 파일의 또 다른 사본을 반환할 수 있습니다.

참고 이 시간은 OTP 만료 기간과 상관없습니다.

예

다음 예에서는 인증서 발급 후 48시간 동안 로컬 CA 서버에서 PKCS12 등록 파일을 검색할 수 있도록 지정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# enrollment-retrieval 48
ciscoasa(config-ca-server)#
```

다음 예에서는 검색 시간을 기본값인 24시간으로 재설정합니다.

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no enrollment-retrieval
ciscoasa(config-ca-server)#
```

관련 명령

명령	설명
crypto ca server	ca-server 컨피그레이션 모드 명령에 대한 액세스를 제공합니다. 그러면 로컬 CA를 구성하고 관리할 수 있습니다.
OTP expiration	CA 등록 페이지를 위해 발급된 일회용 비밀번호의 유효 기간을 지정합니다. 단위는 시간입니다.
smtp from-address	CA 서버로부터 생성되는 모든 이메일에서 E-mail From: 필드에 사용할 이메일 주소를 지정합니다.
smtp subject	로컬 CA 서버로부터 생성되는 모든 이메일의 제목 필드에 표시할 텍스트를 지정합니다.
subject-name-default	CA 서버로부터 발급된 모든 사용자 인증서에서 사용자 이름과 함께 사용할 일반 주체-이름 DN을 지정합니다.

eool

EOOL(End of Options List) 옵션이 IP 옵션 검사 패킷에 있을 경우 수행할 작업을 정의하려면 매개변수 컨피그레이션 모드에서 **eool** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

eool action {allow | clear}

no eool action {allow | clear}

구문 설명

allow	ASA에게 EOOL IP 옵션이 있는 패킷을 통과시키도록 지시합니다.
clear	ASA에게 패킷에서 EOOL IP 옵션을 삭제하고 패킷은 통과시키도록 지시합니다.

기본값

기본적으로 IP 옵션 검사에서는 EOOL IP 옵션이 있는 패킷을 삭제합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 IP 옵션 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.

단일 0바이트로만 이루어진 EOOL 옵션이 모든 옵션의 끝에 나타나 옵션 목록의 끝임을 나타냅니다. 이것은 헤더 길이에 따른 헤더의 끝과 일치하지 않을 수 있습니다.

예

다음 예에서는 정책 맵에서 IP 옵션 검사를 위한 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	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

eou allow

NAC Framework 컨피그레이션에서 클라이언트리스 인증을 활성화하려면 글로벌 컨피그레이션 모드에서 **eou allow** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

eou allow {audit | clientless | none}

no eou allow {audit | clientless | none}

구문 설명

audit	클라이언트리스 인증을 수행합니다.
clientless	클라이언트리스 인증을 수행합니다.
none	클라이언트리스 인증을 비활성화합니다.

기본값

기본 컨피그레이션은 **eou allow clientless** 컨피그레이션을 포함합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
8.0(2)	**audit** 옵션을 추가했습니다.
9.1(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

ASA에서는 다음 두 조건에 모두 해당될 때만 이 명령을 사용합니다.

- 그룹 정책이 NAC Framework NAC 정책 유형을 사용하도록 구성되었습니다.
- 세션의 호스트가 EAPoUDP 요청에 응답하지 않습니다.

예

다음 예에서는 클라이언트리스 인증을 수행하기 위해 ACS를 사용할 수 있게 합니다.

```
ciscoasa(config)# eou allow clientless
ciscoasa(config)#
```

다음 예에서는 ASA에서 감사 서버를 사용하여 클라이언트리스 인증을 수행하도록 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# eou allow audit
ciscoasa(config)#
```

다음 예에서는 감사 서버의 사용을 비활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# no eou allow clientless
ciscoasa(config)#
```

관련 명령

명령	설명
debug eou	NAC Framework 메시징의 디버깅을 위해 EAP over UDP 이벤트의 로깅을 활성화합니다.
eou clientless	NAC Framework 컨피그레이션에서 클라이언트리스 인증을 위해 ACS에 보낼 사용자 이름 및 비밀번호를 변경합니다.
show vpn-session.db	NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.

eou clientless

NAC Framework 컨피그레이션에서 클라이언트리스 인증을 위해 ACS에 보낼 사용자 이름 및 비밀번호를 변경하려면 글로벌 컨피그레이션 모드에서 **eou clientless** 명령을 사용합니다. 기본값을 사용하려면 이 명령의 **no** 형식을 사용합니다.

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

구문 설명

password	EAPoUDP 요청에 응답하지 않는 원격 호스트를 위해 클라이언트리스 인증을 받고자 ACS에 보낸 비밀번호를 변경하려면 입력합니다.
password	클라이언트리스 호스트를 지원하기 위해 ACS에 구성한 비밀번호를 입력합니다. 4자~32자의 ASCII 문자로 입력합니다.
username	EAPoUDP 요청에 응답하지 않는 원격 호스트를 위해 클라이언트리스 인증을 받고자 ACS에 보낸 사용자 이름을 변경하려면 입력합니다.
username	클라이언트리스 호스트를 지원하기 위해 ACS에 구성한 사용자 이름을 입력합니다. 1자~64자의 ASCII 문자로 입력합니다. 맨 앞과 맨 뒤에 공백, 파운드 기호(#), 물음표(?), 따옴표("), 별표(*), 꺾쇠괄호(<, >)가 올 수 없습니다.

기본값

사용자 이름 및 비밀번호 특성의 기본값은 둘 다 clientless입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
9.1(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

이 명령은 다음 조건에 모두 해당되는 경우에만 유효합니다.

- 클라이언트리스 인증을 지원하도록 ACS가 네트워크에 구성되어 있습니다.
- 클라이언트리스 인증이 ASA에서 활성화되어 있습니다.
- NAC가 ASA에 구성되어 있습니다.

이 명령은 Cisco NAC의 프레임워크 구현에만 적용됩니다.

예

다음 예에서는 클라이언트리스 인증을 위한 사용자 이름을 sherlock으로 변경합니다.

```
ciscoasa(config)# eou clientless username sherlock
ciscoasa(config)#
```

다음 예에서는 클라이언트리스 인증을 위한 사용자 이름을 기본값인 clientless로 변경합니다.

```
ciscoasa(config)# no eou clientless username
ciscoasa(config)#
```

다음 예에서는 클라이언트리스 인증을 위한 비밀번호를 secret으로 변경합니다.

```
ciscoasa(config)# eou clientless password secret
ciscoasa(config)#
```

다음 예에서는 클라이언트리스 인증을 위한 비밀번호를 기본값인 clientless로 변경합니다.

```
ciscoasa(config)# no eou clientless password
ciscoasa(config)#
```

관련 명령

명령	설명
eou allow	NAC Framework 컨피그레이션에서 클라이언트리스 인증을 활성화합니다.
debug eou	NAC Framework 메시징의 디버깅을 위해 EAP over UDP 이벤트의 로깅을 활성화합니다.
debug nac	NAC Framework 이벤트의 로깅을 활성화합니다.

eou initialize

하나 이상의 NAC Framework 세션에 지정된 리소스를 삭제하고 각 세션에 대해 새로운 무조건 포스처 검증을 시작하려면 특별 권한 EXEC 모드에서 **eou initialize** 명령을 사용합니다.

eou initialize {all | group *tunnel-group* **| ip** *ip-address***}**

구문 설명

all	이 ASA의 모든 NAC Framework 세션을 재검증합니다.
group	터널 그룹에 지정된 모든 NAC Framework 세션을 재검증합니다.
ip	단일 NAC Framework 세션을 재검증합니다.
ip-address	터널의 원격 피어 종단의 IP 주소.
tunnel-group	터널을 설정하기 위해 매개변수를 협상하는 데 사용되는 터널 그룹의 이름.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
9.1(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

원격 피어의 포스처에 변경이 있을 경우 또는 지정된 액세스 정책(즉 다운로드된 ACL)이 변경되고 세션에 지정된 리소스를 삭제해야 하는 경우 이 명령을 사용합니다. 이 명령을 입력하면 포스처 검증에 사용된 EAPoUDP 연결 및 액세스 정책이 삭제됩니다. NAC 기본 ACL은 재검증 기간에 유효하므로 세션 초기화 때문에 사용자 트래픽이 중단될 수 있습니다. 이 명령은 포스처 검증에서 제외되는 피어에는 영향을 주지 않습니다.

이 명령은 Cisco NAC의 프레임워크 구현에만 적용됩니다.

예

다음 예에서는 모든 NAC Framework 세션을 초기화합니다.

```
ciscoasa# eou initialize all
ciscoasa
```

다음 예에서는 tg1이라는 터널 그룹에 지정된 모든 NAC Framework 세션을 초기화합니다.

```
ciscoasa# eou initialize group tg1
ciscoasa
```

다음 예에서는 IP 주소가 209.165. 200.225인 엔드포인트에 대해 NAC Framework 세션을 초기화합니다.

```
ciscoasa# eou initialize 209.165.200.225
ciscoasa
```

관련 명령

명령	설명
eou revalidate	하나 이상의 NAC Framework 세션에 즉각적인 포스처 재검증을 시행합니다.
reval-period	NAC Framework 세션에서 성공한 포스처 검증의 간격을 지정합니다.
sq-period	NAC Framework 세션에서 성공한 각 포스처 검증과 그 다음번 호스트 포스처 변경 쿼리의 간격을 지정합니다.
show vpn-session.db	NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.
debug nac	NAC Framework 이벤트의 로깅을 활성화합니다.

eou max-retry

ASA에서 원격 컴퓨터에 EAP over UDP 메시지를 재전송하는 횟수를 변경하려면 글로벌 컨피그레이션 모드에서 **eou max-retry** 명령을 사용합니다. 기본값을 사용하려면 이 명령의 **no** 형식을 사용합니다.

eou max-retry *retries*

no eou max-retry

구문 설명

retries	재전송 타이머의 만료에 대한 응답인 연속 재시도의 횟수를 제한합니다. 1~3 범위의 값을 입력합니다.

기본값

기본값은 3입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
9.1(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

이 명령은 다음 조건에 모두 해당되는 경우에만 유효합니다.

- 클라이언트리스 인증을 지원하도록 ACS가 네트워크에 구성되어 있습니다.
- 클라이언트리스 인증이 ASA에서 활성화되어 있습니다.
- NAC가 ASA에 구성되어 있습니다.

이 명령은 Cisco NAC의 프레임워크 구현에만 적용됩니다.

예

다음 예에서는 EAP over UDP 재전송의 횟수를 1로 제한합니다.

```
ciscoasa(config)# eou max-retry 1
ciscoasa(config)#
```

다음 예에서는 EAP over UDP 재전송의 횟수를 기본값인 3으로 변경합니다.

```
ciscoasa(config)# no eou max-retry
ciscoasa(config)#
```

관련 명령

eou timeout	NAC Framework 컨피그레이션에서 원격 호스트에 EAP over UDP 메시지를 보낸 후 기다리는 시간(초)을 변경합니다.
sq-period	NAC Framework 세션에서 성공한 각 포스처 검증과 그 다음번 호스트 포스처 변경 쿼리의 간격을 지정합니다.
debug eou	NAC Framework 메시징의 디버깅을 위해 EAP over UDP 이벤트의 로깅을 활성화합니다.
debug nac	NAC Framework 이벤트의 로깅을 활성화합니다.
show vpn-session.db	NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.

eou port

NAC Framework 컨피그레이션에서 Cisco Trust Agent와의 EAP over UDP 통신에 사용할 포트 번호를 변경하려면 글로벌 컨피그레이션 모드에서 **eou port** 명령을 사용합니다. 기본값을 사용하려면 이 명령의 **no** 형식을 사용합니다.

eou port *port_number*

no eou port

구문 설명

port_number	EAP over UDP 통신용으로 지정할 클라이언트 엔드포인트의 포트 번호. 이 번호는 Cisco Trust Agent에 구성된 포트 번호입니다. 1024~65535 범위의 값을 입력합니다.

기본값

기본값은 21862입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
9.1(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

이 명령은 Cisco NAC의 프레임워크 구현에만 적용됩니다.

예

다음 예에서는 EAP over UDP 통신용 포트 번호를 62445로 변경합니다.

```
ciscoasa(config)# eou port 62445
ciscoasa(config)#
```

다음 예에서는 EAP over UDP 통신용 포트 번호를 기본값으로 변경합니다.

```
ciscoasa(config)# no eou port
ciscoasa(config)#
```

관련 명령

debug eou	NAC Framework 메시징의 디버깅을 위해 EAP over UDP 이벤트의 로깅을 활성화합니다.
eou initialize	하나 이상의 NAC Framework 세션에 지정된 리소스를 삭제하고 각 세션을 위해 새로운 무조건 포스처 검증을 시작합니다.
eou revalidate	하나 이상의 NAC Framework 세션에 즉각적인 포스처 재검증을 시행합니다.
show vpn-session.db	VLAN 매핑 및 NAC 결과를 비롯하여 VPN 세션에 대한 정보를 표시합니다.
show vpn-session_summary.db	IPsec, Cisco AnyConnect, NAC 세션의 수(VLAN 매핑 세션 데이터 포함)를 표시합니다.

eou revalidate

하나 이상의 NAC Framework 세션에서 즉각적인 포스처 재검증을 시행하려면 특별 권한 EXEC 모드에서 **eou revalidate** 명령을 사용합니다.

eou revalidate {all | group *tunnel-group* **| ip** *ip-address***}**

구문 설명

all	이 ASA의 모든 NAC Framework 세션을 재검증합니다.
group	터널 그룹에 지정된 모든 NAC Framework 세션을 재검증합니다.
ip	단일 NAC Framework 세션을 재검증합니다.
ip-address	터널의 원격 피어 종단의 IP 주소.
tunnel-group	터널을 설정하기 위해 매개변수를 협상하는 데 사용되는 터널 그룹의 이름.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
9.1(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

피어의 포스처 또는 지정된 액세스 정책(즉 다운로드된 ACL)이 변경되었으면 이 명령을 사용합니다. 이 명령은 새로운 무조건 포스처 검증을 시작합니다. 명령을 입력하기 전에 유효했던 포스처 검증 및 지정된 액세스 정책은 새 포스처 검증이 성공하거나 실패할 때까지 계속 유효합니다. 이 명령은 포스처 검증에서 제외되는 피어에는 영향을 주지 않습니다.

이 명령은 Cisco NAC의 프레임워크 구현에만 적용됩니다.

예

다음 예에서는 모든 NAC Framework 세션을 재검증합니다.

```
ciscoasa# eou revalidate all
ciscoasa
```

다음 예에서는 tg-1이라는 터널 그룹에 지정된 모든 NAC Framework 세션을 재검증합니다.

```
ciscoasa# eou revalidate group tg-1
ciscoasa
```

다음 예에서는 IP 주소가 209.165. 200.225인 엔드포인트에 대해 NAC Framework 세션을 재검증합니다.

```
ciscoasa# eou revalidate ip 209.165.200.225
ciscoasa
```

관련 명령

명령	설명
debug eou	NAC Framework 메시징의 디버깅을 위해 EAP over UDP 이벤트의 로깅을 활성화합니다.
eou initialize	하나 이상의 NAC Framework 세션에 지정된 리소스를 삭제하고 각 세션을 위해 새로운 무조건 포스처 검증을 시작합니다.
eou timeout	NAC Framework 컨피그레이션에서 원격 호스트에 EAP over UDP 메시지를 보낸 후 기다리는 시간(초)을 변경합니다.
reval-period	NAC Framework 세션에서 성공한 포스처 검증의 간격을 지정합니다.
sq-period	NAC Framework 세션에서 성공한 각 포스처 검증과 그 다음번 호스트 포스처 변경 쿼리의 간격을 지정합니다.

eou timeout

NAC Framework 컨피그레이션에서 원격 호스트에 EAP over UDP 메시지를 보낸 후에 기다리는 시간(초)을 변경하려면 글로벌 컨피그레이션 모드에서 **eou timeout** 명령을 사용합니다. 기본값을 사용하려면 이 명령의 **no** 형식을 사용합니다.

eou timeout {hold-period | retransmit} *seconds*

no eou timeout {hold-period | retransmit}

구문 설명

hold-period	EAPoUDP 재시도 횟수만큼 EAPoUDP 메시지를 보낸 후 기다리는 최대 시간. **eou initialize** 또는 **eou revalidate** 명령도 이 타이머를 초기화합니다. 이 타이머가 만료되면 ASA는 원격 호스트와의 새로운 EAP over UDP 연결을 시작합니다.
retransmit	EAPoUDP 메시지를 보낸 후 기다리는 최대 시간. 원격 호스트에서 응답하면 이 타이머가 초기화됩니다. **eou initialize** 또는 **eou revalidate** 명령도 이 타이머를 초기화합니다. 타이머가 만료되면 ASA는 원격 호스트에 EAPoUDP 메시지를 재전송합니다.
seconds	ASA에서 기다리는 시간(초). 60~86400 범위의 값을 hold-period 특성에 입력하거나 1~60 범위의 값을 retransmit 특성에 입력합니다.

기본값

hold-period 옵션의 기본값은 180입니다.

retransmit 옵션의 기본값은 3입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
9.1(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

이 명령은 Cisco NAC의 프레임워크 구현에만 적용됩니다.

예

다음 예에서는 새 EAP over UDP 연결을 시작하기 전에 기다리는 시간을 120초로 변경합니다.

```
ciscoasa(config)# eou timeout hold-period 120
ciscoasa(config)#
```

다음 예에서는 새 EAP over UDP 연결을 시작하기 전에 기다리는 시간을 기본값으로 변경합니다.

```
ciscoasa(config)# no eou timeout hold-period
ciscoasa(config)#
```

다음 예에서는 재전송 타이머를 6초로 변경합니다.

```
ciscoasa(config)# eou timeout retransmit 6
ciscoasa(config)#
```

다음 예에서는 재전송 타이머를 기본값으로 변경합니다.

```
ciscoasa(config)# no eou timeout retransmit
ciscoasa(config)#
```

관련 명령

명령	설명
debug eou	NAC Framework 메시징의 디버깅을 위해 EAP over UDP 이벤트의 로깅을 활성화합니다.
eou max-retry	ASA에서 원격 컴퓨터에 EAP over UDP 메시지를 재전송하는 횟수를 변경합니다.

erase

파일 시스템을 지우고 다시 포맷하려면 특별 권한 EXEC 모드에서 **erase** 명령을 사용합니다. 이 명령은 숨겨진 시스템 파일을 비롯한 모든 파일을 덮어쓰고 파일 시스템을 지운 다음 파일 시스템을 재설치합니다.

erase [disk0: | disk1: | flash:]

구문 설명

disk0:	(선택 사항) f를 지정하고 그 다음에 콜론을 표시합니다.
disk1:	(선택 사항) external, 컴팩트 플래시 메모리 카드, 콜론을 차례로 지정합니다.
flash:	(선택 사항) 내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다.

주의 플래시 메모리를 지우면 플래시 메모리에 저장된 라이센싱 정보도 삭제됩니다. 플래시 메모리를 지우기 전에 라이센싱 정보를 저장합니다.

ASA 5500 시리즈에서는 **flash** 키워드의 별칭이 **disk0:**입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

erase 명령은 OxFF 패턴을 사용하여 플래시 메모리의 모든 데이터를 지운 다음 디바이스에 빈 파일 시스템 할당 테이블을 재작성합니다.

(숨겨진 시스템 파일을 제외하고) 표시된 파일을 모두 삭제하려면 **erase** 명령 대신 **delete /recursive** 명령을 입력합니다.

참고 Cisco ASA 5500 시리즈에서 **erase** 명령은 0xFF 패턴으로 디스크의 모든 사용자 데이터를 삭제합니다. 이와 달리 **format** 명령은 파일 시스템 제어 구조를 재설정할 뿐입니다. 원시 디스크 읽기 툴을 사용한 경우에도 이 정보를 볼 수 있습니다.

예

다음 예에서는 파일 시스템을 지우고 다시 포맷합니다.

```
ciscoasa# erase flash:
```

관련 명령

명령	설명
delete	숨겨진 시스템 파일을 제외하고 표시된 모든 파일을 제거합니다.
format	(숨겨진 시스템 파일을 비롯하여) 모든 파일을 지우고 파일 시스템을 포맷합니다.

esp

IPsec Pass-Through 검사용 ESP 및 AH 터널의 매개변수를 지정하려면 매개변수 컨피그레이션 모드에서 **esp** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

{esp | ah} [per-client-max *num***] [timeout** *time***]**

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

구문 설명

esp	ESP 터널을 위한 매개변수를 지정합니다.
ah	AH 터널을 위한 매개변수를 지정합니다.
per-client-max *num*	하나의 클라이언트에서 가능한 터널의 최대 개수를 지정합니다.
timeout *time*	ESP 터널의 유휴 시간 초과를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 UDP 500 트래픽을 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# access-list test-udp-acl extended permit udp any any eq 500
ciscoasa(config)# class-map test-udp-class
ciscoasa(config-pmap-c)# match access-list test-udp-acl

ciscoasa(config)# policy-map type inspect ipsec-pass-thru ipsec-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
ciscoasa(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

ciscoasa(config)# policy-map test-udp-policy
ciscoasa(config-pmap)# class test-udp-class
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

established

설정된 연결을 기반으로 하는 포트에서 반환 연결을 허용하려면 글로벌 컨피그레이션 모드에서 **established** 명령을 사용합니다. **established** 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

구문 설명

est_protocol	설정된 연결 조회에 사용할 IP 프로토콜(UDP 또는 TCP)을 지정합니다.
dest_port	설정된 연결 조회에 사용할 목적지 포트를 지정합니다.
permitfrom	(선택 사항) 지정된 포트에서 시작하는 반환 프로토콜 연결을 허용합니다.
permitto	(선택 사항) 지정된 포트로 향하는 반환 프로토콜 연결을 허용합니다.
port [*-port*]	(선택 사항) 반환 연결의 (UDP 또는 TCP) 목적지 포트를 지정합니다.
protocol	(선택 사항) 반환 연결에서 사용한 IP 프로토콜(UDP 또는 TCP)입니다.
source_port	(선택 사항) 설정된 연결 조회에 사용할 소스 포트를 지정합니다.

기본값

기본 설정은 다음과 같습니다.

- *dest_port*—0(와일드카드)
- *source_port*—0(와일드카드)

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	키워드 **to**와 **from**을 CLI에서 제외했습니다. 그 대신 키워드 **permitto**와 **permitfrom**을 사용합니다.

사용 지침

established 명령을 사용하면 ASA를 지나는 아웃바운드 연결에 대해 반환 액세스를 허용할 수 있습니다. 이 명령은 어떤 네트워크에서 아웃바운드로 이루어지고 ASA의 보호를 받는 원래 연결과 외부 호스트상의 동일한 두 디바이스 사이에서 인바운드로 이루어지는 반환 연결을 지원합니다. **established** 명령을 사용하면 연결 조회에 쓰이는 목적지 포트를 지정할 수 있습니다. 이와 같이 추가된 덕분에 명령에 대한 더 강력한 제어가 가능해졌고 목적지 포트가 확인되지만 소스 포트는 미확인 상태인 프로토콜도 지원할 수 있습니다. **permitto** 및 **permitfrom** 키워드는 반환 인바운드 연결을 정의합니다.

주의 **established** 명령은 항상 **permitto** 및 **permitfrom** 키워드와 함께 지정하는 것이 좋습니다. 이 키워드 없이 **established** 명령을 사용하면 보안상 위험합니다. 외부 시스템과 연결되었을 때 이 시스템이 연결에 관련된 내부 호스트에 제한 없이 연결할 수 있기 때문입니다. 내부 시스템에 대한 공격에서 이를 악용할 수 있습니다.

예

다음 예에서는 **established** 명령을 제대로 사용하지 않으면 보안 위반이 일어날 수 있음을 보여줍니다.

이 예에서는 내부 시스템이 포트 4000에서 외부 호스트와 TCP 연결을 했을 때 이 외부 시스템이 임의의 프로토콜을 사용하여 임의의 포트로 돌아올 수 있음을 보여줍니다.

```
ciscoasa(config)# established tcp 4000 0
```

프로토콜에서 사용할 포트를 지정하지 않을 경우 소스 및 목적지 포트를 **0**으로 지정할 수 있습니다. 와일드카드 포트(0)는 필요할 때만 사용합니다.

```
ciscoasa(config)# established tcp 0 0
```

참고 **established** 명령이 올바르게 작동하려면 클라이언트가 **permitto** 키워드에 의해 지정된 포트에서 수신해야 합니다.

established 명령을 **nat 0** 명령과 함께 사용할 수 있습니다(**전역** 명령 없음).

참고 **established** 명령을 PAT와 함께 사용할 수는 없습니다.

ASA는 **established** 명령의 도움을 받아 XDMCP를 지원합니다.

주의 ASA를 통해 XWindows 시스템 애플리케이션을 사용하면 보안상 위험이 발생할 수 있습니다.

XDMCP는 기본적으로 켜져 있으나, 다음과 같이 **established** 명령을 입력하지 않으면 세션이 종료되지 않습니다.

```
ciscoasa(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

established 명령을 입력하면 내부 XDMCP 기반(UNIX 또는 ReflectionX) 호스트가 외부 XDMCP 기반 XWindows 서버에 액세스할 수 있게 됩니다. UDP/177 기반 XDMCP가 TCP 기반 XWindows 세션을 협상하며, 그 후속으로 TCP 반환 연결이 허용됩니다. 반환 트래픽의 소스 포트가 미확인 상태이므로 *source_port* 필드를 0(와일드카드)으로 지정합니다. *dest_port*는 6000 + *n*이 되어야 합니다. 여기서 *n*은 로컬 디스플레이 번호입니다. 이 값을 변경하려면 이 UNIX 명령을 사용합니다.

```
ciscoasa(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

established 명령이 필요한 이유는 (사용자 상호 작용에 따라) 많은 TCP 연결이 생성되고 이 연결의 소스 포트가 미확인 상태이기 때문입니다. 목적지 포트만 고정입니다. ASA는 투명하게 XDMCP 수정을 수행합니다. 어떤 컨피그레이션도 필요 없습니다. 다만 **established** 명령을 입력하여 TCP 세션을 수용해야 합니다.

다음 예에서는 프로토콜 A를 사용하는 두 호스트 간의 연결을 보여줍니다. 목적지 포트가 B, 소스 포트가 C입니다. ASA를 지나고 프로토콜 D(프로토콜 A와 다를 수 있음)를 사용하는 반환 연결을 허용하려면 소스 포트가 포트 F, 목적지 포트는 포트 E가 되어야 합니다.

```
ciscoasa(config)# established A B C permitto D E permitfrom D F
```

다음 예에서는 내부 호스트에서 시작하여 외부 호스트로 향하고 TCP 목적지 포트 6060과 임의의 소스 포트를 사용하는 연결을 보여줍니다. ASA는 TCP 목적지 포트 6061과 임의의 TCP 소스 포트를 지나는, 호스트 간의 반환 트래픽을 허용합니다.

```
ciscoasa(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

다음 예에서는 내부 호스트에서 시작하여 외부 호스트로 향하고 UDP 목적지 포트 6060과 임의의 소스 포트를 사용하는 연결을 보여줍니다. ASA는 TCP 목적지 포트 6061과 TCP 소스 포트 1024-65535를 지나는, 호스트 간의 반환 트래픽을 허용합니다.

```
ciscoasa(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

다음 예에서는 로컬 호스트가 포트 9999에서 외부 호스트에 대한 TCP 연결을 시작하는 방법을 보여줍니다. 이 예에서는 패킷이 포트 4242의 외부 호스트에서 포트 5454의 로컬 호스트로 돌아가는 것을 허용합니다.

```
ciscoasa(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

관련 명령

명령	설명
clear configure established	모든 established 명령을 제거합니다.
show running-config established	설정된 연결을 기반으로 하는 허용된 인바운드 연결을 표시합니다.

event crashinfo

ASA에서 충돌이 발생할 때 이벤트 관리자 애플릿을 트리거하려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **event crashinfo** 명령을 사용합니다. 충돌 이벤트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

event crashinfo

no event crashinfo

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

output 명령의 값과 상관없이 **action** 명령이 충돌 정보 파일로 전달됩니다. **show tech** 명령에 앞서 출력이 생성됩니다.

참고 일반적으로 충돌 시 ASA의 상태는 미확인입니다. 이 조건에서는 일부 CLI 명령을 실행하는 것이 안전하지 않을 수 있습니다.

예

다음 예에서는 ASA 충돌 시 어떤 애플릿을 트리거합니다.

```
ciscoasa(config-applet)# event crashinfo
```

관련 명령

명령	설명
event none	이벤트 관리자 애플릿을 수동으로 호출합니다.
event syslog id	이벤트 관리자 애플릿에 syslog 이벤트를 추가합니다.
event timer absolute time	절대 이벤트 타이머를 구성합니다.
event timer countdown time	countdown 타이머 이벤트를 구성합니다.
event timer watchdog time	watchdog 타이머 이벤트를 구성합니다.

event manager applet

이벤트를 작업 및 출력과 연결하는 이벤트 관리자 애플릿을 만들거나 수정하려면 글로벌 컨피그레이션 모드에서 이벤트 관리자 애플릿 명령을 사용합니다. 이벤트 관리자 애플릿을 제거하려면 이 명령의 **no** 형식을 사용합니다.

event manager applet *name*

no event manager applet *name*

구문 설명

name	이벤트 관리자 애플릿의 이름을 지정합니다. 이 이름은 최대 32자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

이벤트 관리자 애플릿 컨피그레이션 모드를 시작하려면 **event manager applet** 명령을 사용합니다.

예

다음 예에서는 이벤트 관리자 애플릿을 만들고 이벤트 관리자 애플릿 컨피그레이션 모드를 시작합니다.

```
ciscoasa(config)# event manager applet appletexample1
ciscoasa(config-applet)#
```

관련 명령

명령	설명
description	애플릿에 대해 설명합니다.
event manager run	이벤트 관리자 애플릿을 실행합니다.
show event manager	구성된 각 이벤트 관리자 애플릿에 대한 통계 정보를 표시합니다.
debug event manager	이벤트 관리자를 위한 디버깅 추적을 관리합니다.

event none

이벤트 관리자 애플릿을 수동으로 호출하려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **event none** 명령을 사용합니다. 수동 호출을 제거하려면 이 명령의 **no** 형식을 사용합니다.

event none

no event none

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

event none 명령으로 다른 어떤 이벤트도 구성할 수 있습니다.

예

다음 예에서는 이벤트 관리자 애플릿을 수동으로 호출합니다.

```
ciscoasa(config-applet)# event none
```

관련 명령

명령	설명
event crashinfo	ASA에서 충돌이 발생할 때 이벤트 관리자 애플릿을 트리거합니다.
event syslog id	이벤트 관리자 애플릿에 syslog 이벤트를 추가합니다.
event timer absolute time	절대 이벤트 타이머를 구성합니다.
event timer countdown time	countdown 타이머 이벤트를 구성합니다.
event timer watchdog time	watchdog 타이머 이벤트를 구성합니다.

event syslog id

이벤트 관리자 애플릿에 syslog 이벤트를 추가하려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **event syslog id** 명령을 사용합니다. 이벤트 관리자 애플릿에서 syslog 이벤트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

event syslog id *nnnnnn*[*-nnnnnn*] **[occurs** *n*] **[period** *seconds*]

no event syslog id *nnnnnn*[*-nnnnnn*] **[occurs** *n*] **[period** *seconds*]

구문 설명

nnnnnn	syslog 메시지 ID를 나타냅니다.
occurs *n*	애플릿이 호출되기 위해 syslog 메시지가 표시되는 횟수를 나타냅니다. 기본값은 1입니다. 유효한 값은 1~4294967295입니다.
period *seconds*	이벤트가 발생해야 하는 기간(초)을 나타냅니다. 그리고 애플릿이 호출되는 빈도를 구성된 기간에서 최대 1회로 제한합니다. 유효한 값은 0~604800입니다. 값이 0이면 어떤 기간도 정의되지 않은 것입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

애플릿을 트리거하는 단일 syslog 메시지 또는 syslog 메시지의 범위를 나타내는 데 **event syslog id** 명령을 사용합니다.

예

다음 예에서는 syslog 메시지 106201이 애플릿을 트리거하게 합니다.

```
ciscoasa(config-applet)# event syslog id 106201
```

관련 명령

명령	설명
event crashinfo	ASA에서 충돌이 발생할 때 이벤트 관리자 애플릿을 트리거합니다.
event none	이벤트 관리자 애플릿을 수동으로 호출합니다.
event timer absolute time	절대 이벤트 타이머를 구성합니다.
event timer countdown time	countdown 타이머 이벤트를 구성합니다.
event timer watchdog time	watchdog 타이머 이벤트를 구성합니다.

event timer

타이머 이벤트를 구성하려면 이벤트 관리자 애플릿 컨피그레이션 모드에서 **event timer** 명령을 사용합니다. 타이머 이벤트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

no event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

구문 설명

absolute time	이벤트가 매일 1회, 지정된 시간에 발생하고 자동으로 재시작하도록 지정합니다.
countdown time	이벤트가 한 번 발생하고, 제거되었다가 다시 추가되지 않는 한 재시작하지 않도록 지정합니다.
hh:mm:ss	시간대(time-of-day) 형식을 지정합니다. 시간 범위는 00:00:00(자정)부터 23:59:59까지입니다.
seconds	시간(초)을 지정합니다. 유효한 값은 0~604800입니다. 값이 0이면 타이머가 비활성화됩니다.
watchdog time	이벤트가 구성된 기간마다 1회 발생하고 자동으로 재시작하도록 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
이벤트 관리자 애플릿 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
9.2(1)	이 명령을 도입했습니다.

사용 지침

이벤트가 매일 1회, 지정된 시간에 발생하고 자동으로 재시작하게 하려면 **event timer absolute time** 명령을 사용합니다.

이벤트가 한 번만 발생하고 제거되었다가 다시 추가되지 않는 한 재시작하지 않게 하려면 **event timer countdown time** 명령을 사용합니다.

이벤트가 구성된 기간마다 1회 발생하고 자동으로 재시작하게 하려면 **event timer watchdog time** 명령을 사용합니다.

예

다음 예에서는 이벤트가 매일 1회, 지정된 시간에 발생하게 합니다.

```
ciscoasa(config-applet)# event timer absolute time 10:30:20
```

다음 예에서는 이벤트가 매일 1회, 지정된 시간에 발생하게 합니다.

```
ciscoasa(config-applet)# event timer countdown time 10:30:20
```

다음 예에서는 이벤트가 매일 1회 발생하고 자동으로 재시작하게 합니다.

```
ciscoasa(config-applet)# event timer watchdog time 30
```

관련 명령

명령	설명
event crashinfo	ASA에서 충돌이 발생할 때 이벤트 관리자 애플릿을 트리거합니다.
event none	이벤트 관리자 애플릿을 수동으로 호출합니다.
event syslog id	이벤트 관리자 애플릿에 syslog 이벤트를 추가합니다.
event timer countdown time	countdown 타이머 이벤트를 구성합니다.
event timer watchdog time	watchdog 타이머 이벤트를 구성합니다.

exceed-mss

데이터 길이가 3방향 핸드셰이크 과정에서 피어에 의해 설정된 TCP MSS(최대 세그먼트 크기)를 초과하는 패킷을 허용하거나 삭제하려면 tcp-map 컨피그레이션 모드에서 **exceed-mss** 명령을 사용합니다. 이 지정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

구문 설명

allow	MSS를 초과하는 패킷을 허용합니다. 기본 설정입니다.
drop	MSS를 초과하는 패킷을 삭제합니다.

기본값

패킷은 기본적으로 허용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tcp-map 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.2(4)/8.0(4)	기본 설정이 **drop**에서 **allow**로 변경되었습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용합니다. **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 모드를 시작하려면 **tcp-map** 명령을 사용합니다. 데이터 길이가 3방향 핸드셰이크 과정에서 피어에 의해 설정된 TCP MSS를 초과하는 TCP 패킷을 삭제하려면 tcp-map 컨피그레이션 모드에서 **exceed-mss** 명령을 사용합니다.

예

다음 예에서는 포트 21의 플로우가 MSS를 초과할 경우 이를 삭제합니다.

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# exceed-mss drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq ftp
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	정책을 구성합니다. 즉 트래픽 클래스와 하나 이상의 작업과 연결합니다.
set connection advanced-options	TCP 표준화를 비롯한 고급 연결 기능을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 컨피그레이션 모드에 대한 액세스를 허용합니다.

exempt-list

포스처 검증에서 제외되는 원격 컴퓨터 유형의 목록에 엔트리를 추가하려면 nac-policy-nac-framework 컨피그레이션 모드에서 **exempt-list** 명령을 사용합니다. 제외 목록에서 엔트리를 삭제하려면 이 명령의 **no** 형식을 사용하고 삭제할 엔트리의 운영 체제 및 ACL 이름을 지정합니다.

exempt-list os "*os-name***" [disable | filter** *acl-name* **[disable]]**

no exempt-list os "*os-name***" [disable | filter** *acl-name* **[disable]]**

구문 설명

acl-name	ASA 컨피그레이션에 있는 ACL의 이름. 지정될 때 **filter** 키워드 다음에 와야 합니다.
disable	다음과 같이 두 가지 기능 중 하나를 수행합니다. • "os-name" 다음에 입력할 경우 ASA는 제외를 무시하고 그 운영 체제를 실행하는 원격 호스트에 NAC 포스처 검증을 적용합니다. • *acl-name*의 다음에 입력하면 ASA는 그 운영 체제를 제외하지만 해당 트래픽에 ACL을 지정하지 않습니다.
filter	컴퓨터의 운영 체제가 *os name*과 일치할 경우 트래픽을 필터링하도록 ACL을 적용합니다. **filter**/*acl-name* 쌍은 선택 사항입니다.
os	포스처 검증에서 해당 운영 체제를 제외합니다.
os name	운영 체제 이름. 이름에 공백이 포함된 경우에만 따옴표가 필요합니다 (예: "Windows XP").

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Nac-policy-nac-framework 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.
8.0(2)	명령의 이름을 **vpn-nac-exempt**에서 **exempt-list**로 변경했습니다. 명령이 group-policy 컨피그레이션 모드에서 nac-policy-nac-framework 컨피그레이션 모드로 이동했습니다.

사용 지침

명령에서 운영 체제를 지정할 경우 이전에 예외 목록에 추가된 엔트리를 덮어쓰지 않습니다. 제외할 운영 체제 및 ACL 각각에 대해 한 번씩 명령을 입력합니다.

no exempt-list 명령은 NAC Framework 정책에서 모든 예외를 제거합니다. 이 명령의 **no** 형식을 실행할 때 엔트리를 지정하면 그 엔트리가 예외 목록에서 제거됩니다.

이 NAC 정책의 예외 목록에서 모든 엔트리를 제거하려면 추가 키워드 없이 이 명령의 **no** 형식을 사용합니다.

예

다음 예에서는 Windows XP를 실행하는 모든 호스트를 포스처 검증 제외 컴퓨터 목록에 추가합니다.

```
ciscoasa(config-group-policy)# exempt-list os "Windows XP"
ciscoasa(config-group-policy)
```

다음 예에서는 Windows XP를 실행하는 모든 호스트를 제외하고 이 호스트에서 보낸 트래픽에 acl-1이라는 ACL을 적용합니다.

```
ciscoasa(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

다음 예에서는 동일한 엔트리를 제외 목록에서 제거합니다.

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

다음 예에서는 제외 목록의 모든 엔트리를 제거합니다.

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list
ciscoasa(config-nac-policy-nac-framework)
```

관련 명령

명령	설명
debug nac	NAC Framework 이벤트의 로깅을 활성화합니다.
nac-policy	Cisco NAC 정책을 생성하여 액세스하고 그 유형을 지정합니다.
nac-settings	그룹 정책에 NAC 정책을 지정합니다.
show vpn-session.db	NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.
show vpn-session_summary.db	IPsec, Cisco AnyConnect, NAC 세션의 수를 표시합니다.

exit

현재 컨피그레이션 모드를 종료하거나 특별 권한 또는 사용자 EXEC 모드에서 로그아웃하려면 **exit** 명령을 사용합니다.

exit

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

글로벌 컨피그레이션 이상의 모드를 종료하는 데 키 시퀀스 **Ctrl+Z**를 사용할 수도 있습니다. 이 키 시퀀스는 특별 권한 또는 사용자 EXEC 모드를 지원하지 않습니다.

특별 권한 또는 사용자 EXEC 모드에서 **exit** 명령을 입력하면 ASA에서 로그아웃됩니다. 특별 권한 EXEC 모드에서 사용자 EXEC 모드로 돌아가려면 **disable** 명령을 사용합니다.

예

다음 예에서는 **exit** 명령을 사용하여 글로벌 컨피그레이션 모드를 종료한 다음 세션에서 로그아웃하는 방법을 보여줍니다.

```
ciscoasa(config)# exit
ciscoasa# exit

Logoff
```

다음 예에서는 **exit** 명령을 사용하여 글로벌 컨피그레이션 모드를 종료한 다음 **disable** 명령을 사용하여 특별 권한 EXEC 모드를 종료하는 방법을 보여줍니다.

```
ciscoasa(config)# exit
ciscoasa# disable
ciscoasa#
```

관련 명령

명령	설명
quit	구성 모드를 종료하거나 특별 권한 또는 사용자 EXEC 모드에서 로그아웃합니다.

expiry-time

재검증 없이 객체를 캐싱하는 것의 만료 시간을 구성하려면 캐시 컨피그레이션 모드에서 **expiry-time** 명령을 사용합니다. 컨피그레이션에서 만료 시간을 제거하고 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

expiry-time *time*

no expiry-time

구문 설명

time	ASA에서 재검증 없이 객체를 캐싱하는 시간(분)

기본값

기본값은 1분입니다.

명령 모드

다음 표는 명령을 입력하는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
캐시 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

이 만료 시간은 ASA에서 재검증 없이 객체를 캐싱하는 시간(분)입니다. 재검증에서는 내용을 다시 확인합니다.

예

다음 예에서는 만료 시간을 13분으로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)#expiry-time 13
ciscoasa(config-webvpn-cache)#
```

관련 명령

명령	설명
cache	webvpn 캐시 컨피그레이션 모드를 시작합니다.
cache-compressed	WebVPN 캐시 압축을 구성합니다.
disable	캐싱을 비활성화합니다.
lmfactor	last-modified 타임스탬프만 있는 캐싱 객체에 대해 유효성 재검사 정책을 설정합니다.
max-object-size	캐싱할 객체의 최대 크기를 정의합니다.
min-object-size	캐싱할 객체의 최소 크기를 정의합니다.

export

클라이언트에 내보낼 인증서를 지정하려면 ctl-provider 컨피그레이션 모드에서 **export** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

구문 설명

certificate *trustpoint_name* 클라이언트에 내보낼 인증서를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ctl-provider 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

클라이언트에 내보낼 인증서를 지정하려면 ctl-provider 컨피그레이션 모드에서 **export** 명령을 사용합니다. 신뢰 지점 이름은 **crypto ca trustpoint** 명령으로 정의합니다. 이 인증서는 CTL 클라이언트에 의해 생성된 CTL 파일에 추가됩니다.

예

다음 예에서는 CTL 제공자 인스턴스를 생성하는 방법을 보여줍니다.

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

관련 명령

명령	설명
ctl	CTL 클라이언트의 CTL 파일을 구문 분석하고 신뢰 지점을 설치합니다.
ctl-provider	ctl-provider 컨피그레이션 모드에서 CTL 제공자 인스턴스를 구성합니다.
client	CTL 제공자에 액세스할 수 있는 클라이언트와 클라이언트 인증을 위한 사용자 이름 및 비밀번호를 지정합니다.
service	CTL 제공자가 수신할 포트를 지정합니다.
tls-proxy	TLS 프록시 인스턴스를 정의하고 최대 세션을 설정합니다.

export webvpn AnyConnect-customization

AnyConnect client GUI를 사용자 지정하는 사용자 지정 객체를 내보내려면 특별 권한 EXEC 모드에서 **export webvpn AnyConnect-customization** 명령을 사용합니다.

export webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

구문 설명

name	사용자 지정 객체를 식별하는 이름. 최대 길이는 64자입니다.
type	사용자 지정의 유형: • binary—AnyConnect GUI를 대체하는 실행 파일. • transform—MSI를 사용자 지정하는 변환.
url	XML 사용자 지정 객체를 내보낼 원격 경로 및 파일 이름이며, *URL/filename*의 형식입니다(최대 255자).

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

AnyConnect 사용자 지정 객체는 캐시 메모리에 상주하는 XML 파일로서 AnyConnect 클라이언트 사용자를 위한 GUI 화면을 사용자 지정합니다. 사용자 지정 객체를 내보내면 XML 태그를 포함한 XML 파일이 지정된 URL에 생성됩니다.

*Template*라는 사용자 지정 객체에 의해 생성된 XML 파일은 빈 XML 태그를 포함하며, 새 사용자 지정 객체를 생성하기 위한 기반을 제공합니다. 이 객체는 변경하거나 캐시 메모리에서 삭제할 수 없으나 내보내거나 수정하거나 새 사용자 지정 객체로 다시 ASA에 가져오는 것은 가능합니다.

*Template*의 내용은 초기 DfltCustomization 객체 상태와 동일합니다.

AnyConnect GUI에서 사용하는 리소스 파일과 그 파일 이름의 전체 목록은 *AnyConnect VPN 클라이언트 관리자 설명서*를 참조하십시오.

예

다음 예에서는 AnyConnect GUI에 사용된 Cisco 로고를 내보냅니다.

```
ciscoasa# export webvpn AnyConnect-customization type resource company_logo.bmp
tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

관련 명령

명령	설명
import webvpn customization	XML 파일을 사용자 지정 객체로 캐시 메모리에 가져옵니다.
revert webvpn customization	캐시 메모리에서 사용자 지정 객체를 제거합니다.
show import webvpn customization	캐시 메모리에 상주하는 사용자 지정 객체에 대한 정보를 표시합니다.

export webvpn customization

클라이언트리스 SSL VPN 사용자에게 표시되는 화면을 사용자 지정하는 객체를 내보내려면 특별 권한 EXEC 모드에서 **export webvpn customization** 명령을 사용합니다.

export webvpn customization *name url*

구문 설명

name	사용자 지정 객체를 식별하는 이름. 최대 길이는 64자입니다.
url	XML 사용자 지정 객체를 내보낼 원격 경로 및 파일 이름이며, *URL/filename*의 형식입니다(최대 255자).

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

사용자 지정 객체는 캐시 메모리에 상주하는 XML 파일로서 클라이언트리스 SSL VPN 사용자에게 표시되는 화면을 사용자 지정합니다. 여기에는 로그인 및 로그아웃 화면, 포털 페이지, 사용 가능한 언어 등이 포함됩니다. 사용자 지정 객체를 내보내면 XML 태그를 포함한 XML 파일이 지정된 URL에 생성됩니다.

*Template*라는 사용자 지정 객체에 의해 생성된 XML 파일은 빈 XML 태그를 포함하며, 새 사용자 지정 객체를 생성하기 위한 기반을 제공합니다. 이 객체는 변경하거나 캐시 메모리에서 삭제할 수 없으나 내보내거나 수정하거나 새 사용자 지정 객체로 다시 ASA에 가져오는 것은 가능합니다.

*Template*의 내용은 초기 DfltCustomization 객체 상태와 동일합니다.

export webvpn customization 명령으로 사용자 지정 객체를 내보내고, XML 태그를 변경하며, **import webvpn customization** 명령으로 새 객체로 파일을 가져올 수 있습니다.

예

다음 예에서는 기본 사용자 지정 객체(DfltCustomization)를 내보내고 그 결과 XML 파일인 dflt_custom을 생성합니다.

```
ciscoasa# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

관련 명령

명령	설명
import webvpn customization	XML 파일을 사용자 지정 객체로 캐시 메모리에 가져옵니다.
revert webvpn customization	캐시 메모리에서 사용자 지정 객체를 제거합니다.
show import webvpn customization	캐시 메모리에 상주하는 사용자 지정 객체에 대한 정보를 표시합니다.

export webvpn plug-in

ASA의 플래시 디바이스에서 플러그인을 내보내려면 특별 권한 EXEC 모드에서 **export webvpn plug-in** 명령을 입력합니다.

import webvpn plug-in protocol *protocol URL*

구문 설명

protocol	• **rdp** Remote Desktop Protocol 플러그인을 사용하면 원격 사용자가 Microsoft Terminal Services를 실행하는 컴퓨터에 연결할 수 있습니다. Cisco는 이 플러그인을 변경 없이 재배포합니다. 원본을 제공하는 웹 사이트는 http://properjavardp.sourceforge.net/입니다. • **ssh,telnet** Secure Shell 플러그인을 사용하면 원격 사용자가 원격 컴퓨터와의 보안 채널을 설정하거나 텔넷을 통해 원격 컴퓨터에 연결할 수 있습니다. Cisco는 이 플러그인을 변경 없이 재배포합니다. 원본을 제공하는 웹 사이트는 http://javassh.org/입니다. **주의** **export webvpn plug-in protocol ssh,telnet** *URL* 명령은 SSH 플러그인과 텔넷 플러그인 *모두*내보냅니다. 이 명령을 SSH에 대해 한 번, 텔넷에 대해 한 번 입력해서는 *안 됩니다*. **ssh,telnet** 문자열을 입력할 때 공백을 삽입하지 *마십시오*. • **vnc** Virtual Network Computing 플러그인을 사용하면 원격 사용자가 원격 데스크톱 공유가 켜진 상태에서 모니터, 키보드, 마우스를 사용하여 컴퓨터를 보고 제어할 수 있습니다. Cisco는 이 플러그인을 변경 없이 재배포합니다. 원본을 제공하는 웹 사이트는 http://www.tightvnc.com/입니다.
URL	원격 디바이스의 경로

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

플러그인을 내보내더라도 플래시에서 제거되지 않습니다. 내보내면 지정된 URL에 그 플러그인의 사본이 생성됩니다.

예

다음 명령은 RDP 플러그인을 내보냅니다.

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

관련 명령

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

export webvpn mst-translation

AnyConnect 설치 프로그램을 변환하는 MST(Microsoft transform)를 내보내려면 특별 권한 EXEC 모드에서 **export webvpn mst-translation** 명령을 사용합니다.

export webvpn mst-translation *component* **language** *language URL*

구문 설명

component	이 MST를 적용할 구성 요소. AnyConnect만 선택 가능합니다.
language	내보낸 MST의 언어 코드. 브라우저에서 요구하는 것과 동일한 형식의 코드를 사용합니다.
URL	변환을 내보낼 원격 경로 및 파일 이름이며, *URL/filename*의 형식입니다(최대 255자).

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

AnyConnect 클라이언트 GUI처럼 클라이언트 설치 프로그램에서 표시하는 메시지를 변환할 수 있습니다. ASA는 설치 프로그램에서 표시하는 메시지를 변환하는 데 변환을 사용합니다. 이 변환은 설치를 변경하지만 원래의 보안 서명된 MSI를 그대로 유지합니다. 이 변환은 설치 프로그램의 화면만 변환하며 클라이언트 GUI 화면은 변환하지 않습니다.

언어별로 변환이 있습니다. Orca와 같은 변환 편집기로 변환을 편집하고 메시지 문자열을 변경할 수 있습니다. 그런 다음 ASA에 변환을 가져옵니다. 사용자가 클라이언트를 다운로드할 때 클라이언트는 컴퓨터의 기본 언어(운영 체제의 설치 과정에서 지정된 로캘)를 감지하고 해당 변환을 적용합니다.

현재 30개 언어의 변환을 제공합니다. 이 변환은 cisco.com의 AnyConnect 클라이언트 소프트웨어 다운로드 페이지에서 다음 .zip 파일의 형태로 제공됩니다.

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

이 파일에서 <VERSION>은 AnyConnect 릴리스의 버전(예: 2.2.103)입니다.

예

다음 예에서는 영어 변환을 AnyConnect_Installer_English로 내보냅니다.

```
ciscoasa# export webvpn mst-translation AnyConnect language es
tftp://209.165.200.225/AnyConnect_Installer_English
```

관련 명령

명령	설명
import webvpn customization	XML 파일을 사용자 지정 객체로 캐시 메모리에 가져옵니다.
revert webvpn customization	캐시 메모리에서 사용자 지정 객체를 제거합니다.
show import webvpn customization	캐시 메모리에 상주하는 사용자 지정 객체에 대한 정보를 표시합니다.

export webvpn translation-table

SSL VPN 연결을 설정하는 원격 사용자에게 표시되는 용어를 변환하는 데 쓰이는 변환 테이블을 내보내려면 특별 권한 EXEC 모드에서 **export webvpn translation-table** 명령을 사용합니다.

export webvpn translation-table *translation_domain* **{language** *language* **| template}** *url*

구문 설명

language	이전에 가져온 변환 테이블의 이름을 지정합니다. 브라우저 언어 옵션에서 표시하는 것과 동일한 방식으로 값을 입력합니다.
translation_domain	기능 영역 및 해당 메시지. 표 14-1에서는 사용 가능한 변환 도메인을 나열합니다.
url	객체의 URL을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ASA에서는 브라우저 기반의 클라이언트리스 SSL VPN 연결을 시작하는 사용자에게 표시되는 포털과 화면 그리고 AnyConnect VPN Client 사용자에게 표시되는 사용자 인터페이스를 위한 언어 변환을 제공합니다.

원격 사용자에게 표시되는 각 기능 영역과 그 메시지는 저마다 변환 도메인이 있으며, 이는 *translation_domain* 인수에 의해 지정됩니다. 표 14-1에서는 변환 도메인 및 변환된 기능 영역을 보여줍니다.

표 14-1 변환 도메인 및 해당 기능 영역

변환 도메인	변환된 기능 영역
AnyConnect	Cisco AnyConnect VPN Client의 사용자 인터페이스에 표시되는 메시지
banners	VPN 액세스가 거부될 때 원격 사용자 및 메시지에 표시되는 배너
CSD	CSD(Cisco Secure Desktop)용 메시지
customization	로그인 및 로그아웃 페이지, 포털 페이지, 사용자 지정 가능한 모든 메시지에 표시되는 메시지

변환 도메인	변환된 기능 영역
plugin-ica	Citrix 플러그인용 메시지
plugin-rdp	Remote Desktop Protocol 플러그인용 메시지
plugin-telnet,ssh	텔넷 및 SSH 플러그인용 메시지
plugin-vnc	VNC 플러그인용 메시지
PortForwarder	포트 전달 사용자에게 표시되는 메시지
url-list	사용자가 포털 페이지에서 URL 북마크를 위해 지정하는 텍스트
webvpn	사용자 지정할 수 없는 모든 레이어 7, AAA, 포털 메시지

변환 템플릿은 변환 테이블과 동일한 형식이지만 모든 변환이 비어 있는 XML 파일입니다. ASA용 소프트웨어 이미지 패키지는 표준 기능에 속한 도메인별 템플릿을 포함하고 있습니다. 플러그인용 템플릿은 플러그인과 함께 제공되며, 각자의 변환 도메인을 정의합니다. 클라이언트리스 사용자를 위한 로그인 및 로그아웃 페이지, 포털 페이지, URL 북마크를 사용자 지정할 수 있으므로 ASA는 사용자 지정 및 URL 목록 변환 도메인 템플릿을 동적으로 생성합니다. 그러면 이 템플릿은 기능 영역의 변경 사항을 자동으로 반영합니다.

이미 가져온 변환 테이블을 내보내면 URL 위치에 그 테이블의 XML 파일이 생성됩니다. **show import webvpn translation-table** 명령을 사용하면 사용 가능한 템플릿 및 이미 가져온 테이블의 목록을 표시할 수 있습니다.

export webvpn translation-table 명령으로 템플릿 또는 변환 테이블을 다운로드하고, 메시지를 변경하며, **import webvpn translation-table** 명령으로 변환 테이블을 가져옵니다.

예

다음 예에서는 변환 도메인인 *customization*을 위한 템플릿을 내보냅니다. 이는 클라이언트리스 SSL VPN 연결을 설정하는 원격 사용자를 위해 로그인 및 로그아웃 페이지, 포털 페이지, 사용자 지정 가능한 모든 메시지를 변환하는 데 사용됩니다. ASA는 *Sales*라는 이름으로 XML 파일을 만듭니다.

```
ciscoasa# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

다음 예에서는 이미 가져온 중국어용 변환 테이블인 *zh*를 내보냅니다. 이 약어는 Microsoft Internet Explorer 브라우저의 인터넷 옵션에서 중국어에 대해 지정된 약어와 같습니다. ASA는 *Chinese*라는 이름으로 XML 파일을 만듭니다.

```
ciscoasa# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

관련 명령

명령	설명
import webvpn translation-table	변환 테이블을 가져옵니다.
revert	캐시 메모리에서 변환 테이블을 제거합니다.
show import webvpn translation-table	가져온 변환 테이블에 대한 정보를 표시합니다.

export webvpn url-list

원격 위치에 URL 목록을 내보내려면 특별 권한 EXEC 모드에서 **export webvpn url-list** 명령을 사용합니다.

export webvpn url-list *name url*

구문 설명

name	URL 목록을 식별하는 이름. 최대 길이는 64자입니다.
url	URL 목록 소스의 원격 경로. 최대 길이는 255자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

기본적으로 WebVPN에는 URL 목록이 없습니다.

Template이라는 객체를 **export webvpn url-list** 명령과 함께 다운로드할 수 있습니다. Template 객체는 변경하거나 삭제할 수 없습니다. Template 객체의 내용은 편집하고 사용자 지정 URL 목록으로 저장할 수 있으며, **import webvpn url-list** 명령으로 가져와 사용자 지정 URL 목록으로 추가할 수 있습니다.

이미 가져온 URL 목록을 내보내면 URL 위치에 그 목록의 XML 파일이 생성됩니다. **show import webvpn url-list** 명령을 사용하면 사용 가능한 템플릿 및 이미 가져온 테이블의 목록을 볼 수 있습니다.

예

다음 예에서는 *servers*라는 URL 목록을 내보냅니다.

```
ciscoasa# export webvpn url-list servers2 tftp://209.165.200.225
ciscoasa#
```

관련 명령

명령	설명
import webvpn url-list	URL 목록을 가져옵니다.
revert webvpn url-list	캐시 메모리에서 URL 목록을 제거합니다.
show import webvpn url-list	가져온 URL 목록에 대한 정보를 표시합니다.

export webvpn webcontent

이미 가져왔고 원격 클라이언트리스 SSL VPN 사용자에게 표시되는 플래시 메모리의 콘텐츠를 내보내려면 특별 권한 EXEC 모드에서 **export webvpn webcontent** 명령을 사용합니다.

export webvpn webcontent *source url destination url*

구문 설명

destination url	내보낼 URL. 최대 길이는 255자입니다.
source url	해당 콘텐츠가 있는 ASA 플래시 메모리 내 URL. 최대 길이는 64자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

webcontent 옵션으로 내보낸 콘텐츠는 원격 클라이언트리스 사용자에게 표시되는 콘텐츠입니다. 여기에는 이미 가져와 클라이언트리스 포털에서 표시하는 도움말 콘텐츠 및 사용자 지정 객체에서 사용하는 로고가 포함됩니다.

물음표(**?**)를 **export webvpn webcontent** 명령의 다음에 입력하여 내보낼 수 있는 콘텐츠의 목록을 표시할 수 있습니다. 예:

```
ciscoasa# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

예

다음 예에서는 TFTP를 사용하여 *logo.gif* 파일을 *logo_copy.gif*라는 파일 이름으로 209.165.200.225에 내보냅니다.

```
ciscoasa# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

관련 명령

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

15 장

failover ~ fallback 명령

failover

장애 조치를 활성화하려면 글로벌 컨피그레이션 모드에서 **failover** 명령을 사용합니다. 장애 조치를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

failover

no failover

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

장애 조치가 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령은 컨피그레이션에서 장애 조치를 활성화하거나 비활성화하는 기능으로 한정되었습니다(**failover active** 참조).

사용 지침

장애 조치를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

주의 장애 조치 키로 통신 보안을 설정하지 않는 한 장애 조치 및 상태 기반 장애 조치(Stateful Failover) 링크를 통해 전송되는 모든 정보는 일반 텍스트로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(Pre-Shared key)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 장애 조치 키로 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

ASA 5505 디바이스는 무상태 장애 조치(Stateless Failover)만 허용하며, Easy VPN 하드웨어 클라이언트의 기능을 하지 않을 경우에만 가능합니다.

예

다음 예에서는 장애 조치를 비활성화합니다.

```
ciscoasa(config)# no failover
ciscoasa(config)#
```

관련 명령

명령	설명
clear configure failover	실행 중인 컨피그레이션에서 **failover** 명령을 지우고 장애 조치의 기본 값을 복원합니다.
failover active	스탠바이 유닛을 액티브 상태로 전환합니다.
show failover	유닛의 장애 조치 상태에 대한 정보를 표시합니다.
show running-config failover	실행 중인 컨피그레이션의 **failover** 명령을 표시합니다.

failover active

스탠바이 ASA 또는 장애 조치 그룹을 액티브 상태로 전환하려면 특별 권한 EXEC 모드에서 **failover active** 명령을 사용합니다. 액티브 ASA 또는 장애 조치 그룹을 스탠바이 상태로 전환하려면 이 명령의 **no** 형식을 사용합니다.

failover active [group *group_id***]**

no failover active [group *group_id***]**

구문 설명

group *group_id*	(선택 사항) 액티브 상태로 만들 장애 조치 그룹을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	장애 조치 그룹을 포함하도록 이 명령을 수정했습니다.

사용 지침

스탠바이 유닛에서 장애 조치 스위치를 시작하려면 **failover active** 명령을 사용합니다. 또는 액티브 유닛에서 **no failover active** 명령을 사용하여 장애 조치 스위치를 시작합니다. 이 기능을 사용하여 오류 상태의 유닛을 정상화하거나 유지 보수를 위해 액티브 유닛을 오프라인화할 수 있습니다. 상태 기반 장애 조치를 사용하지 않을 경우 모든 액티브 연결이 끊기며, 장애 조치가 이루어진 후 클라이언트에서 다시 연결을 설정해야 합니다.

장애 조치 그룹에 대한 전환은 액티브/액티브 장애 조치에서만 가능합니다. 액티브/액티브 장애 조치 유닛에서 장애 조치 그룹을 지정하지 않고 **failover active** 명령을 입력할 경우 이 유닛의 모든 그룹이 액티브 상태가 됩니다.

예

다음 예에서는 스탠바이 group 1을 액티브 상태로 전환합니다.

```
ciscoasa# failover active group 1
```

관련 명령

명령	설명
failover reset	오류 상태의 ASA를 스탠바이 상태로 만듭니다.

failover exec

장애 조치 쌍의 특정 유닛에서 명령을 실행하려면 특별 권한 EXEC 또는 글로벌 컨피그레이션 모드에서 **failover exec** 명령을 사용합니다.

failover exec {active | standby | mate} *cmd_string*

구문 설명

active	장애 조치 쌍의 액티브 유닛 또는 장애 조치 그룹에서 명령이 실행되도록 지정합니다. 액티브 유닛 또는 장애 조치 그룹에서 입력한 컨피그레이션 명령은 스탠바이 유닛 또는 장애 조치 그룹에 복제됩니다.
cmd_string	실행할 명령. **Show**, 컨피그레이션, EXEC 명령이 지원됩니다.
mate	장애 조치 피어에서 명령이 실행되도록 지정합니다.
standby	장애 조치 쌍의 스탠바이 유닛 또는 장애 조치 그룹에서 명령이 실행되도록 지정합니다. 스탠바이 유닛 또는 장애 조치 그룹에서 입력한 컨피그레이션 명령은 액티브 유닛 또는 장애 조치 그룹에 복제되지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

장애 조치 쌍의 특정 유닛에 명령을 보내는 데 **failover exec** 명령을 사용할 수 있습니다.

컨피그레이션 명령은 액티브 유닛 또는 컨텍스트에서 스탠바이 유닛이나 컨텍스트로 복제되므로, 어떤 유닛에 로그인해도 **failover exec** 명령을 사용하여 올바른 유닛에 컨피그레이션 명령을 입력할 수 있습니다. 예를 들어, 스탠바이 유닛에 로그인한 경우 **failover exec active** 명령을 사용하여 컨피그레이션 변경 사항을 액티브 유닛에 보낼 수 있습니다. 그런 다음 이러한 변경 사항은 스탠바이 유닛에 복제됩니다. **failover exec** 명령을 사용하여 컨피그레이션 명령을 스탠바이 유닛이나 컨텍스트에 보내지 마십시오. 이러한 컨피그레이션 명령은 액티브 유닛에 복제되지 않으며 두 개의 컨피그레이션이 더 이상 동기화되지 않습니다.

configuration, exec, **show** 명령의 결과가 현재 터미널 세션에 표시되므로, **failover exec** 명령을 사용하여 **show** 명령을 피어 유닛에 제공하고 현재 터미널에서 결과를 볼 수 있습니다.

피어 유닛에 명령을 실행하여 로컬 유닛에 명령을 실행하려면 충분한 권한이 있어야 합니다.

명령 모드

failover exec 명령은 터미널 세션의 명령 모드와 별개인 명령 모드 상태를 유지합니다. 기본적으로 **failover exec** 명령 모드는 지정된 디바이스에 대한 글로벌 컨피그레이션 모드입니다. **failover exec** 명령을 사용하면 적절한 명령(예: **interface** 명령)을 전송하여 명령 모드를 변경할 수 있습니다.

지정된 디바이스에 대해 **failover exec** 명령을 변경하더라도 그 디바이스에 액세스하기 위해 사용 중인 세션의 명령 모드는 바뀌지 않습니다. 이를테면 장애 조치 쌍의 액티브 유닛에 로그인하고 글로벌 컨피그레이션 모드에서 다음 명령을 실행할 경우, 계속 글로벌 컨피그레이션 모드에 있지만 **failover exec** 명령을 사용하여 보낸 모든 명령은 인터페이스 컨피그레이션 모드에서 실행됩니다.

```
ciscoasa(config)# failover exec interface GigabitEthernet0/1
ciscoasa(config)#
```

디바이스에 대한 현재 세션의 명령 모드를 변경할 경우 **failover exec** 명령에서 사용되는 명령 모드에 영향을 미치지 않습니다. 예를 들어, 액티브 유닛에서 인터페이스 컨피그레이션 모드를 사용 중이고 **failover exec** 명령 모드를 변경하지 않은 경우 다음 명령이 글로벌 컨피그레이션 모드에서 실행됩니다.

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

failover exec 명령을 실행하여 명령이 전송되는 지정된 디바이스에 명령 모드를 표시하려면 **show failover exec** 명령을 사용합니다.

보안 문제

failover exec 명령에서는 장애 조치 링크를 사용하여 명령을 전송하고 피어 유닛에서 명령 실행 결과를 수신합니다. 도청 또는 MITM(man-in-the-middle) 공격을 막기 위해 장애 조치 링크를 암호화하려면 **failover key** 명령을 사용해야 합니다.

제한 사항

- 무중단 업그레이드 절차를 사용하여 유닛 하나를 업그레이드하고 다른 유닛은 업그레이드하지 않을 경우, 두 유닛에서는 명령을 가동하는 데 필요한 **failover exec** 명령을 지원하는 소프트웨어를 실행해야 합니다.
- *cmd_string* 인수에서 명령 완료 및 컨텍스트 도움말이 제공되지 않습니다.
- 다중 컨텍스트 모드의 경우, 피어 유닛에 있는 피어 컨텍스트에 명령을 전송하는 것만 가능합니다. 다른 컨텍스트에 명령을 전송하려면 먼저 로그인한 유닛에서 그 컨텍스트로 변경해야 합니다.
- 다음 명령은 **failover exec** 명령과 함께 사용할 수 없습니다.
  - **changeto**
  - **debug (undebug)**
- 스탠바이 유닛에 오류가 발생한 상태이고 오류의 원인이 서비스 카드 오류인 경우 **failover exec** 명령을 계속 수신할 수 있습니다. 그렇지 않을 경우에는 원격 명령을 실행할 수 없습니다.
- **failover exec** 명령을 사용하여 장애 조치 피어의 특권 EXEC 모드를 글로벌 컨피그레이션 모드로 전환할 수 없습니다. 이를테면 현재 유닛이 특별 권한 EXEC 모드에 있는 상태에서 **failover exec mate configure terminal** 명령을 입력할 경우, **show failover exec mate** 명령 출력에서는 failover exec 세션이 글로벌 컨피그레이션 모드에 있다고 표시합니다. 그러나 현재 유닛에서 글로벌 컨피그레이션 모드를 시작하지 않는 한 **failover exec**을 사용하여 피어 유닛에 컨피그레이션 명령을 입력할 경우 오류가 발생합니다.
- 재귀적 **failover exec** 명령(예: **failover exec mate failover exec mate** *명령)은 입력할 수 없습니다.*
- 사용자 입력 또는 확인이 필요한 명령에는 **/nonconfirm** 옵션을 사용해야 합니다.

예

다음 예에서는 액티브 유닛에서 장애 조치 정보를 표시하기 위해 **failover exec** 명령을 사용하는 방법을 보여줍니다. 명령이 실행되는 유닛이 액티브 유닛이므로 이 명령은 로컬에서 실행됩니다.

```
ciscoasa(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
ciscoasa(config)#
```

다음 예에서는 피어 유닛의 장애 조치 상태를 표시하기 위해 **failover exec** 명령을 사용합니다. 이 명령은 액티브 유닛인 기본 유닛에서 실행되며, 표시되는 정보는 보조 스탠바이 유닛에서 제공합니다.

```
ciscoasa(config)# failover exec mate show failover

Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
```

```
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

다음 예에서는 장애 조치 피어의 장애 조치 컨피그레이션을 표시하기 위해 **failover exec** 명령을 사용합니다. 이 명령은 액티브 유닛인 기본 유닛에서 실행되며, 표시되는 정보는 보조 스탠바이 유닛에서 제공합니다.

```
ciscoasa(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

다음 예에서는 스탠바이 유닛에서 액티브 유닛에 컨텍스트를 생성하기 위해 **failover exec** 명령을 사용합니다. 이 명령은 액티브 유닛에서 다시 스탠바이 유닛으로 복제됩니다. 2개의 "Creating context…" 메시지에 유의하십시오. 하나는 컨텍스트가 생성될 때 피어 유닛의 **failover exec** 명령 출력에서 나온 것이고, 다른 하나는 복제된 명령이 로컬에 컨텍스트를 새성할 때 로컬 유닛에서 나온 것입니다.

```
ciscoasa(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

ciscoasa(config)# failover exec active context text
```

```
Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

ciscoasa(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

다음 예에서는 스탠바이 상태에 있는 장애 조치 피어에 컨피그레이션 명령을 보내기 위해 **failover exec** 명령을 사용할 때 반환되는 경고를 보여줍니다.

```
ciscoasa# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

       **** WARNING ****
       Configuration Replication is NOT performed from Standby unit to Active unit.
       Configurations are no longer synchronized.
ciscoasa(config)#
```

다음 예에서는 스탠바이 유닛에 **show interface** 명령을 보내기 위해 **failover exec** 명령을 사용합니다.

```
ciscoasa(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
```

```
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

다음 예에서는 피어 유닛에 잘못된 명령을 보낼 때 반환되는 오류 메시지를 보여줍니다.

```
ciscoasa# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

다음 예에서는 장애 조치가 비활성화된 상태에서 **failover exec** 명령을 사용할 경우 반환되는 오류 메시지를 보여줍니다.

```
ciscoasa(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

관련 명령

명령	설명
debug fover	장애 조치 관련 디버깅 메시지를 표시합니다.
debug xml	**failover exec** 명령에서 사용하는 XML 파서를 위한 디버깅 메시지를 표시합니다.
show failover exec	**failover exec** 명령 모드를 표시합니다.

failover group

액티브/액티브 장애 조치 그룹을 구성하려면 글로벌 컨피그레이션 모드에서 **failover group** 명령을 사용합니다. 장애 조치 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

failover group *num*

no failover group *num*

구문 설명

num	장애 조치 그룹 번호. 유효한 값은 1 또는 2입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

최대 2개의 장애 조치 그룹을 정의할 수 있습니다. **failover group** 명령은 다중 컨텍스트 모드로 구성된 디바이스의 시스템 컨텍스트에만 추가할 수 있습니다. 장애 조치가 비활성 상태일 때만 장애 조치 그룹을 만들고 제거할 수 있습니다.

이 명령을 입력하면 장애 조치 그룹 명령 모드가 시작합니다. 장애 조치 그룹 컨피그레이션 모드에서는 **primary**, **secondary**, **preempt**, **replication http**, **interface-policy**, **mac address**, **polltime interface** 명령을 사용할 수 있습니다. 글로벌 컨피그레이션 모드로 돌아가려면 **exit** 명령을 사용합니다.

참고 액티브/액티브 장애 조치 컨피그레이션에서는 **failover polltime interface**, **failover interface-policy**, **failover replication http**, **failover mac address** 명령이 어떤 효과도 없습니다. 장애 조치 그룹 컨피그레이션 모드 명령인 **polltime interface**, **interface-policy**, **replication http**, **mac address**에 의해 재정의됩니다.

장애 조치 그룹을 제거할 때 장애 조치 그룹 1을 마지막으로 제거해야 합니다. 장애 조치 그룹 1은 항상 관리자 컨텍스트를 갖습니다. 어떤 장애 조치 그룹에 지정되지 않은 컨텍스트는 기본적으로 장애 조치 그룹 1에 지정됩니다. 컨텍스트가 명시적으로 지정된 장애 조치 그룹은 제거할 수 없습니다.

참고 둘 이상의 액티브/액티브 장애 조치 쌍이 같은 네트워크에 있을 경우, 한 쌍의 인터페이스에 지정된 기본 가상 MAC 주소가 다른 쌍의 인터페이스에 지정될 수도 있습니다. 이는 기본 가상 MAC 주소가 결정되는 방식 때문입니다. 네트워크에 중복 MAC 주소가 생기는 것을 방지하기 위해 **mac address** 명령을 사용하여 각 물리적 인터페이스에 가상 액티브 및 스탠바이 MAC 주소를 지정해야 합니다.

예

다음 부분적 예에서는 2개의 장애 조치 그룹이 있을 경우 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)# exit
ciscoasa(config)#
```

관련 명령

명령	설명
asr-group	비대칭 라우팅 인터페이스 그룹 ID를 지정합니다.
interface-policy	모니터링을 통해 인터페이스 오류를 발견할 경우에 대한 장애 조치 정책을 지정합니다.
join-failover-group	장애 조치 그룹에 컨텍스트를 지정합니다.
mac address	장애 조치 그룹에 있는 컨텍스트를 위한 가상 mac 주소를 정의합니다.
polltime interface	모니터링되는 인터페이스에 보내는 hello 메시지의 간격을 지정합니다.
preempt	재부팅하면 우선 순위가 더 높은 유닛이 액티브 유닛이 되도록 지정합니다.
primary	장애 조치 그룹에서 기본 유닛에 더 높은 우선 순위를 부여합니다.
replication http	선택된 장애 조치 그룹에 대해 HTTP 세션 복제를 지정합니다.
secondary	장애 조치 그룹에서 보조 유닛에 더 높은 우선 순위를 부여합니다.

failover interface ip

장애 조치 인터페이스 및 상태 기반 장애 조치 인터페이스를 위해 IPv4 주소와 마스크 또는 IPv6 주소와 접두사를 지정하려면 글로벌 컨피그레이션 모드에서 **failover interface ip** 명령을 사용합니다. IP 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]

no failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]

구문 설명

if_name	장애 조치 또는 상태 기반 장애 조치 인터페이스의 인터페이스 이름.
ip_address mask	기본 디바이스의 장애 조치 또는 상태 기반 장애 조치 인터페이스를 위해 IP 주소와 마스크를 지정합니다.
ipv6_address	기본 디바이스의 장애 조치 또는 상태 기반 장애 조치 인터페이스를 위해 IPv6 주소를 지정합니다.
prefix	주소의 상위 연속 비트 중 몇 개가 IPv6 접두사(IPv6 주소에서 네트워크 부분)에 해당하는지 나타냅니다.
standby *ip_address*	보조 디바이스에서 기본 디바이스와 통신하는 데 사용하는 IP 주소를 지정합니다.
standby*ipv6_address*	보조 디바이스에서 기본 디바이스와 통신하는 데 사용하는 IPv6 주소를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.2(2)	이 명령에 IPv6 지원을 추가했습니다.

사용 지침

스탠바이 주소는 기본 주소와 동일한 서브넷에 있어야 합니다.

컨피그레이션에 **failvover interface ip** 명령을 하나만 포함할 수 있습니다. 따라서 장애 조치 인터페이스는 IPv6 주소 또는 IPv4 주소 중 하나만 가질 수 있습니다. IPv6 주소와 IPv4 주소를 모두 인터페이스에 지정할 수는 없습니다.

ASA가 투명 방화벽 모드에서 작동하더라도 장애 조치 및 상태 기반 장애 조치 인터페이스는 레이어 3 기능이므로 시스템의 전역에 해당됩니다.

다중 컨텍스트 모드에서는 시스템 컨텍스트에서 장애 조치를 구성합니다. 단, **monitor-interface** 명령은 제외합니다.

이 명령은 LAN 장애 조치를 위해 ASA를 부트스트랩할 때 컨피그레이션에 포함되어야 합니다.

예

다음 예에서는 장애 조치 인터페이스를 위해 IPv4 주소와 마스크를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

다음 예에서는 장애 조치 인터페이스를 위해 IPv6 주소와 접두사를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# failover interface ip lanlink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

관련 명령

명령	설명
clear configure failover	실행 중인 컨피그레이션에서 **failover** 명령을 지우고 장애 조치의 기본값을 복원합니다.
failover lan interface	장애 조치 통신에 사용하는 인터페이스를 지정합니다.
failover link	상태 기반 장애 조치에 사용하는 인터페이스를 지정합니다.
monitor-interface	지정된 인터페이스의 상태를 모니터링합니다.
show running-config failover	실행 중인 컨피그레이션의 **failover** 명령을 표시합니다.

failover interface-policy

모니터링을 통해 인터페이스 오류를 발견할 경우에 대한 장애 조치 정책을 지정하려면 글로벌 컨피그레이션 모드에서 **failover interface-policy** 명령을 사용합니다. 기본값으로 복원하려면 이 명령의 **no** 형식을 사용합니다.

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

구문 설명

num	백분율일 때는 1~100의 숫자를 지정하고, 숫자일 때는 1을 인터페이스 최대 개수로 지정합니다.
%	(선택 사항) 숫자 *num*이 모니터링되는 인터페이스의 비율(백분율)임을 지정합니다.

기본값

기본 설정은 다음과 같습니다.

- *num*은 1입니다.
- 물리적 인터페이스의 모니터링은 기본적으로 활성화됩니다. 논리적 인터페이스의 모니터링은 기본적으로 비활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

num 인수와 선택 사항인 **%** 키워드의 사이에 공백이 없습니다.

오류가 발생한 인터페이스의 수가 구성된 정책에 부합하고 다른 ASA가 정상적으로 작동하는 경우, ASA는 오류가 발생했음을 스스로에게 표시하며(액티브 ASA에서 오류가 발생했다면) 장애 조치가 일어날 수 있습니다. **monitor-interface** 명령에 의해 모니터링 대상으로 지정된 인터페이스만이 정책에서 계산됩니다.

참고 이 명령은 액티브/스탠바이 장애 조치에만 적용됩니다. 액티브/액티브 장애 조치에서는 장애 조치 그룹 컨피그레이션 모드에서 **interface-policy** 명령을 사용하여 각 장애 조치 그룹에 대해 인터페이스 정책을 구성합니다.

예

다음 예에서는 장애 조치 정책을 지정하는 2가지 방법을 보여줍니다.

```
ciscoasa(config)# failover interface-policy 20%

ciscoasa(config)# failover interface-policy 5
```

관련 명령

명령	설명
failover polltime	유닛 및 인터페이스 폴링 시간을 지정합니다.
failover reset	오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원합니다.
monitor-interface	장애 조치 모니터링 대상인 인터페이스를 지정합니다.
show failover	유닛의 장애 조치 상태에 대한 정보를 표시합니다.

failover ipsec pre-shared-key

모든 장애 조치 통신을 암호화하기 위해 유닛 간의 장애 조치 및 상태 링크에 IPsec LAN-to-LAN 터널을 설정하려면 글로벌 컨피그레이션 모드에서 **failover ipsec pre-shared-key** 명령을 사용합니다. 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

failover ipsec pre-shared-key *key*

no failover ipsec pre-shared-key

구문 설명

0	암호화되지 않은 비밀번호를 지정합니다. 이는 기본값입니다.
8	암호화된 비밀번호를 지정합니다. 마스터 패스프레이즈를 사용하는 경우(**password encryption aes** 및 **key config-key password-encryption** 명령 참조) 이 키는 컨피그레이션에서 암호화됩니다. 컨피그레이션에서(예: **more system:running-config** 출력에서) 복사할 경우 **8** 키워드를 사용하여 키가 암호화되었는지 지정합니다. **참고** **failover ipsec pre-shared-key** 는 **show running-config** 출력에 ***** 로 표시되며 , 이러한 가려진 키는 복사할 수 없습니다 .
key	두 유닛 모두에서 지정하는 *키*로서 IKEv2에서 터널을 설정하는 데 사용합니다. 최대 128자입니다.

명령 기본값

0(암호화되지 않음)이 기본값입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

사용 지침

장애 조치 통신에 대한 보안을 설정하지 않는 한, 장애 조치 및 상태 기반 장애 조치 링크를 지나는 모든 정보는 일반 텍스트의 형태로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(Pre-Shared key)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

기존의 **failover key** 방식보다는 **failover ipsec pre-shared-key** 암호화 방식을 사용하는 것이 좋습니다.

IPsec 암호화와 기존 **failover key** 암호화를 함께 사용할 수 없습니다. 두 방법을 모두 구성할 경우 IPsec가 사용됩니다. 그러나 마스터 패스프레이즈를 사용할 경우(**password encryption aes** 및 **key config-key password-encryption** 명령 참조), IPsec 암호화를 구성하기에 앞서 **no failover key** 명령을 사용하여 장애 조치 키를 제거해야 합니다.

참고 장애 조치 LAN-LAN 터널의 경우 IPsec(기타 VPN) 라이센스는 계산에 포함하지 않습니다.

예

다음 예에서는 IPsec PSK(pre-shared key)를 구성합니다.

```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

관련 명령

명령	설명
show running-config failover	실행 중인 컨피그레이션의 장애 조치 명령을 표시합니다.
show vpn-sessiondb	장애 조치 IPsec 터널을 포함하여 VPN 터널에 대한 정보를 표시합니다.

failover key

장애 조치 쌍의 유닛 간에 (장애 조치 및 상태 링크를 통해) 이루어지는 암호화된, 인증된 통신을 위한 키를 지정하려면 글로벌 컨피그레이션 모드에서 **failover key** 명령을 사용합니다. 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

failover key [0 | 8] {hex *key* **|** *shared_secret***}**

no failover key

구문 설명

0	암호화되지 않은 비밀번호를 지정합니다. 이는 기본값입니다.
8	암호화된 비밀번호를 지정합니다. 마스터 패스프레이즈를 사용하는 경우(**password encryption aes** 및 **key config-key password-encryption** 명령 참조) 이 공유 암호는 컨피그레이션에서 암호화됩니다. 컨피그레이션에서(예: **more system:running-config** 출력에서) 복사할 경우 **8** 키워드를 사용하여 공유 암호가 암호화되도록 지정합니다. **참고** **failover key** shared secret 은 **show running-config** 출력에 ***** 로 표시되며 , 이러한 가려진 키는 복사할 수 없습니다 .
hex *key*	암호화 키에 대해 16진수 값을 지정합니다. 키는 32개의 16진수(0-9, a-f)로 구성되어야 합니다.
shared_secret	영숫자 공유 암호를 지정합니다. 이 암호는 1자~63자입니다. 숫자, 문자, 구두점의 어떤 조합도 가능합니다. 공유 암호는 암호화 키를 생성하는 데 사용됩니다.

기본값

0(암호화되지 않음)이 기본값입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**failover lan key**에서 **failover key**로 명령을 수정했습니다.
7.0(4)	**hex** *key* 키워드 및 인수를 포함하도록 명령을 수정했습니다.
8.3(1)	**0** 및 **8** 키워드와 함께 마스터 패스프레이즈를 지원하도록 명령을 수정했습니다.

사용 지침

장애 조치 통신에 대한 보안을 설정하지 않는 한, 장애 조치 및 상태 기반 장애 조치 링크를 지나는 모든 정보는 일반 텍스트의 형태로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(Pre-Shared key)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

기존의 **failover key** 방식보다는 **failover ipsec pre-shared-key** 암호화 방식을 사용하는 것이 좋습니다.

IPsec 암호화(**failover ipsec pre-shared-key** 명령)와 기존 **failover key** 암호화를 모두 사용할 수는 없습니다. 두 방법을 모두 구성할 경우 IPsec가 사용됩니다. 그러나 마스터 패스프레이즈를 사용할 경우(**password encryption aes** 및 **key config-key password-encryption** 명령 참조), IPsec 암호화를 구성하기에 앞서 **no failover key** 명령을 사용하여 장애 조치 키를 제거해야 합니다.

예

다음 예에서는 장애 조치 쌍의 유닛 간에 이루어지는 장애 조치 통신에 대해 보안을 설정하기 위해 공유 암호를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# failover key abcdefg
```

다음 예에서는 장애 조치 쌍의 두 유닛 간에 이루어지는 장애 조치 통신에 대해 보안을 설정하기 위해 16진수 키를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

다음 예에서는 **more system:running-config** 출력에서 암호화된 비밀번호를 복사하여 붙여넣는 방법을 보여줍니다.

```
ciscoasa(config)# failover key 8 TPZCVNgdegLhWMa
```

관련 명령

명령	설명
show running-config failover	실행 중인 컨피그레이션의 장애 조치 명령을 표시합니다.

failover lan interface

장애 조치 통신에 사용하는 인터페이스를 지정하려면 글로벌 컨피그레이션 모드에서 **failover lan interface** 명령을 사용합니다. 장애 조치 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

failover lan interface *if_name* {*phy_if*[**.***sub_if*] | *vlan_if*]}

no failover lan interface [*if_name* {*phy_if*[**.***sub_if*] | *vlan_if*]}]

구문 설명

if_name	장애 조치 전용 ASA 인터페이스의 이름을 지정합니다.
phy_if	물리적 인터페이스를 지정합니다.
sub_if	(선택 사항) 하위 인터페이스 번호를 지정합니다.
vlan_if	ASA 5505에서 VLAN 인터페이스를 장애 조치 링크로 지정하는 데 사용합니다.

기본값

구성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	*phy_if* 인수를 포함하도록 명령을 수정했습니다.
7.2(1)	*vlan_if* 인수를 포함하도록 명령을 수정했습니다.

사용 지침

LAN 장애 조치에는 장애 조치 트래픽을 전달할 전용 인터페이스가 필요합니다. 그러나 상태 기반 장애 조치 링크에도 LAN 장애 조치 인터페이스를 사용할 수 있습니다.

참고 LAN 장애 조치와 상태 기반 장애 조치에 동일한 인터페이스를 사용할 경우, 이 인터페이스는 LAN 기반 장애 조치 및 상태 기반 장애 조치 트래픽을 모두 처리하기에 충분한 용량이 있어야 합니다.

디바이스에 있는 어떤 미사용 이더넷 인터페이스도 장애 조치 인터페이스로 사용할 수 있습니다. 이름과 함께 구성된 상태인 인터페이스는 지정할 수 없습니다. 장애 조치 링크 인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않습니다. 오로지 장애 조치 통신 용도로 사용됩니다. 이 인터페이스는 장애 조치 링크에서만(선택에 따라 상태 링크에서도) 사용해야 합니다. 링크에 호스트 및 라우터가 없는 상태로 전용 스위치를 사용하는 방법으로 또는 크로스오버 이더넷 케이블로 링크를 직접 연결하는 방법으로 LAN 기반 장애 조치 링크를 연결할 수 있습니다.

참고 VLAN을 사용할 때는 장애 조치 링크에 전용 VLAN을 사용합니다. 장애 조치 링크 VLAN을 다른 VLAN과 공유할 경우 일시적인 트래픽 문제, ping 및 ARP 오류가 발생할 수 있습니다. 장애 조치 링크 연결에 스위치를 사용할 경우 스위치 및 ASA에서 장애 조치 전용 인터페이스를 사용합니다. 이 인터페이스를 일반 네트워크 트래픽을 전달하는 하위 인터페이스와 공유하지 마십시오.

다중 컨텍스트 모드 시스템에서는 장애 조치 링크가 시스템 컨텍스트에 있습니다. 시스템 컨텍스트에서 구성할 수 있는 인터페이스는 이 인터페이스와 상태 링크(사용될 경우)뿐입니다. 다른 인터페이스는 모두 보안 컨텍스트에 할당되고 그 컨텍스트 내에서 구성됩니다.

참고 장애 조치 링크의 IP 주소와 MAC 주소는 장애 조치 시 변경되지 않습니다.

이 명령의 **no** 형식은 장애 조치 인터페이스 IP 주소 컨피그레이션도 지웁니다.

이 명령은 LAN 장애 조치를 위해 ASA를 부트스트랩할 때 컨피그레이션에 포함되어야 합니다.

주의 장애 조치 키로 통신 보안을 설정하지 않는 한 장애 조치 및 상태 기반 장애 조치(Stateful Failover) 링크를 통해 전송되는 모든 정보는 일반 텍스트로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(Pre-Shared key)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 장애 조치 키로 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

예

다음 예에서는 ASA 5500 시리즈(ASA 5505 제외)의 하위 인터페이스를 사용하여 장애 조치 LAN 인터페이스를 구성합니다.

```
ciscoasa(config)# failover lan interface folink GigabitEthernet0/3.1
```

다음 예에서는 ASA 5505에서 장애 조치 LAN 인터페이스를 구성합니다.

```
ciscoasa(config)# failover lan interface folink Vlan6
```

관련 명령

명령	설명
failover lan unit	LAN 기반 장애 조치의 기본 또는 보조 유닛을 지정합니다.
failover link	상태 기반 장애 조치 인터페이스를 지정합니다.

failover lan unit

ASA를 LAN 장애 조치 컨피그레이션의 기본 유닛 또는 보조 유닛으로 구성하려면 글로벌 컨피그레이션 모드에서 **failover lan unit** 명령을 사용합니다. 기본 설정으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

failover lan unit {primary | secondary}

no failover lan unit {primary | secondary}

구문 설명

primary	ASA를 기본 유닛으로 지정합니다.
secondary	ASA를 보조 유닛으로 지정합니다.

기본값

Secondary.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

액티브/스탠바이 장애 조치에서는 장애 조치 유닛을 기본 유닛 및 보조 유닛으로 지정함으로써 부팅 때 어떤 유닛이 액티브 상태가 되는가를 나타냅니다. 다음과 같은 경우에는 부팅 시 기본 유닛이 액티브 상태가 됩니다.

- 기본 유닛과 보조 유닛 모두 최초 장애 조치 폴링 검사 내에서 부트 시퀀스를 완료합니다.
- 기본 유닛이 보조 유닛보다 먼저 부팅됩니다.

기본 유닛이 부팅될 때 보조 유닛이 이미 액티브 상태라면 기본 유닛은 제어권을 갖지 못하고 스탠바이 유닛이 됩니다. 그러한 경우 (액티브 상태인) 보조 유닛에서 **no failover active** 명령을 입력하여 기본 유닛을 다시 액티브 상태로 강제 전환해야 합니다.

액티브/액티브 장애 조치에서는 각 장애 조치 그룹에 기본 또는 보조 유닛 기본 설정이 주어집니다. 두 유닛이(장애 조치 폴링 기간 내에) 동시에 시작할 경우 장애 조치 쌍의 어떤 유닛에서 장애 조치 그룹의 컨텍스트가 액티브 상태가 되는가는 이 기본 설정에 의해 결정됩니다.

이 명령은 LAN 장애 조치를 위해 ASA를 부트스트랩할 때 컨피그레이션에 포함되어야 합니다.

예

다음 예에서는 ASA를 LAN 기반 장애 조치의 기본 유닛으로 설정합니다.

```
ciscoasa(config)# failover lan unit primary
```

관련 명령

명령	설명
failover lan interface	장애 조치 통신에 사용하는 인터페이스를 지정합니다.

failover link

상태 기반 장애 조치 인터페이스를 지정하려면 글로벌 컨피그레이션 모드에서 **failover link** 명령을 사용합니다. 상태 기반 장애 조치 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

failover link *if_name* **[***phy_if***]**

no failover link

구문 설명

if_name	상태 기반 장애 조치 전용 ASA 인터페이스의 이름을 지정합니다.
phy_if	(선택 사항) 물리적 또는 논리적 인터페이스 포트를 지정합니다. 상태 기반 장애 조치 인터페이스에서 장애 조치 통신용으로 지정된 인터페이스를 공유하거나 표준 방화벽 인터페이스를 공유할 경우 이 인수는 필요하지 않습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	*phy_if* 인수를 포함하도록 명령을 수정했습니다.
7.0(4)	표준 방화벽 인터페이스를 허용하도록 명령을 수정했습니다.

사용 지침

이 명령은 상태 기반 장애 조치를 지원하지 않는 ASA 5505에서는 사용할 수 없습니다.

물리적 또는 논리적 인터페이스 인수는 장애 조치 통신이나 표준 방화벽 인터페이스를 공유하지 않을 때 필요합니다.

failover link 명령은 상태 기반 장애 조치를 활성화합니다. 상태 기반 장애 조치를 비활성화하려면 **no failover link** 명령을 입력합니다. 전용 상태 기반 장애 조치 인터페이스를 사용하는 경우 **no failover link** 명령은 상태 기반 장애 조치 인터페이스 IP 주소 컨피그레이션도 지웁니다.

상태 기반 장애 조치를 사용하려면 상태 기반 장애 조치 링크에서 모든 상태 정보를 전달하도록 구성해야 합니다. 상태 기반 장애 조치 링크를 구성하는 3가지 방법이 있습니다.

- 상태 기반 장애 조치 링크를 위한 전용 이더넷 인터페이스를 사용할 수 있습니다.
- LAN 기반 장애 조치를 사용하는 경우 장애 조치 링크를 공유할 수 있습니다.
- 내부 인터페이스와 같은 일반 데이터 인터페이스를 공유할 수 있습니다. 그러나 이 옵션은 권장되지 않습니다.

상태 기반 장애 조치 링크를 위한 전용 이더넷 인터페이스를 사용할 경우 스위치나 크로스오버 케이블 중 하나를 사용하여 유닛을 직접 연결할 수 있습니다. 스위치를 사용할 때는 이 링크에 다른 호스트나 라우터가 없어야 합니다.

참고 ASA에 직접 연결된 Cisco 스위치 포트에서 PortFast 옵션을 활성화합니다.

장애 조치 링크를 상태 기반 장애 조치 링크로 사용할 경우에는 가능한 가장 빠른 이더넷 인터페이스를 사용해야 합니다. 이 인터페이스에 성능 문제가 발생할 경우 상태 기반 장애 조치 링크 전용 인터페이스를 두는 것을 고려하십시오.

데이터 인터페이스를 상태 기반 장애 조치 링크로 사용할 경우, 이 인터페이스를 상태 기반 장애 조치 링크로 지정할 때 다음과 같은 경고가 표시됩니다.

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

데이터 인터페이스를 상태 기반 장애 조치 인터페이스와 공유할 경우 재생 공격(replay attack)에 취약해질 수 있습니다. 또한 대량의 상태 기반 장애 조치 트래픽이 인터페이스에서 전송되어 해당 네트워크 세그먼트에 성능 문제가 발생할 수 있습니다.

참고 데이터 인터페이스를 상태 기반 장애 조치 인터페이스로 사용하는 것을 지원하는 컨텍스트는 라우팅 모드뿐입니다.

다중 컨텍스트 모드 시스템에서는 상태 기반 장애 조치 링크가 시스템 컨텍스트에 있습니다. 시스템 컨텍스트에 있는 인터페이스는 이 인터페이스와 장애 조치 인터페이스뿐입니다. 다른 인터페이스는 모두 보안 컨텍스트에 할당되고 그 컨텍스트 내에서 구성됩니다.

참고 상태 기반 장애 조치 링크가 일반 데이터 인터페이스에 구성되지 않는 한, 상태 기반 장애 조치 링크의 IP 주소 및 MAC 주소는 장애 조치 시 바뀌지 않습니다.

주의 장애 조치 키로 통신 보안을 설정하지 않는 한 장애 조치 및 상태 기반 장애 조치(Stateful Failover) 링크를 통해 전송되는 모든 정보는 일반 텍스트로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(Pre-Shared key)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 장애 조치 키로 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

예

다음 예에서는 전용 인터페이스를 상태 기반 장애 조치 인터페이스로 지정하는 방법을 보여줍니다. 여기서는 인터페이스에 어떤 컨피그레이션도 없는 상태입니다.

```
ciscoasa(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

관련 명령

명령	설명
failover interface ip	**failover** 명령 및 상태 기반 장애 조치 인터페이스의 IP 주소를 구성합니다.
failover lan interface	장애 조치 통신에 사용하는 인터페이스를 지정합니다.

failover mac address

물리적 인터페이스에 대해 장애 조치 가상 MAC 주소를 지정하려면 글로벌 컨피그레이션 모드에서 **failover mac address** 명령을 사용합니다. 가상 MAC 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

구문 설명

active_mac	액티브 ASA의 지정된 인터페이스에 부여된 MAC 주소. MAC 주소는 h.h.h 형식으로 입력해야 합니다. 여기서 h는 16비트 16진수입니다.
phy_if	MAC 주소를 설정할 인터페이스의 물리적 이름.
standby_mac	스탠바이 ASA의 지정된 인터페이스에 부여된 MAC 주소. MAC 주소는 h.h.h 형식으로 입력해야 합니다. 여기서 h는 16비트 16진수입니다.

기본값

구성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

failover mac address 명령을 사용하면 액티브/스탠바이 장애 조치 쌍을 위한 가상 MAC 주소를 구성할 수 있습니다. 가상 MAC 주소가 정의되지 않으면 각 장애 조치 유닛이 부팅할 때 인터페이스에 번인된(burned-in) MAC 주소를 사용하고 이 주소를 장애 조치 피어와 교환합니다. 기본 유닛의 인터페이스 MAC 주소는 액티브 유닛의 인터페이스에 사용됩니다.

그러나 두 유닛이 동시에 온라인 상태가 되지 않고 보조 유닛이 먼저 부팅되어 액티브 상태가 될 경우, 이 유닛은 번인된 MAC 주소를 자신의 인터페이스에 사용합니다. 기본 유닛이 온라인 상태가 되면 보조 유닛은 기본 유닛으로부터 MAC 주소를 받습니다. 이러한 변경 때문에 네트워크 트래픽이 중단될 수 있습니다. 인터페이스에 가상 MAC 주소를 구성하면, 보조 유닛이 액티브 유닛이 될 때 설령 기본 유닛보다 먼저 온라인 상태가 되더라도 올바른 MAC 주소를 사용하게 됩니다.

LAN 기반 장애 조치가 구성된 인터페이스에서는 **failover mac address** 명령이 불필요하며 따라서 사용할 수 없습니다. **failover lan interface** 명령은 장애 조치 상황에서 IP 주소와 MAC 주소를 변경하지 않기 때문입니다. 이 명령은 ASA에서 액티브/액티브 장애 조치가 구성된 경우에는 아무런 효과가 없습니다.

컨피그레이션에 **failover mac address** 명령을 추가할 경우, 가상 MAC 주소를 구성하고 그 컨피그레이션을 플래시 메모리에 저장한 다음 장애 조치 쌍을 다시 로드하는 것이 가장 좋습니다. 액티브 연결이 있는 상태에서 가상 MAC 주소가 추가되면 이 연결은 중지합니다. 또한 가상 MAC 주소 지정이 제대로 작동하려면 **failover mac address** 명령을 포함한 전체 컨피그레이션을 보조 ASA의 플래시 메모리에 기록해야 합니다.

failover mac address가 기본 유닛의 컨피그레이션에 지정될 경우 보조 유닛의 부트스트랩 컨피그레이션에서도 지정되어야 합니다.

참고 이 명령은 액티브/스탠바이 장애 조치에만 적용됩니다. 액티브/액티브 장애 조치에서는 장애 조치 그룹 컨피그레이션 모드에서 **mac address** 명령을 사용하여 장애 조치 그룹의 각 인터페이스에 대해 가상 MAC 주소를 구성합니다.

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 예에서는 intf2라는 인터페이스를 위해 액티브 및 스탠바이 MAC 주소를 구성합니다.

```
ciscoasa(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

관련 명령

명령	설명
show interface	인터페이스 상태, 컨피그레이션, 통계를 표시합니다.

failover polltime

장애 조치 유닛의 폴링 및 대기 시간을 지정하려면 글로벌 컨피그레이션 모드에서 **failover polltime** 명령을 사용합니다. 기본 폴링 및 대기 시간을 복원하려면 이 명령의 **no** 형식을 사용합니다.

failover polltime [unit] [msec] *poll_time* **[holdtime [msec]** *time***]**

no failover polltime [unit] [msec] *poll_time* **[holdtime [msec]** *time***]**

구문 설명

holdtime *time*	(선택 사항) 어떤 유닛이 피어 유닛에서 오류가 발생한 것으로 선언된 후 얼마 이내에 장애 조치 링크에서 hello 메시지를 받아야 하는지 설정합니다. 유효한 값은 3초~45초이며, 선택 사항인 **msec** 키워드가 사용될 경우에는 800밀리초~999밀리초입니다.
msec	(선택 사항) 지정된 시간이 밀리초 단위임을 나타냅니다.
poll_time	hello 메시지의 간격을 설정합니다. 유효한 값은 1초~15초이며, 선택 사항인 **msec** 키워드가 사용될 경우에는 200밀리초~999밀리초입니다.
unit	(선택 사항) 이 명령이 유닛 폴링 및 대기 시간에 사용됨을 나타냅니다. 이 키워드를 추가하더라도 명령에 영향을 주지 않습니다. 그러나 컨피그레이션에서 이 명령과 **failover polltime interface** 명령을 구별하기가 더 쉬워집니다.

기본값

ASA의 기본값은 다음과 같습니다.

- *poll_time*은 1초입니다.
- **holdtime** *time*은 15초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**failover poll** 명령에서 **failover polltime** 명령으로 변경했고 **unit** 및 **holdtime** 키워드도 추가했습니다.
7.2(1)	**msec** 키워드를 **holdtime** 키워드에 추가했습니다. **polltime** 최소값이 500밀리초에서 200밀리초로 감소했습니다. **holdtime** 최소값이 3초에서 800밀리초로 감소했습니다.

사용 지침

holdtime 값이 유닛 폴링 시간의 3배보다 적을 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.

한 차례의 폴링 기간 동안 유닛의 장애 조치 통신 인터페이스 또는 케이블에서 hello 패킷이 수신되지 않을 경우, 나머지 인터페이스를 통해 추가 테스트가 이루어집니다. 대기 시간에도 피어 유닛의 응답이 없을 경우 그 유닛에 오류가 발생한 것으로 간주하며, 오류가 발생한 유닛이 액티브 유닛이었다면 스탠바이 유닛이 액티브 유닛으로 전환합니다.

failover polltime [**unit**] 명령과 **failover polltime interface** 명령을 모두 컨피그레이션에 포함할 수 있습니다.

참고 장애 조치 컨피그레이션에서 CTIQBE 트래픽이 ASA를 통해 전달될 경우 ASA의 장애 조치 대기 시간을 30초 미만으로 낮춰야 합니다. CTIQBE keepalive 시간 초과는 30초이므로 장애 조치 상황에서 장애 조치가 이루어지기 전에 만료될 수 있습니다. CTIQBE가 시간 초과될 경우 Cisco IP SoftPhone과 Cisco CallManager의 연결이 끊기며 IP SoftPhone 클라이언트는 CallManager에 재등록해야 합니다.

예

다음 예에서는 유닛 폴링 빈도를 3초로 변경합니다.

```
ciscoasa(config)# failover polltime 3
```

다음 예에서는 ASA에서 200밀리초마다 hello 패킷을 보내고 그 시간 내에 장애 조치 인터페이스에서 hello 패킷이 수신되지 않으면 800밀리초 후에 장애 조치하도록 구성합니다. 선택 사항인 **unit** 키워드가 명령에 포함됩니다.

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

관련 명령

명령	설명
failover polltime interface	액티브/스탠바이 장애 조치 컨피그레이션의 인터페이스 폴링 및 대기 시간을 지정합니다.
polltime interface	액티브/액티브 장애 조치 컨피그레이션의 인터페이스 폴링 및 대기 시간을 지정합니다.
show failover	장애 조치 컨피그레이션 정보를 표시합니다.

failover polltime interface

액티브/스탠바이 장애 조치 컨피그레이션에서 데이터 인터페이스 폴링 및 대기 시간을 지정하려면 글로벌 컨피그레이션 모드에서 **failover polltime interface** 명령을 사용합니다. 기본 폴링 및 대기 시간을 복원하려면 이 명령의 **no** 형식을 사용합니다.

failover polltime interface [msec] *time* **[holdtime** *time***]**

no failover polltime interface [msec] *time* **[holdtime** *time***]**

구문 설명

holdtime *time*	(선택 사항) 피어에서 오류가 발생한 것으로 선언된 후 얼마 이내에 데이터 인터페이스에서 hello 메시지를 받아야 하는지 설정합니다. 올바른 값의 범위는 5~75초입니다.
interface *time*	인터페이스 모니터링의 폴링 시간을 지정합니다. 유효한 값의 범위는 1초~15초입니다. 선택 사항인 **msec** 키워드가 사용될 경우 유효한 값의 범위는 500밀리초~999밀리초입니다.
msec	(선택 사항) 지정된 시간이 밀리초 단위임을 나타냅니다.

기본값

기본값은 다음과 같습니다.

- poll *time*은 5초입니다.
- **holdtime** *time*은 poll *time*의 5배입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**failover poll** 명령에서 **failover polltime** 명령으로 변경했고 **unit**, **interface**, **holdtime** 키워드를 추가했습니다.
7.2(1)	선택 사항인 **holdtime** *time* 및 밀리초 단위로 폴링 시간을 지정하는 기능을 추가했습니다.

사용 지침

failover polltime interface 명령은 데이터 인터페이스에서 hello 패킷이 전송되는 빈도를 변경하는 데 사용합니다. 이 명령은 액티브/스탠바이 장애 조치에서만 사용할 수 있습니다. 액티브/액티브 장애 조치의 경우, **failover polltime interface** 명령이 아니라 장애 조치 그룹 컨피그레이션 모드의 **polltime interface** 명령을 사용합니다.

holdtime 값이 유닛 폴링 시간의 5배보다 적을 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 시간의 절반이 지날 때까지 인터페이스에서 hello 패킷이 수신되지 않으면 인터페이스 테스트가 시작합니다.

failover polltime unit 명령과 **failover polltime interface** 명령을 모두 컨피그레이션에 포함할 수 있습니다.

참고 장애 조치 컨피그레이션에서 CTIQBE 트래픽이 ASA를 통해 전달될 경우 ASA의 장애 조치 대기 시간을 30초 미만으로 낮춰야 합니다. CTIQBE keepalive 시간 초과는 30초이므로 장애 조치 상황에서 장애 조치가 이루어지기 전에 만료될 수 있습니다. CTIQBE가 시간 초과될 경우 Cisco IP SoftPhone과 Cisco CallManager의 연결이 끊기며 IP SoftPhone 클라이언트는 CallManager에 재등록해야 합니다.

예

다음 예에서는 인터페이스 폴링 빈도를 15초로 설정합니다.

```
ciscoasa(config)# failover polltime interface 15
```

다음 예에서는 인터페이스 폴링 빈도를 500밀리초로, 대기 시간을 5초로 설정합니다.

```
ciscoasa(config)# failover polltime interface msec 500 holdtime 5
```

관련 명령

명령	설명
failover polltime	유닛 장애 조치 폴링 및 대기 시간을 지정합니다.
polltime interface	액티브/액티브 장애 조치 컨피그레이션의 인터페이스 폴링 시간을 지정합니다.
show failover	장애 조치 컨피그레이션 정보를 표시합니다.

failover reload-standby

스탠바이 유닛을 강제로 재부팅하려면 특별 권한 EXEC 모드에서 **failover reload-standby** 명령을 사용합니다.

failover reload-standby

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

장애 조치 유닛이 동기화되지 않을 때 이 명령을 사용합니다. 부팅이 끝나면 스탠바이 유닛이 재시작하고 액티브 유닛과 다시 동기화합니다.

예

다음 예에서는 스탠바이 유닛을 강제로 재부팅하기 위해 액티브 유닛에서 **failover reload-standby** 명령을 사용하는 방법을 보여줍니다.

```
ciscoasa# failover reload-standby
```

관련 명령

명령	설명
write standby	실행 중인 컨피그레이션을 스탠바이 유닛의 메모리에 기록합니다.

failover replication http

HTTP(포트 80) 연결 복제를 활성화하려면 글로벌 컨피그레이션 모드에서 **failover replication http** 명령을 사용합니다. HTTP 연결 복제를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

failover replication http

no failover replication http

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	**failover replicate http** 명령을 **failover replication http** 명령으로 변경했습니다.

사용 지침

기본적으로 ASA는 상태 기반 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. **failover replication http** 명령은 상태 기반 장애 조치 환경에서 HTTP 세션의 상태 기반 복제를 활성화하지만, 이는 시스템 성능에 불리하게 작용할 수 있습니다.

액티브/액티브 장애 조치 컨피그레이션에서는 장애 조치 그룹 컨피그레이션 모드에서 **replication http** 명령을 사용하여 장애 조치 그룹별로 HTTP 세션 복제를 제어합니다.

예

다음 예에서는 HTTP 연결 복제를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# failover replication http
```

관련 명령

명령	설명
replication http	특정 장애 조치 그룹에 대해 HTTP 세션 복제를 활성화합니다.
show running-config failover	실행 중인 컨피그레이션의 **장애 조치** 명령을 표시합니다.

failover replication rate

일괄 동기화(bulk-sync) 연결 복제 속도를 구성하려면 글로벌 컨피그레이션 모드에서 **failover replication rate** 명령을 사용합니다. 기본 설정으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

failover replication rate *rate*

no failover replication rate

구문 설명

rate	초당 연결 수를 설정합니다. 이 값과 기본 설정은 모델의 초당 최대 연결 수에 따라 달라집니다.

명령 기본값

모델에 따라 달라집니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.4(4.1)/8.5(1.7)	이 명령을 도입했습니다.

사용 지침

상태 기반 장애 조치를 사용할 때 ASA에서 스탠바이 유닛에 연결을 복제하는 속도를 구성할 수 있습니다. 기본적으로 15초의 기간에 스탠바이 유닛에 연결이 복제됩니다. 그러나 일괄 동기화가 일어나면(예: 처음으로 장애 조치를 활성화할 때) 초당 최대 연결 수의 제한 때문에 많은 수의 연결을 동기화하는 데 15초가 충분하지 않을 수 있습니다. 이를테면 ASASM의 최대 연결 수는 8백만입니다. 15초에 8백만 개의 연결을 복제하려면 초당 533K의 연결이 생성됩니다. 그러나 초당 연결 수 최대 한도는 300K입니다. 이제 복제 속도를 초당 연결 수 최대 한도보다 적거나 같게 지정할 수 있습니다. 그리고 동기화 기간은 모든 연결이 동기화되도록 조정됩니다.

예

다음 예에서는 장애 조치 복제 속도를 초당 연결 수 20000으로 설정합니다.

```
ciscoasa(config)# failover replication rate 20000
```

관련 명령

명령	설명
failover rate http	HTTP 연결 복제를 활성화합니다.

failover reset

오류가 발생한 ASA를 오류 없는 상태로 복원하려면 특별 권한 EXEC 모드에서 **failover reset** 명령을 사용합니다.

failover reset [group *group_id***]**

구문 설명

group	(선택 사항) 장애 조치 그룹을 지정합니다. **group** 키워드는 액티브/액티브 장애 조치에만 적용됩니다.
group_id	장애 조치 그룹 번호.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	선택 사항인 장애 조치 그룹 ID를 추가하기 위해 이 명령을 수정했습니다.

사용 지침

failover reset 명령을 사용하면 오류가 발생한 유닛 또는 그룹을 오류 없는 상태로 변경할 수 있습니다. **failover reset** 명령은 두 유닛 중 어디서도 입력할 수 있으나, 항상 액티브 유닛에서 입력하는 것이 좋습니다. 액티브 유닛에서 **failover reset** 명령을 입력하면 스탠바이 유닛이 "오류 없는 상태"가 됩니다.

show failover 또는 **show failover state** 명령을 사용하여 유닛의 장애 조치 상태를 표시할 수 있습니다.

이 명령은 **no** 형식이 없습니다.

액티브/액티브 장애 조치에서 **failover reset**을 입력하면 전체 유닛이 재설정됩니다. 이 명령에서 장애 조치 그룹을 지정하면 지정된 그룹만 재설정됩니다.

예

다음 예에서는 오류가 발생한 유닛을 오류 없는 상태로 변경하는 방법을 보여줍니다.

```
ciscoasa# failover reset
```

관련 명령

명령	설명
failover interface-policy	모니터링을 통해 인터페이스 오류를 발견할 경우에 대한 장애 조치 정책을 지정합니다.
show failover	유닛의 장애 조치 상태에 대한 정보를 표시합니다.

failover standby config-lock

스탠바이 유닛 또는 장애 조치 쌍의 스탠바이 컨텍스트에서 컨피그레이션 변경을 잠그려면 글로벌 컨피그레이션 모드에서 **failover standby config-lock** 명령을 사용합니다. 스탠바이 유닛에 대한 컨피그레이션을 허용하려면 이 명령의 **no** 형식을 사용합니다.

failover standby config-lock

no failover standby config-lock

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

기본적으로 스탠바이 유닛/컨텍스트에서 컨피그레이션을 수행하는 작업은 경고 메시지와 함께 허용됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.3(2)	이 명령을 도입했습니다.

사용 지침

스탠바이 유닛(액티브/스탠바이 장애 조치) 또는 스탠바이 컨텍스트(액티브/액티브 장애 조치)의 컨피그레이션 변경을 잠글 수 있습니다. 그러면 정상적인 컨피그레이션 동기화를 벗어난 범위에서 스탠바이 유닛을 변경할 수 없게 됩니다.

예

다음 예에서는 스탠바이 유닛에 대한 컨피그레이션을 허용하지 않습니다.

```
ciscoasa(config)# failover standby config-lock
```

관련 명령

명령	설명
clear configure failover	실행 중인 컨피그레이션에서 **failover** 명령을 지우고 장애 조치의 기본값을 복원합니다.
failover active	스탠바이 유닛을 액티브 상태로 전환합니다.
show failover	유닛의 장애 조치 상태에 대한 정보를 표시합니다.
show running-config failover	실행 중인 컨피그레이션의 **failover** 명령을 표시합니다.

failover timeout

비대칭 라우팅 세션에 대해 장애 조치 재연결 시간 초과의 값을 지정하려면 글로벌 컨피그레이션 모드에서 **failover timeout** 명령을 사용합니다. 시간 초과의 기본값으로 복원하려면 이 명령의 **no** 형식을 입력합니다.

failover timeout *hh*[**:***mm*[**:**[*ss*]]

no failover timeout [*hh*[**:***mm*[**:**[*ss*]]]

구문 설명

hh	시간 초과의 값을 시간 단위로 지정합니다. 유효한 값의 범위는 -1~1193입니다. 기본적으로 이 값은 0으로 설정됩니다. 이 값을 -1로 설정하면 시간 초과가 비활성화되어 아무리 시간이 지나더라도 재연결할 수 있게 됩니다. 다른 시간 초과의 값을 지정하지 않고 이 값을 0으로 설정하면 이 명령이 기본값으로 돌아갑니다. 즉 재연결하지 않습니다. **no failover timeout** 명령을 입력해도 이 값이 기본값(0)으로 설정됩니다. **참고** 이 명령이 기본값으로 설정되면 실행 중인 컨피그레이션에 나타나지 않습니다 .
mm	(선택 사항) 시간 초과의 값을 분 단위로 지정합니다. 유효한 값의 범위는 0~59입니다. 기본적으로 이 값은 0으로 설정됩니다.
ss	(선택 사항) 시간 초과의 값을 초 단위로 지정합니다. 유효한 값의 범위는 0~59입니다. 기본적으로 이 값은 0으로 설정됩니다.

기본값

기본적으로 *hh*, *mm*, *ss*는 0입니다. 즉 재연결하지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	명령 목록에 표시되도록 이 명령을 수정했습니다.

사용 지침

이 명령은 **static** 명령과 함께, **nailed** 옵션도 포함하여 사용합니다. **nailed** 옵션을 사용하면 부팅 후 또는 시스템이 액티브 상태가 된 후 지정된 시간 동안 연결이 재설정될 수 있습니다. **failover timeout** 명령이 그 시간을 지정합니다. 구성되지 않으면 연결이 재설정될 수 없습니다. **failover timeout** 명령은 **asr-group** 명령에 영향을 주지 않습니다.

참고 **nailed** 옵션을 **static** 명령에 추가하면 그 연결에 대해서는 TCP 상태 추적 및 시퀀스 검사를 건너뜁니다.

이 명령의 **no** 형식을 입력하면 기본값이 복원됩니다. **failover timeout 0**을 입력해도 기본값이 복원됩니다. 이 명령이 기본값으로 설정되면 실행 중인 컨피그레이션에 나타나지 않습니다.

예

다음 예에서는 스탠바이 group 1을 액티브 상태로 전환합니다.

```
ciscoasa(config)# failover timeout 12:30
ciscoasa(config)# show running-config failover
no failover
failover timeout 12:30:00
```

관련 명령

명령	설명
static	로컬 IP 주소를 전역 IP 주소에 매핑함으로써 지속적인 일대일 주소 변호나 규칙을 구성합니다.

fallback

연결의 무결성이 저하될 때 Cisco Intercompany Media Engine이 VoIP에서 PSTN으로 폴백하는 데 사용하는 폴백 타이머를 구성하려면 uc-ime 컨피그레이션 모드에서 **fallback** 명령을 사용합니다. 폴백 설정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

fallback {sensitivity-file *filename* **| monitoring timer** *timer_millisec* **hold-down timer** *timer_sec***}**

no fallback fallback {sensitivity-file *filename* **| monitoring timer** *timer_millisec* **hold-down timer** *timer_sec***}**

구문 설명

filename	감도 파일(sensitivity file)의 이름을 지정합니다. 디스크에 있는 파일의 이름을 .fbs 파일 확장자까지 포함하여 입력합니다. 파일 이름을 지정하는 데 로컬 디스크의 경로를 포함할 수 있습니다(예: `disk0:/file001.fbs`).
hold-down timer	ASA에서 Cisco UCM에 PSTN으로 폴백할지 여부를 알리기 전에 기다리는 시간을 설정합니다.
monitoring timer	ASA가 인터넷에서 받은 RTP 패킷을 샘플링하는 시간을 설정합니다. ASA에서는 이 데이터 샘플을 사용하여 어떤 통화에서 PSTN으로의 폴백이 필요한지 결정합니다.
sensitivity-file	통화 중 PSTN 폴백에 사용할 파일을 지정합니다. 감도 파일은 ASA에서 구문 분석하고 RMA 라이브러리에 입력합니다.
timer_millisec	모니터링 타이머의 길이(밀리초)를 지정합니다. 10~600 범위의 정수를 입력합니다. 기본적으로 모니터링 타이머의 길이는 100밀리초입니다.
timer_sec	보류 타이머의 길이(초)를 지정합니다. 10~360 범위의 정수를 입력합니다. 기본적으로 보류 타이머의 길이는 20초입니다.

기본값

기본적으로 모니터링 타이머의 길이는 100밀리초입니다.

기본적으로 보류 타이머의 길이는 20초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Uc-ime 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

사용 지침

Cisco Intercompany Media Engine의 폴백 타이머를 지정합니다.

인터넷 연결은 그 품질의 차이가 크고 시간이 지나면서 달라질 수 있습니다. 따라서 연결의 품질이 우수하여 VoIP를 통해 통화를 전송했더라도 통화 중에 연결의 품질이 나빠질 수 있습니다. 최종 사용자에게 전반적으로 우수한 경험을 제공하기 위해 Cisco Intercompany Media Engine은 통화 중 폴백(mid-call fallback)을 시도합니다.

통화 중 폴백을 수행하려면 ASA에서 인터넷에서 보내는 RTP 패킷을 모니터링하고 RMA(RTP Monitoring Algorithm) API에 정보를 보내야 합니다. RMA API는 폴백의 필요 여부를 ASA에 알립니다. 폴백이 필요할 경우 ASA는 Cisco UCM에 REFER 메시지를 보내 통화를 PSTN으로 폴백해야 한다고 알립니다.

참고 SIP 검사를 위해 Cisco Intercompany Media Engine 프록시가 활성화된 상태에서 폴백 타이머를 변경할 수 없습니다. 폴백 타이머를 변경하기 전에 SIP 검사에서 Cisco Intercompany Media Engine 프록시를 제거합니다.

예

다음 예에서는 폴백 타이머를 지정하면서 Cisco Intercompany Media Engine을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# uc-ime local_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
```

다음 예에서는 감도 파일을 지정하면서 Cisco Intercompany Media Engine을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# uc-ime local_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 sensitivity-file local_uc-ime_fallback_policy
```

관련 명령

명령	설명
show running-config uc-ime	Cisco Intercompany Media Engine 프록시의 실행 중인 컨피그레이션을 표시합니다.
show uc-ime	폴백 알림, 매핑 서비스 세션, 시그널링 세션에 대한 통계 또는 세부 정보를 표시합니다.
uc-ime	ASA에 Cisco Intercompany Media Engine 프록시를 만듭니다.

16 장

file-bookmarks ~ functions 명령

file-bookmarks

인증된 WebVPN 사용자에게 표시되는 WebVPN Home 페이지에서 File Bookmarks 제목 또는 File Bookmarks 링크를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **file-bookmarks** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

file-bookmarks {link {style *value*} **| title {style** *value* **| text** *value*}}

no file-bookmarks {**link** {**style** *value*} **|** **title** {**style** *value* **|** **text** *value*}}

구문 설명

link	링크의 변경 사항을 지정합니다.
title	제목의 변경 사항을 지정합니다.
style	HTML 스타일의 변경 사항을 지정합니다.
text	텍스트의 변경 사항을 지정합니다.
value	표시할 실제 텍스트 또는 CSS 매개변수(최대 256자).

기본값

기본 링크 스타일은 color:#669999;border-bottom: 1px solid #669999;text-decoration:none입니다.

기본 제목 스타일은 color:#669999;background-color:#99CCCC;font-weight:bold입니다.

기본 제목 텍스트는 "File Folder Bookmarks"입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

style 옵션은 임의의 유효한 CSS 매개변수로 표시됩니다. 이 매개변수에 대한 설명은 본 설명서의 범위에 속하지 않습니다. CSS 매개변수에 대한 자세한 내용은 W3C 웹 사이트(www.w3.org)의 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F는 편리한 CSS 매개변수 목록을 포함하고 있으며 www.w3.org/TR/CSS21/propidx.html에서 이용할 수 있습니다.

WebVPN 페이지 - 페이지 색상의 가장 대표적인 변경 방법에 대한 몇 가지 팁을 소개합니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 (HTML에서 인식된다면) 색상의 이름을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며, 각 색상(빨강, 녹색, 파랑)을 나타내는 0~255 범위의 10진수입니다. 쉼표로 구분하여 입력한 값은 해당 강도의 각 색상이 나머지 색상과 조합되는 것을 의미합니다.
- HTML 형식은 #000000이며, 6자리의 16진수입니다. 1번째와 2번째 자리는 빨강을, 3번째와 4번째 자리는 녹색을, 5번째와 6번째는 파랑을 나타냅니다.

참고 손쉽게 WebVPN 페이지를 사용자 지정하려면 ASDM을 사용하는 것이 좋습니다. 색 견본, 미리 보기 등 스타일 요소를 편리하게 구성할 수 있는 기능을 제공합니다.

예

다음 예에서는 File Bookmarks 제목을 "Corporate File Bookmarks"로 사용자 지정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

관련 명령

명령	설명
application-access	WebVPN Home 페이지의 Application Access 상자를 사용자 지정합니다.
browse-networks	WebVPN Home 페이지의 Browse Networks 상자를 사용자 지정합니다.
web-applications	WebVPN Home 페이지의 Web Application 상자를 사용자 지정합니다.
web-bookmarks	WebVPN Home 페이지의 Web Bookmarks 제목 또는 링크를 사용자 지정합니다.

file-browsing

파일 서버 또는 공유에 대해 CIFS/FTP 파일 브라우징을 활성화하거나 비활성화하려면 dap webvpn 컨피그레이션 모드에서 **file-browsing** 명령을 사용합니다.

file-browsing enable | disable

구문 설명

enable | disable	파일 서버 또는 공유를 브라우징하는 기능을 활성화하거나 비활성화합니다.

기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Dap webvpn 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

다음 사용 참고 사항은 파일 브라우징에 적용됩니다.

- 파일 브라우징은 다국어를 지원하지 않습니다.
- 브라우징에는 NBNS(마스터 브라우저 또는 WINS)가 필요합니다. 이것이 실패하거나 구성되지 않은 경우 DNS를 사용합니다.

ASA는 다양한 소스의 특성 값을 적용할 수 있습니다. 다음 계층 구조에 따라 적용합니다.

1. DAP 레코드
2. 사용자 이름
3. 그룹 정책
4. 터널 그룹에 대한 그룹 정책
5. 기본 그룹 정책

특성의 DAP 값은 사용자, 그룹 정책 또는 터널 그룹에 대해 구성된 값보다 우선순위가 높습니다.

DAP 레코드에 대한 특성을 활성화하거나 비활성화하면 ASA는 그 값을 강제적으로 적용합니다. 이를테면 dap webvpn 컨피그레이션 모드에서 파일 브라우징을 비활성화하면 ASA는 더 이상 값을 찾지 않습니다. 그 대신 **file-browsing** 명령에 대해 어떤 값도 설정하지 않으면 그 특성은 DAP 레코드기 없으므로, ASA는 사용자 이름, 필요하다면 그룹 정책의 AAA 특성까지 내려와 적용할 값을 찾습니다.

예

다음 예에서는 Finance라는 DAP 레코드에 대해 파일 브라우징을 활성화하는 방법을 보여줍니다.

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# file-browsing enable
ciscoasa(config-dap-webvpn)#
```

관련 명령

명령	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
file-entry	액세스할 파일 서버 이름을 입력하는 기능을 활성화하거나 비활성화합니다.

file-encoding

CIFS(Common Internet File System) 서버의 페이지에 대한 문자 인코딩을 지정하려면 webvpn 컨피그레이션 모드에서 **file-encoding** 명령을 사용합니다. 파일 인코딩 특성의 값을 제거하려면 이 명령의 **no** 형식을 사용합니다.

file-encoding {server-name | server-ip-addr} *charset*

no file-encoding {**server-name** | **server-ip-addr**}

구문 설명

charset	최대 40자의 문자열이며, http://www.iana.org/assignments/character-sets에 지정된 유효한 문자 집합 중 하나와 같습니다. 이 페이지에 있는 문자 집합의 이름 또는 별칭을 사용할 수 있습니다. 이를테면 iso-8859-1, shift_jis, ibm850입니다. 이 문자열은 대/소문자를 구분하지 않습니다. 명령 해석기가 ASA 컨피그레이션에서 대문자를 소문자로 변환합니다.
server-ip-addr	문자 인코딩을 지정하려는 CIFS 서버의 IP 주소로서 점으로 구분된 10진수로 표기됩니다.
server-name	문자 인코딩을 지정하려는 CIFS 서버의 이름. ASA는 사용자가 지정하는 대/소문자를 유지하지만, 서버의 이름과 매칭할 때는 대/소문자를 구분하지 않습니다.

기본값

WebVPN 컨피그레이션에 명시적인 파일 인코딩 엔트리가 없는 모든 CIFS 서버의 페이지는 문자 인코딩 특성에서 문자 인코딩 값을 상속합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

webvpn 문자 인코딩 특성의 값과 다른 문자 인코딩 엔트리가 필요한 모든 CIFS 서버를 위해 파일 인코딩 엔트리를 입력합니다.

CIFS 서버에서 WebVPN 사용자에게 다운로드된 WebVPN 포털 페이지는 서버를 식별하는 WebVPN 파일 인코딩 특성의 값을 인코딩합니다. 또는 그런 값이 없다면 문자 인코딩 특성의 값을 상속합니다. 원격 사용자의 브라우저는 이 값을 자체 문자 인코딩 집합의 엔트리에 매핑하여 사용하기에 적합한 문자 집합를 확인합니다. WebVPN 컨피그레이션에서 CIFS 서버를 위한 파일 인코딩 엔트리를

지정하지 않고 문자 인코딩 특성도 설정되지 않은 경우, WebVPN 포털 페이지는 값을 지정하지 않습니다. WebVPN 포털 페이지에서 문자 인코딩을 지정하지 않을 경우 또는 브라우저에서 지원하지 않는 문자 인코딩 값을 지정할 경우, 원격 브라우저는 자체 기본 인코딩을 사용합니다.

페이지뿐 아니라 파일 이름 또는 디렉토리 경로를 올바르게 렌더링하는 것과 관련하여 문제가 있을 경우, 전역으로는 WebVPN 문자 인코딩 특성을 사용하여, 개별적으로는 파일 인코딩 재정의를 통해 CIFS 서버를 알맞은 문자 인코딩에 매핑함으로써 CIFS 페이지를 정확하게 처리하고 표시할 수 있습니다.

참고 문자 인코딩 값과 파일 인코딩 값은 브라우저에서 사용하는 글꼴 패밀리를 제외하지 않습니다. 다음 예와 같이 일본어 Shift_JIS 문자 인코딩을 사용하는 경우 이 값 중 하나의 설정을 webvpn 사용자 지정 명령 모드의 **page style** 명령으로 보완하여 글꼴 패밀리를 대체해야 합니다. 또는 webvpn 사용자 지정 명령 모드에서 **no page style** 명령을 입력하여 글꼴 패밀리를 제거해야 합니다.

예

다음 예에서는 일본어 Shift_JIS 문자를 지원하기 위해 "CISCO-server-jp"라는 CIFS 서버의 파일 인코딩 특성을 설정하고 글꼴 패밀리를 제거하며 기본 배경색을 유지합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding CISCO-server-jp shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

다음 예에서는 IBM860(일명 "CP860") 문자를 지원하기 위해 CIFS 서버 10.86.5.174의 파일 인코딩 특성을 설정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding 10.86.5.174 cp860
ciscoasa(config-webvpn)
```

관련 명령

명령	설명
character-encoding	WebVPN 컨피그레이션의 파일 인코딩 엔트리에 지정된 서버의 페이지를 제외하고 모든 WebVPN 포털 페이지에 사용되는 전역 문자 인코딩을 지정합니다.
show running-config webvpn	WebVPN을 위해 실행 중인 컨피그레이션을 표시합니다. 기본 컨피그레이션을 포함하려면 **all** 키워드를 사용합니다.
debug webvpn cifs	CIFS에 대한 디버깅 메시지를 표시합니다.

file-entry

사용자가 액세스할 파일 서버 이름을 입력하는 기능을 활성화하거나 비활성화하려면 dap webvpn 컨피그레이션 모드에서 **file-entry** 명령을 사용합니다.

file-entry enable | disable

구문 설명

**enable	disable**	액세스할 파일 서버 이름을 입력하는 기능을 활성화하거나 비활성화합니다.

기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Dap webvpn 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ASA에서는 다음 계층 구조에 따라 다양한 소스의 특성 값을 적용할 수 있습니다.

1. DAP 레코드
2. 사용자 이름
3. 그룹 정책
4. 연결 프로필에 대한 그룹 정책(터널 그룹)
5. 기본 그룹 정책

특성의 DAP 값은 사용자, 그룹 정책 또는 연결 프로필에 대해 구성된 값보다 우선순위가 높습니다.

DAP 레코드에 대한 특성을 활성화하거나 비활성화하면 ASA는 그 값을 강제적으로 적용합니다. 이를테면 dap webvpn 컨피그레이션 모드에서 파일 엔트리를 비활성화하면 ASA는 더 이상 값을 찾지 않습니다. 그 대신 **file-entry** 명령에 대해 어떤 값도 설정하지 않으면 그 특성은 DAP 레코드기 없으므로, ASA는 사용자 이름, 필요하다면 그룹 정책의 AAA 특성까지 내려와 적용할 값을 찾습니다.

예

다음 예에서는 Finance라는 DAP 레코드에 대해 파일 엔트리를 활성화하는 방법을 보여줍니다.

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# file-entry enable
ciscoasa(config-dap-webvpn)#
```

관련 명령

명령	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
file-browsing	파일 서버 또는 공유를 브라우징하는 기능을 활성화하거나 비활성화합니다.

filter

WebVPN 연결에서 이 그룹 정책 또는 사용자 이름을 위해 사용할 액세스 목록의 이름을 지정하려면 webvpn 컨피그레이션 모드에서 **filter** 명령을 사용합니다. 액세스 목록을 제거하려면 이 명령의 **no** 형식을 사용합니다.

filter {value *ACLname* **| none}**

no filter

구문 설명

none	WebVPN 유형 액세스 목록이 없음을 나타냅니다. null 값을 설정하여 액세스 목록을 허용하지 않습니다. 다른 그룹 정책에서 액세스 목록을 상속할 수 없게 합니다.
value *ACLname*	이전에 구성한 액세스 목록의 이름을 제공합니다.

기본값

WebVPN 액세스 목록은 **filter** 명령을 사용하여 지정할 때까지 적용되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

no 옵션은 다른 그룹 정책에서 값을 상속하는 것을 허용합니다. 필터 값을 상속할 수 없게 하려면 **filter value none** 명령을 사용합니다.

이 사용자 또는 그룹 정책에 대해 다양한 유형의 트래픽을 허용하거나 거부하도록 ACL을 구성합니다. 그런 다음 **filter** 명령을 사용하여 WebVPN 트래픽에 대해 이 ACL을 적용합니다.

WebVPN은 **vpn-filter** 명령에 정의된 ACL을 사용하지 않습니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 *acl_in*이라는 액세스 목록을 호출하는 필터를 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# filter acl_in
```

관련 명령

명령	설명
access-list	액세스 목록을 생성하거나 다운로드 가능한 액세스 목록을 사용합니다.
webvpn	group-policy 컨피그레이션 모드 또는 username 컨피그레이션 모드에서 사용합니다. 그룹 정책 또는 사용자 이름에 적용되는 매개변수를 구성하기 위해 webvpn 컨피그레이션 모드를 시작할 수 있게 합니다.

filter activex

ASA를 지나는 HTTP 트래픽에서 ActiveX 객체를 제거하려면 글로벌 컨피그레이션 모드에서 **filter activex** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

filter activex *port* **[-***port***] | except** *local_ip mask foreign_ip foreign_mask*

no filter activex *port* **[-***port***] | except** *local_ip mask foreign_ip foreign_mask*

구문 설명

except	이전 필터 조건에 대한 예외를 생성합니다.
foreign_ip	액세스 요청의 대상인 최하위 보안 레벨 인터페이스의 IP 주소. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
foreign_mask	*foreign_ip* 인수의 네트워크 마스크. 항상 특정 마스크 값을 지정합니다. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
local_ip	액세스 요청의 출처인 최상위 보안 레벨 인터페이스의 IP 주소. 이 주소를 0.0.0.0(또는 단축하여 0)으로 설정하여 모든 호스트를 지정할 수 있습니다.
mask	*local_ip* 인수의 네트워크 마스크. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
port	필터링이 적용되는 TCP 포트. 일반적으로 이는 포트 21이지만, 다른 값도 허용됩니다. 포트 21에 대해 http 또는 url 리터럴을 사용할 수 있습니다. 허용되는 값의 범위는 0~65535입니다.
-port	(선택 사항) 포트 범위를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ActiveX 객체는 보호되는 네트워크의 호스트 및 서버를 공격할 목적의 코드를 포함할 가능성이 있어 보안 위험이 될 수 있습니다. **filter activex** 명령으로 ActiveX 객체를 비활성화할 수 있습니다.

ActiveX 컨트롤(이전의 OLE 또는 OCX 컨트롤)은 웹 페이지 또는 기타 애플리케이션에 삽입할 수 있는 구성 요소입니다. 이러한 컨트롤으로는 사용자 지정 양식, 달력, 그 밖에 정보를 수집하거나 표시하는 광범위한 서드파티 양식 등이 있습니다. 기술적 관점에서 ActiveX는 워크스테이션 장애를 유발하거나 네트워크 보안 문제를 야기하거나 서버 공격에 이용되는 등 여러모로 네트워크 클라이언트에 문제가 될 수 있습니다.

filter activex 명령은 HTML 웹 페이지 내에서 HTML **object** 명령을 주석 처리하는 방법으로 이 명령을 차단합니다. HTML 파일의 ActiveX 필터링은 선별적으로 <applet>, </applet>, <object classid>, </object> 태그를 주석으로 대체하는 방식입니다. 중첩 태그의 필터링은 최상위 태그를 주석으로 전환합니다.

주의 <object> 태그는 Java 애플릿, 이미지 파일, 멀티미디어 객체에도 사용되는데, 이 역시 이 명령으로 차단됩니다.

<object> 또는 </object> HTML 태그가 여러 네트워크 패킷에 걸쳐 있는 경우 또는 태그의 코드가 MTU의 바이트 수보다 길 경우 ASA에서 태그를 차단할 수 없습니다.

사용자가 **alias** 명령에 의해 참조되는 IP 주소 또는 WebVPN 트래픽을 위한 IP 주소에 액세스할 경우 ActiveX 차단이 일어나지 않습니다 .

예

다음 예에서는 모든 아웃바운드 연결에서 ActiveX 객체가 차단되도록 지정합니다.

```
ciscoasa(config)# filter activex 80 0 0 0 0
```

이 명령은 임의의 로컬 호스트에서 보낸 포트 80의 웹 트래픽 및 임의의 외부 호스트와의 연결에 ActiveX 객체 차단을 적용하도록 지정합니다.

관련 명령

명령	설명
filter url	URL 필터링 서버로 트래픽을 전달합니다.
filter java	ASA를 지나는 HTTP 트래픽에서 Java 애플릿을 제거합니다.
show running-config filter	필터링 컨피그레이션을 표시합니다.
url-block	필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답에 사용할 URL 버퍼를 관리합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

filter ftp

Websense 또는 N2H2 서버에 의해 필터링될 FTP 트래픽을 식별하려면 글로벌 컨피그레이션 모드에서 **filter ftp** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

filter ftp *port* **[-***port***] | except** *local_ip mask foreign_ip foreign_mask* **[allow] [interact-block]**

no filter ftp *port* **[-***port***] | except** *local_ip mask foreign_ip foreign_mask* **[allow] [interact-block]**

구문 설명

allow	(선택 사항) 서버를 사용할 수 없을 때 아웃바운드 연결이 필터링 없이 ASA를 지나게 합니다. 이 옵션을 생략한 상태에서 N2H2 또는 Websense 서버의 연결이 끊기면 ASA는 N2H2 또는 Websense 서버가 다시 연결될 때까지 포트 80(웹) 트래픽을 차단합니다.
except	이전 필터 조건에 대한 예외를 생성합니다.
foreign_ip	액세스 요청의 대상인 최하위 보안 레벨 인터페이스의 IP 주소. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
foreign_mask	*foreign_ip* 인수의 네트워크 마스크. 항상 특정 마스크 값을 지정합니다. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
interact-block	(선택 사항) 사용자가 대화형 FTP 프로그램을 통해 FTP 서버에 연결할 수 없게 합니다.
local_ip	액세스 요청의 출처인 최상위 보안 레벨 인터페이스의 IP 주소. 이 주소를 0.0.0.0(또는 단축하여 0)으로 설정하여 모든 호스트를 지정할 수 있습니다.
mask	*local_ip* 인수의 네트워크 마스크. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
port	필터링이 적용되는 TCP 포트. 일반적으로 이는 포트 21이지만, 다른 값도 허용됩니다. 포트 80에 대해 ftp 리터럴을 사용할 수 있습니다.
-*port*	(선택 사항) 포트 범위를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

filter ftp 명령을 사용하면 Websense 또는 N2H2 서버에 의해 필터링될 FTP 트래픽을 식별할 수 있습니다.

이 기능을 활성화하면 사용자가 서버에 FTP GET 요청을 할 경우 ASA는 FTP 서버 및 Websense 또는 N2H2 서버에 동시에 요청을 보냅니다. Websense 또는 N2H2 서버가 연결을 허용하면 ASA는 성공 FTP 반환 코드가 변경되지 않은 채로 사용자에게 전달될 수 있게 합니다. 이를테면 성공 반환 코드가 "250: CWD command successful"입니다.

Websense 또는 N2H2 서버가 연결을 거부할 경우 ASA는 FTP 반환 코드를 수정하여 연결이 거부되었음을 알립니다. 이를테면 ASA는 코드 250을 "550 Requested file is prohibited by URL filtering policy"로 바꿉니다. Websense는 PUT 명령이 아닌 FTP GET 명령만 필터링합니다.

전체 디렉토리 경로를 제공하지 않는 대화형 FTP 세션을 차단하려면 **interactive-block** 옵션을 사용합니다. 대화형 FTP 클라이언트는 사용자가 전체 경로를 입력하지 않고도 디렉토리를 변경할 수 있게 합니다. 예를 들어, 사용자가 **cd /public/files** 대신 **cd ./files**를 입력할 수 있습니다. 이 명령을 사용하기 전에 URL 필터링 서버를 식별하고 활성화해야 합니다.

예

다음 예에서는 FTP 필터링을 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter ftp 21 0 0 0 0
ciscoasa(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

관련 명령

명령	설명
filter https	Websense 또는 N2H2 서버에 의해 필터링될 HTTPS 트래픽을 식별합니다.
filter java	ASA를 지나는 HTTP 트래픽에서 Java 애플릿을 제거합니다.
filter url	URL 필터링 서버로 트래픽을 전달합니다.
show running-config filter	필터링 컨피그레이션을 표시합니다.
url-block	필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답에 사용할 URL 버퍼를 관리합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

filter https

N2H2 또는 Websense 서버에 의해 필터링될 HTTPS 트래픽을 식별하려면 글로벌 컨피그레이션 모드에서 **filter https** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

filter https *port* **[-***port***] | except** *local_ip mask foreign_ip foreign_mask* **[allow]**

no filter https *port* **[-***port***] | except** *local_ip mask foreign_ip foreign_mask* **[allow]**

구문 설명

allow	(선택 사항) 서버를 사용할 수 없을 때 아웃바운드 연결이 필터링 없이 ASA를 지나게 합니다. 이 옵션을 생략한 상태에서 N2H2 또는 Websense 서버의 연결이 끊기면 ASA는 N2H2 또는 Websense 서버가 다시 연결될 때까지 포트 443 트래픽을 차단합니다.
except	(선택 사항) 이전 필터 조건에 대한 예외를 생성합니다.
foreign_ip	액세스 요청의 대상인 최하위 보안 레벨 인터페이스의 IP 주소. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
foreign_mask	*foreign_ip* 인수의 네트워크 마스크. 항상 특정 마스크 값을 지정합니다. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
local_ip	액세스 요청의 출처인 최상위 보안 레벨 인터페이스의 IP 주소. 이 주소를 0.0.0.0(또는 단축하여 0)으로 설정하여 모든 호스트를 지정할 수 있습니다.
mask	*local_ip* 인수의 네트워크 마스크. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
port	필터링이 적용되는 TCP 포트. 일반적으로 이는 포트 443이지만, 다른 값도 허용됩니다. 포트 443에 대해 https 리터럴을 사용할 수 있습니다.
-*port*	(선택 사항) 포트 범위를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA는 외부 Websense 또는 N2H2 필터링 서버를 사용하여 HTTPS 및 FTP 사이트의 필터링을 지원합니다.

HTTPS 필터링은 허용되지 않는 사이트에 대해서는 SSL 연결 협상을 완료할 수 없게 하는 방식입니다. 브라우저에서는 "The Page or the content cannot be displayed."와 같은 오류 메시지를 표시합니다.

HTTPS 콘텐츠는 암호화되므로 ASA는 디렉토리 및 파일 이름 정보 없이 URL 조회를 보냅니다.

예

다음 예에서는 10.0.2.54 호스트에서 보낸 것을 제외하고 모든 아웃바운드 HTTPS 연결을 필터링합니다.

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter https 443 0 0 0 0
ciscoasa(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

관련 명령

명령	설명
filter activex	ASA를 지나는 HTTP 트래픽에서 ActiveX 객체를 제거합니다.
filter java	ASA를 지나는 HTTP 트래픽에서 Java 애플릿을 제거합니다.
filter url	URL 필터링 서버로 트래픽을 전달합니다.
show running-config filter	필터링 컨피그레이션을 표시합니다.
url-block	필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답에 사용할 URL 버퍼를 관리합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

filter java

ASA를 지나는 HTTP 트래픽에서 Java 애플릿을 제거하려면 글로벌 컨피그레이션 모드에서 **filter java** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

filter java {[*port***[-***port***] | except }** *local_ip local_mask foreign_ip foreign_mask***]**

no filter java {[*port***[-***port***] | except }** *local_ip local_mask foreign_ip foreign_mask***]**

구문 설명

except	(선택 사항) 이전 필터 조건에 대한 예외를 생성합니다.
foreign_ip	액세스 요청의 대상인 최하위 보안 레벨 인터페이스의 IP 주소. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
foreign_mask	*foreign_ip* 인수의 네트워크 마스크. 항상 특정 마스크 값을 지정합니다. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
local_ip	액세스 요청의 출처인 최상위 보안 레벨 인터페이스의 IP 주소. 이 주소를 0.0.0.0(또는 단축하여 0)으로 설정하여 모든 호스트를 지정할 수 있습니다.
local_mask	*local_ip* 인수의 네트워크 마스크. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
port	필터링이 적용되는 TCP 포트. 일반적으로 이는 포트 80이지만, 다른 값도 허용됩니다. 포트 80에 대해 http 또는 url 리터럴을 사용할 수 있습니다.
*port***-***port*	(선택 사항) 포트 범위를 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

Java 애플릿은 보호되는 네트워크의 호스트 및 서버를 공격할 목적의 코드를 포함할 가능성이 있어 보안 위험이 될 수 있습니다. **filter java** 명령으로 Java 애플릿을 제거할 수 있습니다.

filter java 명령은 아웃바운드 연결에서 ASA으로 반환되는 Java 애플릿을 필터링합니다. 사용자는 계속 HTML 페이지를 수신하지만, 애플릿의 웹 페이지 소스가 주석 처리되어 애플릿이 실행되지 않습니다. **filter java** 명령은 WebVPN 트래픽을 필터링하지 않습니다.

<applet> 또는 </applet> HTML 태그가 여러 네트워크 패킷에 걸쳐 있는 경우 또는 태그의 코드가 MTU의 바이트 수보다 길 경우 ASA에서 태그를 차단할 수 없습니다. Java 애플릿이 <object> 태그로 묶여 있는 것이 확실하다면 **filter activex** 명령을 사용하여 제거합니다.

예

다음 예에서는 모든 아웃바운드 연결에서 Java 애플릿이 차단되도록 지정합니다.

```
ciscoasa(config)# filter java 80 0 0 0 0
```

다음 예에서는 임의의 로컬 호스트에서 보낸 포트 80의 웹 트래픽 및 임의의 외부 호스트와의 연결에 Java 애플릿 차단을 적용하도록 지정합니다.

다음 예에서는 보호되는 네트워크의 호스트에서 Java 애플릿의 다운로드를 차단합니다.

```
ciscoasa(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

관련 명령

명령	설명
filter activex	ASA를 지나는 HTTP 트래픽에서 ActiveX 객체를 제거합니다.
filter url	URL 필터링 서버로 트래픽을 전달합니다.
show running-config filter	필터링 컨피그레이션을 표시합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

filter url

URL 필터링 서버에 트래픽을 전달하려면 글로벌 컨피그레이션 모드에서 **filter url** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

filter url *port* **[-***port***] | except** *local_ip local_mask foreign_ip foreign_mask* **[allow] [cgi-truncate] [longurl-truncate | longurl-deny] [proxy-block]**

no filter url *port* **[-***port***] | except** *local_ip mask foreign_ip foreign_mask* **[allow] [cgi-truncate] [longurl-truncate | longurl-deny] [proxy-block]**

구문 설명

allow	서버를 사용할 수 없을 때 아웃바운드 연결이 필터링 없이 ASA를 지나게 합니다. 이 옵션을 생략한 상태에서 N2H2 또는 Websense 서버의 연결이 끊기면 ASA는 N2H2 또는 Websense 서버가 다시 연결될 때까지 포트 80(웹) 트래픽을 차단합니다.
cgi_truncate	URL에 물음표로 시작하는 매개변수 목록이 있을 경우(예: CGI 스크립트), 물음표와 그 다음에 나오는 모든 문자를 제거하는 방식으로 필터링 서버에 보낼 URL을 자릅니다.
except	이전 **filter** 조건에 대한 예외를 생성합니다.
foreign_ip	액세스 요청의 대상인 최하위 보안 레벨 인터페이스의 IP 주소. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
foreign_mask	*foreign_ip* 인수의 네트워크 마스크. 항상 특정 마스크 값을 지정합니다. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
HTTP	포트 80을 지정합니다. 80 대신 http 또는 www를 입력하여 포트 80을 지정할 수 있습니다.
local_ip	액세스 요청의 출처인 최상위 보안 레벨 인터페이스의 IP 주소. 이 주소를 0.0.0.0(또는 단축하여 0)으로 설정하여 모든 호스트를 지정할 수 있습니다.
local_mask	*local_ip* 인수의 네트워크 마스크. 0.0.0.0(또는 단축하여 0)을 사용하여 모든 호스트를 지정할 수 있습니다.
longurl-deny	URL이 URL 버퍼 크기 한도를 초과하거나 URL 버퍼를 사용할 수 없을 경우 URL 요청을 거부합니다.
longurl-truncate	URL이 URL 버퍼 한도를 초과할 경우 발신 호스트 이름 또는 IP 주소만 N2H2 또는 Websense 서버에 보냅니다.
-port	(선택 사항) 필터링이 적용되는 TCP 포트. 일반적으로 이는 포트 80이지만, 다른 값도 허용됩니다. 포트 80에 대해 http 또는 url 리터럴을 사용할 수 있습니다. 선택적으로 하이픈 다음에 제2 포트를 추가하여 포트의 범위를 식별할 수 있습니다.
proxy-block	사용자가 HTTP 프록시 서버에 연결할 수 없게 합니다.
url	ASA를 지나는 데이터에서 URL을 필터링합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

filter url 명령을 사용하면 N2H2 또는 Websense 필터링 애플리케이션으로 지정하는 WWW URL에 아웃바운드 사용자가 액세스하는 것을 막을 수 있습니다.

참고 **url-server** 명령이 구성된 다음에 **filter url** 명령을 실행해야 합니다.

filter url 명령의 **allow** 옵션은 N2H2 또는 Websense 서버의 연결이 끊길 때 ASA가 어떻게 동작할지 결정합니다. **allow** 옵션을 **filter url** 명령과 함께 사용할 경우 N2H2 또는 Websense 서버의 연결이 끊기면 포트 80 트래픽은 필터링 없이 ASA를 지납니다. **allow** 옵션 없이 사용할 경우 서버의 연결이 끊기면 ASA는 서버가 다시 연결될 때까지 아웃바운드 포트 80(웹) 트래픽을 차단합니다. 또는 다른 URL 서버가 사용 가능할 경우 다음 URL 서버에 제어 권한을 넘깁니다.

참고 **allow** 옵션이 설정된 경우, N2H2 또는 Websense 서버의 연결이 끊기면 ASA는 대체 서버에 제어 권한을 넘깁니다.

N2H2 또는 Websense 서버는 ASA와 연계하면서 회사 보안 정책에 따라 사용자의 웹 사이트 액세스를 거부합니다.

필터링 서버 사용

Websense 프로토콜 버전 4는 호스트와 ASA 간의 그룹 및 사용자 이름 인증을 활성화합니다. ASA에서 사용자 이름 조회를 수행한 다음 Websense 서버가 URL 필터링 및 사용자 이름 로깅을 처리합니다.

N2H2 서버는 IFP Server를 실행하는 Windows 워크스테이션(2000, NT 또는 XP)이어야 하며, 512MB 이상의 RAM이 권장됩니다. 또한 N2H2 서비스를 위한 긴 URL 지원의 한도는 3KB로 Websense의 한도보다 적습니다.

Websense 프로토콜 버전 4는 다음과 같이 향상되었습니다.

- URL 필터링에서는 ASA가 Websense 서버에 정의된 정책을 사용하여 발신 URL 요청을 확인할 수 있게 합니다.
- 사용자 이름 로깅은 Websense 서버의 사용자 이름, 그룹, 도메인 이름을 추적합니다.
- 사용자 이름 조회를 통해 ASA는 사용자 인증 테이블을 사용하여 호스트의 IP 주소를 사용자 이름에 매핑할 수 있습니다.

Websense에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.

http://www.websense.com/

컨피그레이션 절차

다음 단계에 따라 URL을 필터링합니다.

1. 해당 벤더의 **url-server** 명령 버전을 사용하여 N2H2 또는 Websense 서버를 지정합니다.
2. **filter** 명령으로 필터링을 활성화합니다.
3. 필요하다면 **url-cache** 명령으로 처리량을 늘립니다. 그러나 이 명령은 Websense 어카운팅 보고서에 영향을 미칠 수 있는 Websense 로그를 업데이트하지 않습니다. **url-cache** 명령을 사용하기 전에 Websense 실행 로그를 취합합니다.
4. 실행 정보를 보려면 **show url-cache statistics** 및 **show perfmon** 명령을 사용합니다.

긴 URL 사용

Websense 필터링 서버에서는 최대 4KB의 URL 필터링이, N2H2 필터링 서버에서는 최대 3KB가 지원됩니다.

허용된 최대 길이보다 긴 URL 요청의 처리를 허용하려면 **longurl-truncate** 및 **cgi-truncate** 옵션을 사용합니다.

URL이 최대 길이보다 길 경우, **longurl-truncate** 또는 **longurl-deny** 옵션을 활성화하지 않았다면 ASA는 패킷을 삭제합니다.

longurl-truncate 옵션은 URL이 허용된 최대 길이보다 길 경우 ASA에서 필터링 서버에 평가를 위해 보낼 때 URL의 호스트 이름 또는 IP 주소 부분만 보내게 합니다. URL이 허용된 최대 길이보다 길 경우 아웃바운드 URL 트래픽을 거부하려면 **longurl-deny** 옵션을 사용합니다.

CGI URL을 잘라 매개변수 없이 CGI 스크립트 위치 및 스크립트 이름만 포함하게 하려면 **cgi-truncate** 옵션을 사용합니다. 긴 HTTP 요청 중 상당수는 CGI 요청입니다. 매개변수 목록이 매우 길 경우, 기다렸다가 매개변수 목록을 포함한 전체 CGI 요청을 보낸다면 메모리 리소스를 소진하고 ASA의 성능에 영향을 미칠 수 있습니다.

HTTP 응답 버퍼링

기본적으로 사용자가 특정 웹 사이트와의 연결을 요청하면 ASA는 웹 서버와 필터링 서버에 동시에 요청을 보냅니다. 필터링 서버가 웹 콘텐츠 서버보다 먼저 응답하지 않을 경우 웹 서버의 응답이 삭제됩니다. 그러면 웹 클라이언트의 입장에서는 웹 서버의 응답이 지연되는 것입니다.

HTTP 응답 버퍼를 활성화하면 웹 콘텐츠 서버의 회신이 버퍼링되고, 필터링 서버가 연결을 허용할 경우 그 응답이 요청한 사용자에게 전달됩니다. 따라서 만일의 지연을 방지할 수 있습니다.

HTTP 응답 버퍼를 활성화하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# url-block block block-buffer-limit
```

block-buffer-limit 인수를 버퍼링될 최대 블록 수로 대체합니다. 사용 가능한 값은 1부터 128까지이며, 이는 한 번에 버퍼링할 수 있는 1550바이트 블록의 수입니다.

예

다음 예에서는 10.0.2.54 호스트에서 보낸 것을 제외하고 모든 아웃바운드 HTTP 연결을 필터링합니다.

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter url 80 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

다음 예에서는 포트 8080에서 수신하는 프록시 서버로 향하는 모든 아웃바운드 HTTP 연결을 차단합니다.

```
ciscoasa(config)# filter url 8080 0 0 0 0 proxy-block
```

관련 명령

명령	설명
filter activex	ASA를 지나는 HTTP 트래픽에서 ActiveX 객체를 제거합니다.
filter java	ASA를 지나는 HTTP 트래픽에서 Java 애플릿을 제거합니다.
url-block	필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답에 사용할 URL 버퍼를 관리합니다.
url-cache	N2H2 또는 Websense 서버의 응답을 보류한 상태에서 URL 캐싱을 활성화하고 캐시의 크기를 설정합니다.
url-server	**filter** 명령과 함께 사용할 N2H2 또는 Websense 서버를 식별합니다.

fips enable

시스템 또는 모듈에 대한 FIPS 규정준수를 적용하는 정책 확인을 활성화하려면 글로벌 컨피그레이션 모드에서 **fips enable** 명령을 사용합니다. 정책 확인을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

fips enable

no fips enable

구문 설명

enable	FIPS 규정준수를 적용하기 위한 정책 확인을 활성화하거나 비활성화합니다.

기본값

이 명령은 기본 설정이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(4)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

FIPS 규정준수 작업 모드에서 실행하려면 **fips enable** 명령과 보안 정책에 지정된 정확한 컨피그레이션을 모두 적용해야 합니다. 내부 API는 디바이스가 런타임에 정확한 컨피그레이션을 적용하도록 마이그레이션할 수 있게 합니다.

FIPS 규정준수 모드가 시작 컨피그레이션에 있으면 FIPS POST(power-on self-tests)가 실행되고 다음 콘솔 메시지를 인쇄합니다.

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

                Cisco Systems, Inc.
                170 West Tasman Drive
                San Jose, California 95134-1706

....
```

```
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

예

다음은 시스템에서 FIPS 규정준수를 적용하기 위한 정책 확인을 보여줍니다.

```
ciscoasa(config)# fips enable
```

관련 명령

명령	설명
clear configure fips	NVRAM에 저장된 시스템 또는 모듈 FIPS 컨피그레이션 정보를 지웁니다.
crashinfo console disable	플래시에 대한 크래시 쓰기 정보의 읽기, 쓰기, 컨피그레이션을 비활성화합니다.
fips self-test poweron	POST를 실행합니다.
show crashinfo console	플래시에 대한 크래시 쓰기를 읽고 쓰고 구성합니다.
show running-config fips	ASA에서 실행 중인 FIPS 컨피그레이션을 표시합니다.

fips self-test poweron

POST를 실행하려면 특별 권한 EXEC 모드에서 **fips self-test powereon** 명령을 사용합니다.

fips self-test poweron

구문 설명

poweron	POST를 실행합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(4)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

이 명령을 입력하면 디바이스에서 FIPS 140-2 규정준수에 필요한 모든 자체 테스트를 실행합니다. 이 테스트에는 암호화 알고리즘 테스트, 소프트웨어 무결성 테스트, 주요 기능 테스트가 포함됩니다.

예

다음 예에서는 시스템에서 POST를 실행하는 것을 보여줍니다.

```
ciscoasa(config)# fips self-test poweron
```

관련 명령

명령	설명
clear configure fips	NVRAM에 저장된 시스템 또는 모듈 FIPS 컨피그레이션 정보를 지웁니다.
crashinfo console disable	플래시에 대한 크래시 쓰기 정보의 읽기, 쓰기, 컨피그레이션을 비활성화합니다.
fips enable	시스템 또는 모듈에서 FIPS 규정준수를 적용하기 위한 정책 확인을 활성화하거나 비활성화합니다.
show crashinfo console	플래시에 대한 크래시 쓰기를 읽고 쓰고 구성합니다.
show running-config fips	ASA에서 실행 중인 FIPS 컨피그레이션을 표시합니다.

firewall transparent

방화벽 모드를 투명 모드로 설정하려면 글로벌 컨피그레이션 모드에서 **firewall transparent** 명령을 사용합니다. 라우티드 모드를 복원하려면 이 명령의 **no** 형식을 사용합니다.

firewall transparent

no firewall transparent

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

기본값

기본적으로 ASA는 라우티드 모드에 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.5(1)/9.0(1)	다중 컨텍스트 모드에서 컨텍스트별로 이를 설정할 수 있습니다.

사용 지침

투명 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

다중 컨텍스트 모드에서 컨텍스트별로 이 명령을 설정할 수 있습니다.

모드를 변경할 경우, 다수의 명령이 양쪽 모드에서 모두 지원되지 않으므로 ASA에서는 컨피그레이션을 지웁니다. 컨피그레이션이 이미 채워져 있는 경우 모드를 변경하기 전에 해당 컨피그레이션을 백업하십시오. 새 컨피그레이션을 생성할 때 이러한 백업을 참조할 수 있습니다.

firewall transparent 명령으로 모드를 변경하는 텍스트 컨피그레이션을 ASA에 다운로드할 경우, 컨피그레이션의 맨 위에 해당 명령을 입력해야 합니다. ASA에서는 이 명령을 읽는 즉시 모드를 변경한 다음 다운로드된 컨피그레이션을 계속 읽습니다. 명령이 컨피그레이션에서 뒤쪽에 나타날 경우 ASA에서는 컨피그레이션에서 앞에 있던 모든 줄을 지웁니다.

예

다음 예에서는 방화벽 모드를 투명으로 변경합니다.

```
ciscoasa(config)# firewall transparent
```

관련 명령

명령	설명
arp-inspection	ARP 패킷을 고정 ARP 엔트리와 비교하는 ARP 검사를 활성화합니다.
mac-address-table static	고정 MAC 주소 엔트리를 MAC 주소 테이블에 추가합니다.
mac-learn	MAC 주소 파악을 비활성화합니다.
show firewall	방화벽 모드를 표시합니다.
show mac-address-table	동적 및 고정 엔트리를 포함하여 MAC 주소 테이블을 표시합니다.

firewall vlan-group(IOS)

방화벽 그룹에 VLAN을 지정하려면 글로벌 컨피그레이션 모드에서 **firewall vlan-group** 명령을 입력합니다. VLAN을 제거하려면 이 명령의 **no** 형식을 사용합니다.

firewall vlan-group *firewall_group vlan_range*

no firewall vlan-group *firewall_group vlan_range*

구문 설명

firewall_group	그룹 ID를 정수로 지정합니다.
vlan_range	그룹에 지정된 VLAN을 나타냅니다. *vlan_range*는 다음 방법 중 하나로 식별되는 하나 이상의 VLAN(2~1000, 1025~ 4094)일 수 있습니다. • 단일 번호(*n*) • 범위(*n-x*) 번호 또는 범위는 쉼표로 구분합니다. 이를테면 다음 번호를 입력합니다. `5,7-10,13,45-100` **참고** 라우티드 포트와 WAN 포트는 내부 VLAN 을 사용하므로 , 1020~1100 범위의 VLAN 이 이미 사용 중인 가능성이 있습니다 .

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

Cisco IOS 소프트웨어에서 **firewall vlan-group** 명령을 사용하여 최대 16개의 방화벽 VLAN 그룹을 만든 다음 그 그룹을 ASA에 지정합니다(**firewall module** 명령 사용). 예를 들어, 모든 VLAN을 하나의 그룹에 지정하거나 내부 그룹과 외부 그룹을 만들거나 고객별로 그룹을 만들 수도 있습니다. 각 그룹은 무제한 VLAN을 포함할 수 있습니다.

동일한 VLAN을 여러 방화벽 그룹에 지정할 수 없습니다. 그러나 여러 방화벽 그룹을 ASA에 지정하고 단일 방화벽 그룹을 여러 ASA에 지정할 수 있습니다. 예를 들어, 여러 ASA에 지정할 VLAN은 각 ASA에 고유하게 지정될 VLAN과 다른 그룹에 상주할 수 있습니다.

예

다음 예에서는 3개의 방화벽 VLAN 그룹을 생성하는 방법을 보여줍니다. ASA마다 하나씩 지정되며, VLAN을 포함하는 방화벽은 두 ASA에 지정됩니다.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

다음은 **show firewall vlan-group** 명령의 샘플 출력입니다.

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

다음은 **show firewall module** 명령의 샘플 출력이며, 모든 VLAN 그룹을 보여줍니다.

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

관련 명령

명령	설명
firewall module	ASA에 VLAN 그룹을 지정합니다.
show firewall vlan-group	VLAN 그룹 및 여기에 지정된 VLAN을 표시합니다.
show module	설치된 모듈을 모두 표시합니다.

flow-export active refresh-interval

flow-update 이벤트 간의 시간 간격을 지정하려면 글로벌 컨피그레이션 모드에서 **flow-export active refresh-interval** 명령을 사용합니다.

flow-export active refresh-interval *value*

구문 설명

value	flow-update 이벤트의 시간 간격(분)을 지정합니다. 유효한 값은 1분~60분입니다.

기본값

기본값은 1분입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.1(2)	이 명령을 도입했습니다.

사용 지침

이미 **flow-export delay flow-create** 명령을 구성한 상태에서 **flow-export active refresh-interval** 명령을 지연 시간보다 5초 이상 길지 않은 간격 값과 함께 구성할 경우, 다음 경고 메시지가 콘솔에 나타납니다.

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

이미 **flow-export active refresh-interval** 명령을 구성한 상태에서 **flow-export delay flow-create** 명령을 간격 값보다 5초 이상 짧지 않은 지연 시간의 값과 함께 구성할 경우 다음 경고 메시지가 콘솔에 나타납니다.

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

예

다음 예에서는 30분의 시간 간격을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# flow-export active refresh-interval 30
```

관련 명령

명령	설명
clear flow-export counters	NetFlow의 모든 런타임 카운터를 0으로 재설정합니다.
flow-export destination	NetFlow 컬렉터의 IP 주소 또는 호스트 이름 및 NetFlow 컬렉터가 수신하는 UDP 포트를 지정합니다.
flow-export template timeout-rate	템플릿 정보가 NetFlow 컬렉터에 보내지는 간격을 제어합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 다음 표시되는 syslog 메시지 및 NetFlow 데이터와 관련된 syslog 메시지를 활성화합니다.
show flow-export counters	NetFlow를 위한 런타임 카운터 집합을 표시합니다.

flow-export delay flow-create

flow-create 이벤트 내보내기를 늦추려면 글로벌 컨피그레이션 모드에서 **flow-export delay flow-create** 명령을 사용합니다. 지연 없이 flow-create 이벤트를 내보내려면 이 명령의 **no** 형식을 사용합니다.

flow-export delay flow-create *seconds*

no flow-export delay flow-create *seconds*

구문 설명

seconds	flow-create 이벤트 내보내기의 지연 시간(초)을 지정합니다. 유효한 값은 1초~180초입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.1(2)	이 명령을 도입했습니다.

사용 지침

flow-export delay flow-create 명령이 구성되지 않을 경우 flow-create 이벤트는 지연 없이 내보내집니다.

구성된 지연 시간보다 일찍 플로우가 해제될 경우 flow-create 이벤트가 전송되지 않습니다. 그 대신 extended flow teardown 이벤트가 전송됩니다.

예

다음 예에서는 flow-create 이벤트의 내보내기를 10초 늦추는 방법을 보여줍니다.

```
ciscoasa(config)# flow-export delay flow-create 10
```

관련 명령

명령	설명
clear flow-export counters	NetFlow의 모든 런타임 카운터를 0으로 재설정합니다.
flow-export destination	NetFlow 컬렉터의 IP 주소 또는 호스트 이름 및 NetFlow 컬렉터가 수신하는 UDP 포트를 지정합니다.
flow-export template timeout-rate	템플릿 정보가 NetFlow 컬렉터에 보내지는 간격을 제어합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 다음 표시되는 syslog 메시지 및 NetFlow 데이터와 관련된 syslog 메시지를 활성화합니다.
show flow-export counters	NetFlow를 위한 런타임 카운터 집합을 표시합니다.

flow-export destination

NetFlow 패킷이 향하는 컬렉터를 구성하려면 글로벌 컨피그레이션 모드에서 **flow-export destination** 명령을 사용합니다. NetFlow 패킷의 컬렉터를 제거하려면 이 명령의 **no** 형식을 사용합니다.

flow-export destination *interface-name ipv4-address* | *hostname udp-port*

no flow-export destination *interface-name ipv4-address* | *hostname udp-port*

구문 설명

hostname	NetFlow 컬렉터의 호스트 이름을 지정합니다.
interface-name	목적지에 도착하기 위해 지날 인터페이스의 이름을 지정합니다.
ipv4-address	NetFlow 컬렉터의 IP 주소를 지정합니다. IPv4만 지원됩니다.
udp-port	NetFlow 컬렉터가 수신하는 UDP 포트를 지정합니다. 유효한 값은 1~65535입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.1(1)	이 명령을 도입했습니다.
8.1(2)	플로우 내보내기 목적지의 최대 개수가 5개로 늘어났습니다.

사용 지침

flow-export destination 명령을 사용하여 ASA에서 NetFlow 컬렉터에 NetFlow 데이터를 내보내도록 구성할 수 있습니다.

참고 보안 컨텍스트당 최대 5개의 내보내기 목적지(컬렉터)를 입력할 수 있습니다. 새 목적지를 입력하면 템플릿 레코드가 새로 추가된 컬렉터에 보내집니다. 5개보다 많은 목적지를 추가하려 하면 다음 오류 메시지가 나타납니다.

"ERROR: A maximum of 5 flow-export destinations can be configured."

ASA에서 NetFlow 데이터를 내보내도록 구성된 경우, 성능 향상을 위해 **logging flow-export-syslogs disable** 명령을 입력하여 이중 syslog 메시지(NetFlow에서도 캡처하는 메시지)를 비활성화하는 것이 좋습니다.

예

다음 예에서는 NetFlow 데이터를 위해 컬렉터를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# flow-export destination inside 209.165.200.224 2055
```

관련 명령

명령	설명
clear flow-export counters	NetFlow의 모든 런타임 카운터를 0으로 재설정합니다.
flow-export delay flow-create	flow-create 이벤트 내보내기를 지정된 시간만큼 늦춥니다.
flow-export template timeout-rate	템플릿 정보가 NetFlow 컬렉터에 보내지는 간격을 제어합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 다음 표시되는 syslog 메시지 및 NetFlow 데이터와 관련된 syslog 메시지를 활성화합니다.
show flow-export counters	NetFlow를 위한 런타임 카운터 집합을 표시합니다.

flow-export event-type destination

각 컬렉터에 어떤 NetFlow 레코드를 보내야 하는지 결정하기 위해 NetFlow 컬렉터 및 필터의 주소를 구성하려면 policy-map 클래스 컨피그레이션 모드에서 **flow-export event-type destination** 명령을 사용합니다. NetFlow 컬렉터 및 필터의 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

flow-export event-type {all | flow-create | flow-denied | flow-update | flow-teardown} destination

no flow-export event-type {all | flow-create | flow-denied | flow-update | flow-teardown} destination

구문 설명

all	4가지 이벤트 유형을 모두 지정합니다.
flow-create	flow-create 이벤트를 지정합니다.
flow-denied	flow-denied 이벤트를 지정합니다.
flow-teardown	flow-teardown 이벤트를 지정합니다.
flow-update	flow-update 이벤트를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Policy-map 클래스 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.1(2)	이 명령을 도입했습니다.

사용 지침

NetFlow 이벤트는 Modular Policy Framework를 통해 구성됩니다. Modular Policy Framework가 NetFlow를 위해 구성되지 않을 경우 어떤 이벤트도 로깅되지 않습니다. 클래스가 구성된 순서에 따라 트래픽이 매칭됩니다. 일치하는 항목을 찾으면 다른 클래스는 확인하지 않습니다. NetFlow 이벤트의 구성 요구 사항은 다음과 같습니다.

- flow-export 목적지(즉 NetFlow 컬렉터)는 그 IP 주소에 의해 고유하게 식별됩니다.
- 지원되는 이벤트 유형은 flow-create, flow-teardown, flow-denied, flow-update, all입니다. all은 앞의 4가지 이벤트 유형을 모두 포함하는 것입니다.
- Flow-export 작업은 인터페이스 정책에서 지원되지 않습니다.
- Flow-export 작업은 **class-default** 명령에서 그리고 **match any** 또는 **match access-list** 명령이 있는 클래스에서만 지원됩니다.

- 어떤 NetFlow 컬렉터도 정의되지 않은 경우 어떤 구성 작업도 일어나지 않습니다.
- NetFlow Secure Event Logging 필터링은 순서와 상관없습니다.

참고 유효한 NetFlow 컨피그레이션을 만들려면 flow-export 목적지 컨피그레이션과 flow-export event-type 컨피그레이션이 모두 필요합니다. flow-export 목적지 컨피그레이션만으로는 아무 것도 할 수 없습니다. flow-export event-type 컨피그레이션을 위한 클래스 맵도 구성해야 합니다. 기본 클래스 맵으로 하거나 사용자가 만들 수 있습니다.

예

다음 예에서는 호스트 10.1.1.1과 20.1.1.1 간의 모든 NetFlow 이벤트를 목적지 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
clear flow-export counters	NetFlow의 모든 런타임 카운터를 0으로 재설정합니다.
flow-export delay flow-create	flow-create 이벤트 내보내기를 지정된 시간만큼 늦춥니다.
flow-export template timeout-rate	템플릿 정보가 NetFlow 컬렉터에 보내지는 간격을 제어합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 다음 표시되는 syslog 메시지 및 NetFlow 데이터와 관련된 syslog 메시지를 활성화합니다.
show flow-export counters	NetFlow를 위한 런타임 카운터 집합을 표시합니다.

flow-export template timeout-rate

템플릿 정보가 NetFlow 컬렉터에 보내지는 간격을 제어하려면 글로벌 컨피그레이션 모드에서 **flow-export template timeout-rate** 명령을 사용합니다. 템플릿 시간 초과를 기본값으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

flow-export template timeout-rate *minutes*

no flow-export template timeout-rate *minutes*

구문 설명

minutes	간격(분)을 지정합니다. 유효한 값은 1분~3600분입니다.
template	내보내기 템플릿을 구성하는 데 **timeout-rate** 키워드를 활성화합니다.
timeout-rate	템플릿이 처음 전송된 후 재전송될 때까지 경과한 시간(간격)을 지정합니다.

기본값

이 간격의 기본값은 30분입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.1(1)	이 명령을 도입했습니다.

사용 지침

사용되는 컬렉터에 따라 그리고 컬렉터에서 예상하는 템플릿의 새로 고침 속도로 시간 초과 비율을 구성해야 합니다.

보안 어플라이언스에서 NetFlow 데이터를 내보내도록 구성된 경우, 성능 향상을 위해 **logging flow-export-syslogs disable** 명령을 입력하여 이중 syslog 메시지(NetFlow에서도 캡처하는 메시지)를 비활성화하는 것이 좋습니다.

예

다음 예에서는 NetFlow에서 60분마다 모든 컬렉터에 템플릿 레코드를 보내도록 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# flow-export template timeout-rate 60
```

관련 명령

명령	설명
clear flow-export counters	NetFlow 데이터와 관련된 모든 런타임 카운터를 재설정합니다.
flow-export destination	NetFlow 컬렉터의 IP 주소 또는 호스트 이름 및 NetFlow 컬렉터가 수신하는 UDP 포트를 지정합니다.
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** 명령을 입력한 다음 표시되는 syslog 메시지 및 NetFlow 데이터와 관련된 syslog 메시지를 활성화합니다.
show flow-export counters	NetFlow를 위한 런타임 카운터 집합을 표시합니다.

flowcontrol

흐름 제어를 위해 일시 중지(XOFF) 프레임을 활성화하려면 인터페이스 컨피그레이션 모드에서 **flowcontrol** 명령을 사용합니다. 일시 중지 프레임을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

flowcontrol send on [*low_water high_water pause_time***] [noconfirm]**

no flowcontrol send on [*low_water high_water pause_time***] [noconfirm]**

구문 설명

high_water	최고 수위를 10GigabitEthernet은 0KB~511KB, 1GigabitEthernet은 0KB~47KB(4GE-SSM의 GigabitEthernet 인터페이스라면 0KB~11KB)의 범위에서 설정합니다. 버퍼 사용량이 최고 수위를 초과하면 NIC가 일시 중지 프레임을 보냅니다.
low_water	최저 수위를 10GigabitEthernet은 0KB~511KB, 1GigabitEthernet은 0KB~47KB(4GE-SSM의 GigabitEthernet 인터페이스라면 0KB~11KB)의 범위에서 설정합니다. NIC(네트워크 인터페이스 컨트롤러)에서 일시 중지 프레임을 보낸 다음 버퍼 사용량이 최저 수위 아래로 떨어지면 NIC는 XON 프레임을 보냅니다. 연결 파트너가 XON 프레임을 받은 후 트래픽을 다시 시작할 수 있습니다.
noconfirm	확인 없이 명령을 적용합니다. 이 명령이 인터페이스를 재설정하므로, 이 옵션을 사용하지 않으면 컨피그레이션 변경을 확인하는 메시지가 표시됩니다.
pause_time	일시 중지 새로 고침 임계값을 0슬롯~65535슬롯에서 설정합니다. 각 슬롯은 64바이트를 전송하는 데 걸리는 시간입니다. 따라서 유닛당 시간은 연결 속도에 좌우됩니다. 연결 파트너는 XON을 수신한 후 또는 XOFF가 만료된 후 일시 중지 프레임의 이 타이머 값에 따라 트래픽을 다시 시작할 수 있습니다. 버퍼 사용량이 지속적으로 최고 수위를 넘을 경우, 일시 중지 프레임이 반복해서 전송되며 이는 일시 중지 새로 고침 임계값에 의해 제어됩니다. 기본값은 26624입니다.

명령 기본값

일시 중지 프레임은 기본적으로 비활성화되어 있습니다.

10GigabitEthernet의 경우 다음 기본 설정을 참조하십시오.

- 기본 최고 수위는 128KB입니다.
- 기본 최저 수위는 64KB입니다.
- 일시 중지 새로 고침 임계값의 기본값은 26624슬롯입니다.

1GigabitEthernet의 경우 다음 기본 설정을 참조하십시오.

- 기본 최고 수위는 24KB입니다.
- 기본 최저 수위는 16KB입니다.
- 일시 중지 새로 고침 임계값의 기본값은 26624슬롯입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(2)	ASA 5580의 10GigabitEthernet 인터페이스에서 이 명령을 도입했습니다.
8.2(3)	ASA 5585-X 지원을 추가했습니다.
8.2(5)/8.4(2)	모든 모델에서 1GigabitEthernet 인터페이스 지원을 추가했습니다.

사용 지침

이 명령은 1GigabitEthernet 및 10GigabitEthernet 인터페이스에서 지원됩니다. 이 명령은 관리 인터페이스를 지원하지 않습니다.

물리적 인터페이스에 대해 이 명령을 입력합니다.

트래픽 버스트가 있을 경우 이러한 버스트가 NIC에서 FIFO 버퍼의 버퍼링 용량을 초과하고 링 버퍼를 수신하면 패킷 손실이 발생할 수 있습니다. 흐름 제어를 위한 일시 중지 프레임을 활성화하면 이러한 문제를 완화할 수 있습니다.

이 명령을 활성화하면 일시 중지(XOFF) 및 XON 프레임은 FIFO 버퍼 사용량을 기준으로 NIC 하드웨어에서 자동으로 생성됩니다.

1. 버퍼 사용량이 최고 수위를 초과하면 NIC가 일시 중지 프레임을 보냅니다.
2. 일시 중지를 보낸 후 버퍼 사용량이 최저 수위 아래로 감소하면 NIC는 XON 프레임을 보냅니다.
3. 연결 파트너는 XON을 수신한 후 또는 XOFF가 만료된 후 일시 중지 프레임의 타이머 값에 따라 트래픽을 다시 시작할 수 있습니다.
4. 버퍼 사용량이 지속적으로 최고 수위를 넘을 경우, NIC는 일시 중지 프레임을 반복해서 전송하며, 이는 일시 중지 새로 고침 임계값에 의해 제어됩니다.

이 명령을 사용할 때 다음과 같은 경고 메시지가 표시됩니다.

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

메시지 없이 매개변수를 변경하려면 **noconfirm** 키워드를 사용합니다.

참고 802.3x 에 정의된 흐름 제어 프레임만 지원됩니다 . 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다 .

예

다음 예에서는 기본 설정을 사용하여 일시 중지 프레임을 활성화합니다.

```
ciscoasa(config)# interface tengigabitethernet 1/0
ciscoasa(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
ciscoasa(config-if)# y
```

관련 명령

명령	설명
interface	인터페이스 컨피그레이션 모드를 시작합니다.

format

모든 파일을 지우고 파일 시스템을 포맷하려면 특별 권한 EXEC 모드에서 **format** 명령을 사용합니다.

format {disk0: | disk1: | flash:}

구문 설명

disk0*:*	내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다.
disk1:	외부 플래시 메모리 카드를 지정하고 그 다음에 콜론을 표시합니다.
flash:	내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다. ASA 5500 시리즈에서는 **flash** 키워드의 별칭이 **disk0**입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

format 명령은 지정된 파일 시스템의 모든 데이터를 지운 다음 디바이스에 FAT 정보를 다시 씁니다.

주의 **format** 명령은 손상된 플래시 메모리를 정리하기 위해 필요한 경우에만 각별히 주의하여 사용합니다.

(숨겨진 시스템 파일을 제외하고) 표시된 파일을 모두 삭제하려면 **format** 명령 대신 **delete /recursive** 명령을 입력합니다.

참고 Cisco ASA 5500 시리즈에서 **erase** 명령은 0xFF 패턴으로 디스크의 모든 사용자 데이터를 삭제합니다. 이와 달리 **format** 명령은 파일 시스템 제어 구조를 재설정할 뿐입니다. 원시 디스크 읽기 툴을 사용한 경우에도 이 정보를 볼 수 있습니다.

손상된 파일 시스템을 복구하려면 **fsck** 명령을 입력한 다음 **format** 명령을 입력해보십시오.

예

이 예에서는 플래시 메모리를 포맷하는 방법을 보여줍니다.

```
ciscoasa# format flash:
```

관련 명령

명령	설명
delete	사용자에게 표시되는 모든 파일을 제거합니다.
erase	모든 파일을 삭제하고 플래시 메모리를 포맷합니다.
fsck	손상된 파일 시스템을 복구합니다.

forward interface

스위치가 내장된 모델의 경우(예: ASA 5505), 어떤 VLAN이 다른 VLAN과의 접속을 시작하기 위한 연결을 복원하려면 인터페이스 컨피그레이션 모드에서 **forward interface** 명령을 사용합니다. 어떤 VLAN이 다른 VLAN과의 접속을 시작할 수 없게 하려면 이 명령의 **no** 형식을 사용합니다.

forward interface vlan *number*

no forward interface vlan *number*

구문 설명

vlan *number*	이 VLAN 인터페이스가 트래픽을 시작할 수 없는 VLAN ID를 지정합니다.

기본값

기본적으로 모든 인터페이스는 다른 모든 인터페이스에 대해 트래픽을 시작할 수 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

라이센스에서 지원하는 VLAN의 수에 따라 어떤 VLAN을 제한해야 하는 경우가 있습니다.

라우티드 모드에서는 ASA 5505 Base 라이센스로 최대 3개의 활성 VLAN을, Security Plus 라이센스는 최대 5개의 활성 VLAN을 구성할 수 있습니다. 활성 VLAN은 **nameif** 명령이 구성된 VLAN입니다. ASA 5505에서는 어떤 라이센스에서든 최대 5개의 비활성 LVAN을 구성할 수 있으나, 이를 활성화할 경우 라이센스의 지침을 따라야 합니다.

Base 라이센스에서는 3번째 VLAN을 **no forward interface** 명령으로 구성하여 이 VLAN이 다른 VLAN과의 접속을 시작할 수 없게 해야 합니다.

이를테면 인터넷 액세스를 위해 외부에 VLAN 1개를, 내부 업무용 네트워크에 또 다른 VLAN 1개를 그리고 홈 네트워크에 3번째 VLAN을 지정합니다. 홈 네트워크는 업무용 네트워크에 액세스할 필요가 없으므로, 홈 VLAN에서 **no forward interface** 명령을 사용할 수 있습니다. 업무용 네트워크는 홈 네트워크에 액세스할 수 있으나, 홈 네트워크는 업무용 네트워크에 액세스할 수 없습니다.

이미 2개의 VLAN 인터페이스가 **nameif** 명령으로 구성된 경우, 3번째 인터페이스에서는 반드시 **no forward interface** 명령을 **nameif** 명령보다 먼저 입력해야 합니다. ASA는 ASA 5505의 Base 라이센스에서 3개의 VLAN 인터페이스가 정상적으로 작동하는 것을 허용하지 않습니다.

예

다음 예에서는 3개의 VLAN 인터페이스를 구성합니다. 3번째 홈 인터페이스는 업무용 인터페이스에 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

...
```

관련 명령

명령	설명
backup interface	어떤 인터페이스를 이를테면 ISP에 대한 백업 링크가 되도록 지정합니다.
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
interface vlan	VLAN 인터페이스를 만들고 인터페이스 컨피그레이션 모드를 시작합니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
switchport access vlan	VLAN에 스위치 포트를 지정합니다.

fqdn(crypto ca trustpoint)

등록 과정에서 인증서의 SAN(Subject Alternative Name) 확장에 지정된 FQDN을 포함시키려면 crypto ca trustpoint 컨피그레이션 모드에서 **fqdn** 명령을 사용합니다. FQDN의 기본 설정을 복원하려면 이 명령의 **no** 형식을 사용합니다.

fqdn [*fqdn* **| none]**

no fqdn

구문 설명

fqdn	FQDN을 지정합니다. 최대 길이는 64자입니다.
none	어떤 FQDN도 지정하지 않습니다.

기본값

기본 설정은 FQDN을 포함하지 않는 것입니다.

명령 모드

다음 표는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ASA에서 인증서를 사용하는 Nokia VPN Client의 인증을 지원하도록 구성하는 경우 **none** 키워드를 사용합니다. Nokia VPN Client의 인증서 인증 지원에 대한 자세한 내용은 **crypto isakmp identity** 또는 **isakmp identity** 명령을 참조하십시오.

예

다음 예에서는 trustpoint central의 crypto ca-trustpoint 컨피그레이션 모드를 시작하고 trustpoint central에 대한 등록 요청에 FQDN인 engineering을 포함시킵니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# fqdn engineering
ciscoasa(config-ca-trustpoint)#
```

관련 명령

명령	설명
crypto ca trustpoint	crypto ca-trustpoint 컨피그레이션 모드를 시작합니다.
default enrollment	등록 매개변수를 기본값으로 되돌립니다.
enrollment retry count	등록 요청 보내기의 재시도 횟수를 지정합니다.
enrollment retry period	등록 요청을 전송하기 전에 기다리는 시간(분)을 지정합니다.
enrollment terminal	이 신뢰 지점에 잘라내기/붙여넣기 등록을 지정합니다.

fqdn(network object)

네트워크 객체에 대한 FQDN을 구성하려면 객체 컨피그레이션 모드에서 **fqdn** 명령을 사용합니다. 컨피그레이션에서 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

fqdn [v4 | v6] *fqdn*

no fqdn [v4 | v6] *fqdn*

구문 설명

fqdn	호스트 및 도메인을 포함하여 FQDN을 지정합니다. FQDN은 숫자 또는 문자로 시작하고 끝나야 합니다. 처음과 시작을 제외한 위치에는 문자, 숫자, 하이픈만 사용할 수 있습니다. 레이블은 점으로 구분됩니다(예: www.cisco.com).
v4	(선택 사항) IPv4 도메인 이름을 지정합니다.
v6	(선택 사항) IPv6 도메인 이름을 지정합니다.

기본값

기본적으로 도메인 이름은 IPv4 도메인입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
객체 네트워크 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.4(2)	이 명령을 도입했습니다.

사용 지침

기존 네트워크 객체를 다른 값으로 구성할 경우 새 컨피그레이션이 기존 컨피그레이션을 대체합니다.

예

다음 예에서는 네트워크 객체를 만드는 방법을 보여줍니다.

```
ciscoasa (config)# object network FQDN_1
ciscoasa (config-network-object)# fqdn example.cisco.com
```

관련 명령

명령	설명
clear configure object	생성된 모든 객체를 지웁니다.
description	네트워크 객체에 설명을 추가합니다.
fqdn	FQDN 네트워크 객체를 지정합니다.
host	호스트 네트워크 객체를 지정합니다.
nat	네트워크 객체를 위한 NAT를 활성화합니다.
object network	네트워크 객체를 만듭니다.
object-group network	네트워크 객체 그룹을 만듭니다.
range	네트워크 객체를 위한 주소 범위를 지정합니다.
show running-config object network	네트워크 객체 컨피그레이션을 표시합니다.
subnet	서브넷 네트워크 객체를 지정합니다.

fragment

패킷 단편화를 추가적으로 관리하고 NFS와의 호환성을 개선하려면 글로벌 컨피그레이션 모드에서 **fragment** 명령을 사용합니다. 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

fragment reassembly {**full** | **virtual**} {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment reassembly {**full** | **virtual**} {**size** | **chain** | **timeout** *limit*} [*interface*]

구문 설명

chain *limit*	하나의 완전한 IP 패킷이 최대 몇 개로 분할될 수 있는지 지정합니다.
interface	(선택 사항) ASA 인터페이스를 지정합니다. 인터페이스가 지정되지 않을 경우 이 명령은 모든 인터페이스에 적용됩니다.
reassembly full | **virtual**	ASA를 통해 라우팅되는 IP 프래그먼트의 완전 또는 가상 재결합을 지정합니다. ASA에서 종료하는 IP 프래그먼트는 항상 완전히 재결합됩니다.
size *limit*	재결합을 기다리는 IP 재결합 데이터베이스에 포함될 수 있는 프래그먼트의 최대 개수를 설정합니다. **참고** ASA 는 대기열 크기가 전체의 2/3 에 도달하면 기존 패브릭 체인에 포함되지 않은 프래그먼트를 더 이상 수용하지 않습니다 . 대기열의 나머지 1/3 은 소스 / 목적지 IP 주소와 IP 식별 번호가 이미 부분적으로 대기 중인 불완전 프래그먼트 체인과 동일한 프래그먼트를 수용하는 데 사용됩니다. 이 제한은 프래그먼트 플러딩 공격이 있을 때 합법적인 프래그먼트 체인이 재결합되게 하는 DoS 방지 메커니즘입니다 .
timeout *limit*	단편화된 전체 패킷이 도착할 때까지 기다리는 최대 시간(초)을 지정합니다. 패킷의 1번째 프래그먼트가 도착하면 타이머가 시작합니다. 패킷의 모든 프래그먼트가 지정된 시간(초)에 도착하지 않을 경우 이미 수신된 패킷의 프래그먼트는 모두 폐기됩니다.

기본값

기본 설정은 다음과 같습니다.

- **chain**은 24개 패킷입니다.
- *interface*는 모든 인터페이스입니다.
- **size**는 200입니다.
- **timeout**은 5초입니다.
- 가상 재결합이 활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	반드시 **chain**, **size** 또는 **timeout** 키워드 중 하나를 선택하도록 이 명령을 수정했습니다. 이전 릴리스의 소프트웨어와 달리 이 키워드 중 하나라도 입력하지 않고 **fragment** 명령을 입력할 수 없습니다.
8.0(4)	**reassembly full** | **virtual** 옵션을 추가했습니다.

사용 지침

기본적으로 ASA는 완전한 IP 패킷을 재구성하기 위해 최대 24개의 프래그먼트를 수용합니다. 네트워크 보안 정책에 따라 ASA에서 단편화된 패킷이 ASA를 지나는 것을 막도록 구성하는 것을 고려해야 합니다. 이를 위해서는 각 인터페이스에서 **fragment chain 1** *interface* 명령을 입력합니다. 이 한도를 1로 설정하면 모든 패킷이 완전해야, 즉 단편화되지 않아야 합니다.

ASA를 지나는 네트워크 트래픽의 상당 부분이 NFS라면 데이터베이스 오버플로를 방지하기 위해 추가적인 튜닝이 필요할 수 있습니다.

NFS 서버와 클라이언트 간의 MTU 크기가 작은 환경(예: WAN 인터페이스)에서는 **chain** 키워드에 추가적인 튜닝이 필요할 수 있습니다. 이러한 경우 효율성을 높이기 위해 NFS over TCP를 사용하는 것이 좋습니다.

size *limit*를 큰 값으로 설정하면 ASA가 프래그먼트 플러딩에 의한 DoS 공격에 더 취약해질 수 있습니다. **size** *limit*를 1550 또는 16384 풀에 있는 총 블록 수와 같게 또는 그보다 크게 설정하지 마십시오.

기본값은 프래그먼트 플러딩에 의한 DoS 공격을 제한합니다.

다음 프로세스는 **reassembly** 옵션 설정과 상관없이 수행됩니다.

- 프래그먼트 집합이 구성되거나 시간 초과 간격이 경과할 때까지 IP 프래그먼트가 수집됩니다(**timeout** 옵션 참조).
- 어떤 프래그먼트 집합이 구성되면 그 집합에 대해 무결성 검사가 실시됩니다. 이 검사에서는 중복, 테일 오버플로, 체인 오버플로가 없는지 확인합니다(**chain** 옵션 참조).

fragment reassembly virtual 명령이 구성될 경우 프래그먼트 집합은 추가 처리를 위해 전송 계층으로 전달됩니다.

fragment reassembly full 명령이 구성될 경우 프래그먼트 집합은 먼저 하나의 IP 패킷으로 병합됩니다. 이 단일 IP 패킷이 추가 처리를 위해 전송 계층으로 전달됩니다.

예

다음 예에서는 외부 및 내부 인터페이스에서 단편화된 패킷을 막는 방법을 보여줍니다.

```
ciscoasa(config)# fragment chain 1 outside
ciscoasa(config)# fragment chain 1 inside
```

단편화된 패킷을 막을 또 다른 인터페이스 각각에서 **fragment chain 1** *interface* 명령을 입력합니다.

다음 예에서는 외부 인터페이스의 프래그먼트 데이터베이스를 최대 크기 2000, 최대 체인 길이 45, 대기 시간 10초로 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# fragment size 2000 outside
ciscoasa(config)# fragment chain 45 outside
ciscoasa(config)# fragment timeout 10 outside
```

다음 예에서는 **show fragment** 명령의 출력을 보여줍니다. 이 명령에는 **reassembly virtual** 옵션이 포함되었습니다.

```
ciscoasa(config)# show fragment
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

관련 명령

명령	설명
clear configure fragment	모든 IP 프래그먼트 재결합 컨피그레이션을 기본값으로 재설정합니다.
clear fragment	IP 프래그먼트 재결합 모듈의 작업 데이터를 지웁니다.
show fragment	IP 프래그먼트 재결합 모듈의 작업 데이터를 표시합니다.
show running-config fragment	IP 프래그먼트 재결합 컨피그레이션을 표시합니다.

frequency

선택된 SLA 작업이 반복되는 속도를 설정하려면 SLA 모니터 프로토콜 컨피그레이션 모드에서 **frequency** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

frequency *seconds*

no frequency

구문 설명

seconds	SLA 프로브의 간격(초). 유효한 값의 범위는 1초~604800초입니다. 이 값은 **timeout** 값보다 작을 수 없습니다.

기본값

기본 빈도는 60초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
SLA 모니터 프로토콜 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

SLA 작업이 그 작업의 수명 기간에 지정된 빈도로 반복됩니다. 예:

- **ipIcmpEcho** 작업이 60초의 빈도로 반복됩니다. 즉 이 작업의 수명 기간에 60초마다 에코 요청 패킷을 보냅니다.
- 에코 작업의 기본 패킷 수는 1입니다. 이 패킷은 작업이 시작할 때 전송되고 다시 60초마다 전송됩니다.

각 SLA 작업이 지정된 빈도의 값보다 오랫동안 실행될 경우, 즉시 작업을 반복하지 않고 "busy"라는 통계 카운터가 증가합니다.

frequency 명령에 대해 지정된 값이 **timeout** 명령에 대해 지정된 값보다 작아서는 안 됩니다.

예

다음 예에서는 ID가 123인 SLA 작업을 구성하고 ID가 1인 추적 엔트리를 만들어 SLA의 도달 범위를 추적합니다. SLA 작업의 빈도는 3초로 설정되고, 시간 초과 값이 1000밀리초로 설정됩니다.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

명령	설명
sla monitor	SLA 모니터링 작업을 정의합니다.
timeout	SLA 작업이 응답을 기다리는 시간을 정의합니다.

fsck

파일 시스템 검사를 수행하고 손상을 복구하려면 특별 권한 EXEC 모드에서 **fsck** 명령을 사용합니다.

fsck [/noconfirm] {disk0: | disk1: | flash:}

구문 설명

/noconfirm	(선택 사항) 복구를 확인하는 메시지를 표시하지 않습니다.
disk0:	내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다.
disk1:	외부 플래시 메모리 카드를 지정하고 그 다음에 콜론을 표시합니다.
flash:	내부 플래시 메모리를 지정하고 그 다음에 콜론을 표시합니다. **flash** 키워드의 별칭이 **disk0**입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

fsck 명령이 검사하고 손상된 파일 시스템의 복구를 시도합니다. 더 영구적인 절차를 시도하기에 앞서 이 명령을 사용합니다.

FSCK 유틸리티에서 (정전, 비정상적인 종료 등으로 인한) 디스크 손상을 해결할 경우 FSCK*xxx*.REC라는 이름의 복구 파일을 만듭니다. 이 파일은 FSCK가 실행되는 동안 복구되었던 파일의 일부 또는 전체 파일을 포함할 수 있습니다. 드물게 데이터 복구를 위해 이 파일을 검사해야 하는 경우가 있습니다. 일반적으로 이 파일은 필요하지 않으므로 삭제해도 안전합니다.

참고 FSCK 유틸리티는 시작 시 자동으로 실행되므로 직접 **fsck** 명령을 입력하지 않았더라도 복구 파일이 표시될 수 있습니다.

예

다음 예에서는 플래시 메모리의 파일 시스템을 검사하는 방법을 보여줍니다.

```
ciscoasa# fsck disk0:
```

관련 명령

명령	설명
delete	사용자에게 표시되는 모든 파일을 제거합니다.
erase	모든 파일을 삭제하고 플래시 메모리를 포맷합니다.
format	파일 시스템의 모든 파일(숨겨진 시스템 파일 포함)을 지우고 파일 시스템을 다시 설치합니다.

ftp mode passive

FTP 모드를 패시브로 설정하려면 글로벌 컨피그레이션 모드에서 **ftp mode passive** 명령을 사용합니다. FTP 클라이언트를 액티브 모드로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

ftp mode passive

no ftp mode passive

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

ftp mode passive 명령은 FTP 모드를 패시브로 설정합니다. ASA에서는 FTP를 사용하여 FTP 서버에 이미지 파일이나 컨피그레이션 파일을 업로드하거나 이 서버로부터 다운로드할 수 있습니다. **ftp mode passive** 명령은 ASA의 FTP 클라이언트가 FTP 서버와 상호 작용하는 방식을 제어합니다.

패시브 FTP에서는 클라이언트가 제어 연결과 데이터 연결을 모두 시작합니다. 패시브 모드란 서버 상태를 나타냅니다. 즉 서버가 클라이언트에 의해 시작된 제어 연결과 데이터 연결 모두 수동적으로 받고 있는 것입니다.

패시브 모드에서는 목적지 포트와 소스 포트 모두 단명 포트입니다(1023보다 큼). 이 모드는 클라이언트에 의해 설정되는데, 클라이언트가 **passive** 명령을 실행하여 패시브 데이터 연결의 설정을 시작합니다. 패시브 모드에서 데이터 연결의 수신자가 되는 서버는 해당 연결을 수신하는 포트의 번호를 알려주며 응답합니다.

예

다음 예에서는 FTP 모드를 패시브로 설정합니다.

```
ciscoasa(config)# ftp mode passive
```

관련 명령

copy	FTP 서버에 이미지 파일 또는 컨피그레이션 파일을 업로드하거나 이 서버에서 다운로드합니다.
debug ftp client	FTP 클라이언트 활동에 대한 자세한 정보를 표시합니다.
show running-config ftp mode	FTP 클라이언트 컨피그레이션을 표시합니다.

functions

릴리스 8.0(2)에서는 **functions** 명령을 사용할 수 없습니다. 더 이상 사용하지 않으며, 단지 역호환성을 위해 이 명령 참조에 포함되었습니다. 웹 사이트, 파일 액세스, 플러그인을 위한 URL 목록, 사용자 지정, 언어 변환을 만들려면 **import** 및 **export** 명령을 사용합니다.

이 사용자 또는 그룹 정책에 대해 WebVPN을 통한 포트 전달 Java 애플릿의 자동 다운로드, Citrix 지원, 파일 액세스, 파일 브라우징, 파일 서버 입력, 웹 타입 ACL 적용, HTTP 프록시, 포트 전달 또는 URL 입력을 구성하려면 webvpn 컨피그레이션 모드에서 **functions** 명령을 사용합니다. 구성된 기능을 제거하려면 이 명령의 **no 형식을 사용합니다.**

functions {auto-download | citrix | file-access | file-browsing | file-entry | filter | http-proxy | url-entry | port-forward | none}

no functions {auto-download | citrix | file-access | file-browsing | file-entry | filter | http-proxy | url-entry | port-forward | none}

구문 설명

auto-download	WebVPN 로그인 후 포트 전달 Java 애플릿의 자동 다운로드를 활성화하거나 비활성화합니다. 먼저 포트 전달, Outlook/Exchange 프록시 또는 HTTP 프록시를 활성화해야 합니다.
citrix	MetaFrame Application Server에서 원격 사용자에 대한 터미널 서비스 지원을 활성화하거나 비활성화합니다. 이 키워드를 사용하면 ASA가 보안 Citrix 컨피그레이션 내에서 보안 게이트웨이의 역할을 할 수 있습니다. 이 서비스는 사용자가 표준 웹 브라우저를 통해 MetaFrame 애플리케이션에 액세스할 수 있게 합니다.
file-access	파일 액세스를 활성화하거나 비활성화합니다. 활성화하면 WebVPN 홈 페이지의 서버 목록에서 파일 서버를 나열합니다. 파일 브라우징 및/또는 파일 입력을 활성화하려면 파일 액세스를 활성화해야 합니다.
file-browsing	파일 서버 및 공유에 대한 브라우징을 활성화하거나 비활성화합니다. 사용자의 파일 서버 입력을 허용하려면 파일 브라우징을 활성화해야 합니다.
file-entry	사용자가 파일 서버의 이름을 입력하는 기능을 활성화하거나 비활성화합니다.
filter	웹 타입 ACL을 적용합니다. 활성화하면 ASA는 WebVPN **filter** 명령으로 정의된 웹 타입 ACL을 적용합니다.
http-proxy	HTTP 애플릿 프록시를 원격 사용자에게 전달하는 기능을 활성화하거나 비활성화합니다. 이 프록시는 Java, ActiveX, 플래시와 같이 적합한 맹글링(mangling)을 방해하는 기술에 유용합니다. 이는 ASA를 계속 사용할 수 있게 하면서 맹글링을 건너뜁니다. 전달된 프록시는 브라우저의 기존 프록시 컨피그레이션을 자동으로 수정하고 모든 HTTP 및 HTTPS 요청을 새 프록시 컨피그레이션으로 리디렉션합니다. HTML, CSS, JavaScript, VBScript, ActiveX, Java 등 모든 클라이언트 쪽 기술을 지원합니다. 유일하게 지원하는 브라우저는 Microsoft Internet Explorer입니다.
none	모든 WebVPN 기능에 null 값을 설정합니다. 기본 또는 지정된 그룹 정책에서 기능을 상속할 수 없게 합니다.
port-forward	포트 전달을 활성화합니다. 활성화하면 ASA는 WebVPN **port-forward** 명령으로 정의된 포트 전달 목록을 사용합니다.
url-entry	사용자의 URL 입력을 활성화하거나 비활성화합니다. 활성화하면 ASA는 구성된 URL 또는 네트워크 ACL이 있는 URL을 계속 제한합니다. URL 입력이 비활성화되면 ASA는 WebVPN 사용자를 홈 페이지에 있는 URL로 제한합니다.

기본값

기능은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
7.1(1)	**auto-download** 및 **citrix** 키워드를 추가했습니다.
8.0(2)	이 명령을 더 이상 사용하지 않습니다.

사용 지침

functions none 명령을 통해 생성된 null 값을 포함하여 구성된 모든 기능을 제거하려면 이 명령의 **no** 형식을 인수 없이 사용합니다. **no** 옵션은 다른 그룹 정책에서 값을 상속하는 것을 허용합니다. 기능 값을 상속할 수 없게 하려면 **functions none** 명령을 사용합니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 파일 액세스 및 파일 브라우징을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# functions file-access file-browsing
```

관련 명령

명령	설명
webvpn	group-policy 컨피그레이션 모드 또는 username 컨피그레이션 모드에서 사용합니다. 그룹 정책 또는 사용자 이름에 적용되는 매개변수를 구성하기 위해 webvpn 모드를 시작할 수 있습니다.

17 장

gateway ~ hw-module module shutdown 명령

gateway

특정 게이트웨이를 관리하는 통화 에이전트 그룹을 지정하려면 mgcp 맵 컨피그레이션 모드에서 **gateway** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

gateway *ip_address* [*group_id*]

구문 설명

gateway	특정 게이트웨이를 관리하는 통화 에이전트의 그룹.
group_id	통화 에이전트 그룹의 ID이며, 범위는 0~2147483647입니다.
ip_address	게이트웨이의 IP 주소.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Mgcp 맵 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

특정 게이트웨이를 관리하는 통화 에이전트 그룹을 지정하려면 **gateway** 명령을 사용합니다. 게이트웨이의 IP 주소는 *ip_address* 옵션으로 지정합니다. *group_id* 옵션은 게이트웨이를 관리하는 통화 에이전트의 *group_id*와 일치해야 하는 0~4294967295 사이의 숫자입니다. 게이트웨이는 하나의 그룹에만 속할 수 있습니다.

예

다음 예에서는 통화 에이전트 10.10.11.5 및 10.10.11.6에서 게이트웨이 10.10.10.115를 제어하고 통화 에이전트 10.10.11.7 및 10.10.11.8에서 두 게이트웨이 10.10.10.116 및 10.10.10.117을 모두 제어할 수 있게 합니다.

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

관련 명령

명령	설명
debug mgcp	MGCP를 위한 디버깅 정보의 표시를 활성화합니다.
mgcp-map	MGCP 맵을 정의하고 mgcp 맵 컨피그레이션 모드를 활성화합니다.
show mgcp	MGCP 컨피그레이션 및 세션 정보를 표시합니다.

gateway-fqdn

ASA의 FQDN을 구성하려면 **gateway-fqdn** 명령을 사용합니다. 컨피그레이션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

gateway-fqdn value {**FQDN_Name** | **none**}

no gateway-fqdn

구문 설명

fqdn-name	AnyConnect 클라이언트에 푸시할 ASA FQDN을 정의합니다.
none	FQDN을 null 값으로 정의합니다. 여기서는 FQDN이 지정되지 않습니다. hostname 및 domain-name 명령으로 구성된 전역 FQDN이 있으면 사용됩니다.

기본값

기본 FQDN 이름이 기본 그룹 정책에 설정되지 않았습니다. 새 그룹 정책이 이 값을 상속하도록 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

ASA 간에 로드 밸런싱을 구성한 경우, VPN 세션을 재설정하는 데 쓰이는 ASA IP 주소를 확인하려면 ASA의 FQDN을 지정합니다. 이 설정은 서로 다른 IP 프로토콜의 네트워크 간에 클라이언트 로밍을 지원하는 데 중요합니다(예: IPv4에서 IPv6로).

AnyConnect 프로필에 있는 ASA FQDN을 사용하여 로밍 후에 ASA IP 주소를 얻을 수 없습니다. 로드 밸런싱 시나리오에서는 주소가 정확한 디바이스(터널이 설정된 디바이스)와 매칭되지 않을 수 있습니다.

ASA의 FQDN이 클라이언트에 푸시되지 않을 경우 클라이언트는 이미 터널이 설정된 어떤 IP 주소와도 재연결을 시도합니다. 서로 다른 IP 프로토콜의 네트워크 간 로밍을 지원하려면(IPv4에서 IPv6로) AnyConnect가 로밍 후에 디바이스 FQDN의 이름 확인을 수행해야 합니다. 그러면 터널의 재설정에 어떤 ASA 주소를 사용할지 결정할 수 있습니다. 클라이언트는 초기 연결 과정에서 프로필에 있는 ASA FQDN을 사용합니다. 그 후속 세션 재연결 과정에서는 ASA에서 푸시하는 (그리고 관리자가 그룹 정책에서 구성한) 디바이스 FQDN이 있으면 항상 이를 사용합니다. FQDN이 구성되지 않을 경우 ASA는 무엇이든 ASDM의 Device Setup > Device Name/Password 및 Domain Name에 설정된 것에서 디바이스 FQDN을 얻고 클라이언트에 보냅니다.

ASA에서 디바이스 FQDN을 푸시하지 않을 경우, 클라이언트는 서로 다른 IP 프로토콜의 네트워크 간의 로밍 이후에 VPN 세션을 재설정할 수 없습니다.

예

다음 예에서는 ASA의 FQDN을 ASAName.example.cisco.com으로 설정합니다.

```
ciscoasa(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
ciscoasa(config-group-policy)#
```

다음 예에서는 그룹 정책에서 ASA의 FQDN을 제거합니다. 그러면 그룹 정책은 기본 그룹 정책에서 이 값을 상속합니다.

```
ciscoasa(config-group-policy)# no gateway-fqdn
ciscoasa(config-group-policy)#
```

다음 예에서는 어떤 값도 갖지 않는 FQDN을 정의합니다. ciscoasa 및 domain-name 명령으로 구성된 전역 FQDN이 있으면 사용됩니다.

```
ciscoasa(config-group-policy)# gateway-fqdn none
ciscoasa(config-group-policy)#
```

group

AnyConnect IPsec 연결을 위해 IKEv2 SA(보안 연결)에 Diffie-Hellman 그룹을 지정하려면 ikev2 정책 컨피그레이션 모드에서 **group** 명령을 사용합니다. 이 명령을 제거하고 기본 설정을 사용하려면 이 명령의 **no** 형식을 사용합니다.

group {1 | 2 | 5 | 14 | 19 | 20 | 21 | 24}

no group {1 | 2 | 5 | 14 | 19 | 20 | 21 | 24}

구문 설명

1	768비트 Diffie-Hellman 그룹 1을 지정합니다(FIPS 모드에서는 지원되지 않음).
2	1024비트 Diffie-Hellman 그룹 2를 지정합니다.
5	1536비트 Diffie-Hellman 그룹 5를 지정합니다.
14	ECDH 그룹을 IKEv2 DH 키 교환 그룹으로 선택합니다.
19	ECDH 그룹을 IKEv2 DH 키 교환 그룹으로 선택합니다.
20	ECDH 그룹을 IKEv2 DH 키 교환 그룹으로 선택합니다.
21	ECDH 그룹을 IKEv2 DH 키 교환 그룹으로 선택합니다.
24	ECDH 그룹을 IKEv2 DH 키 교환 그룹으로 선택합니다.

기본값

기본 Diffie-Hellman 그룹은 그룹 2입니다.

사용 지침

IKEv2 SA는 1단계에서 사용되는 키로서 IKEv2 피어가 2단계에서 안전하게 통신할 수 있게 합니다. **crypto ikev2 policy** 명령을 입력한 다음 **group** 명령을 사용하여 SA Diffie-Hellman 그룹을 설정할 수 있습니다. ASA와 AnyConnect 클라이언트는 공유 암호의 상호 전송 없이 그룹 식별자를 사용하여 공유 암호를 얻습니다. Diffie-Hellman 그룹 번호가 낮을수록 실행하는 데 필요한 CPU 시간이 줄어듭니다. Diffie-Hellman 그룹 번호가 높을수록 보안이 우수합니다.

AnyConnect 클라이언트가 비 FIPS 모드에서 작동하고 있다면 ASA는 Diffie-Hellman 그룹 1, 2, 5를 지원합니다. FIPS 모드에서는 그룹 2와 5를 지원합니다. 따라서 ASA에서 그룹 1*만* 사용하도록 구성할 경우 FIPS 모드의 AnyConnect 클라이언트는 연결에 실패합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Ikev2 정책 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
8.4(1)	이 명령이 추가됩니다.
9.0(1)	ECDH 그룹을 IKEv2 DH 키 교환 그룹으로 선택하는 기능을 추가했습니다.

예

다음 예에서는 ikev2 정책 컨피그레이션 모드를 시작하고 Diffie-Hellman 그룹을 그룹 5로 설정합니다.

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 5
```

관련 명령

명령	설명
encryption	AnyConnect IPsec 연결을 위해 IKEv2 SA에서 암호화 알고리즘을 지정합니다.
group	AnyConnect IPsec 연결을 위해 IKEv2 SA에서 Diffie-Hellman 그룹을 지정합니다.
lifetime	AnyConnect IPsec 연결을 위해 IKEv2 SA의 SA 수명을 지정합니다.
prf	AnyConnect IPsec 연결을 위해 IKEv2 SA에서 pseudo-random 기능을 지정합니다.

group-alias

사용자가 터널 그룹을 가리킬 때 사용하는 대체 이름을 하나 이상 만들려면 tunnel-group webvpn 컨피그레이션 모드에서 **group-alias** 명령을 사용합니다. 목록에서 별칭을 제거하려면 이 명령의 **no** 형식을 사용합니다.

group-alias *name* [**enable** | **disable**]

no group-alias *name*

구문 설명

disable	그룹 별칭을 비활성화합니다.
enable	이전에 비활성화되었던 그룹 별칭을 활성화합니다.
name	터널 그룹 별칭의 이름을 지정합니다. 사용자가 선택하는 어떤 문자열도 가능합니다. 단, 공백을 포함할 수 없습니다.

기본값

기본 그룹 별칭은 없지만, 그룹 별칭을 지정할 경우 이 별칭이 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tunnel-group webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

지정하는 그룹 별칭이 로그인 페이지의 드롭다운 목록에 나타납니다. 각 그룹은 여러 개의 별칭을 갖거나 별칭이 없을 수도 있습니다. 동일한 그룹이 여러 개의 CN(예: "Devtest", "QA")으로 알려진 경우 이 명령이 유용합니다.

예

다음 예에서는 "devtest"라는 터널 그룹을 구성하고 이 그룹에 대해 별칭 "QA"와 "Fra-QA"를 설정하는 명령을 보여줍니다.

```
ciscoasa(config)# tunnel-group devtest type webvpn
ciscoasa(config)# tunnel-group devtest webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias QA
ciscoasa(config-tunnel-webvpn)# group-alias Fra-QA
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

명령	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 명명된 터널 그룹 컨피그레이션을 지웁니다.
show webvpn group-alias	지정된 터널 그룹 또는 모든 터널 그룹의 별칭을 표시합니다.
tunnel-group webvpn-attributes	WebVPN 터널 그룹 특성을 구성하기 위해 tunnel-group webvpn 컨피그레이션 모드를 시작합니다.

group-delimiter

그룹 이름 구문 분석을 활성화하고 터널 협상 시 수신되는 사용자 이름으로부터 그룹 이름의 구문 분석을 수행할 때 사용할 구분 기호를 지정하려면 글로벌 컨피그레이션 모드에서 **group-delimiter** 명령을 사용합니다. 이 그룹 이름 구문 분석을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

group-delimiter *delimiter*

no group-delimiter

구문 설명

delimiter	그룹 이름 구분 기호로 사용할 문자를 지정합니다. 유효한 값은 **@**, **#**, **!**입니다.

기본값

기본적으로 어떤 구분 기호도 지정되지 않으므로 그룹 이름 구문 분석이 비활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

터널 협상 시 사용자 이름으로부터 터널 그룹 이름을 구문 분석하는 데 구분 기호를 사용합니다. 기본적으로 어떤 구분 기호도 지정되지 않으므로 그룹 이름 구문 분석이 비활성화됩니다.

예

이 예에서는 그룹 구분 기호를 해시 표시(#)로 변경하는 **group-delimiter** 명령을 보여줍니다.

```
ciscoasa(config)# group-delimiter #
```

관련 명령

명령	설명
clear configure group-delimiter	구성된 그룹 구분 기호를 지웁니다.
show running-config group-delimiter	현재 그룹 구분 기호 값을 표시합니다.
strip-group	strip 그룹 처리를 활성화하거나 비활성화합니다.

group-lock

원격 사용자가 터널 그룹을 통해서만 액세스하도록 제한하려면 group-policy 컨피그레이션 모드 또는 사용자 이름 컨피그레이셔 모드에서 **group-lock** 명령을 실행합니다. 실행 중인 컨피그레이션에서 **group-lock** 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

구문 설명

none	group-lock을 null 값으로 설정하여 어떤 그룹 잠금 제한도 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 그룹 잠금 값을 상속할 수 없게 합니다.
value *tunnel-grp-name*	ASA에서 요구하는 사용자 연결 대상인 기존 터널 그룹의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Group-policy 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 컨피그레이션	• 예	—	• 예	—	—

사용 지침

그룹 잠금을 비활성화하려면 **group-lock none** 명령을 사용합니다. **no group-lock** 명령은 다른 그룹 정책에서 값을 상속하는 것을 허용합니다.

그룹 잠금은 VPN 클라이언트에 구성된 그룹이 사용자가 지정된 터널 그룹과 동일한지 확인하는 방법으로 사용자를 제한합니다. 동일하지 않으면 ASA는 사용자가 연결할 수 없게 합니다. 그룹 잠금을 구성하지 않을 경우 ASA는 지정된 그룹과 상관없이 사용자를 인증합니다.

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 그룹 잠금을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# group-lock value tunnel group name
```

group-object

객체 그룹에 그룹 객체를 추가하려면 객체를 구성할 때 **group-object** 명령을 사용합니다. 그룹 객체를 제거하려면 이 명령의 **no** 형식을 사용합니다.

group-object *obj_grp_name*

no group-object *obj_grp_name*

구문 설명

obj_grp_name	객체 그룹을 식별합니다(1자~64자). 문자, 숫자, "_", "-", "." 문자의 어떤 조합도 가능합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
프로토콜, 네트워크, 서비스, icmp-type, 보안 그룹, 사용자 object-group 컨피그레이션 모드	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.4(2)	ID 방화벽 기능에 사용하기 위해 object-group 사용자 컨피그레이션 모드에서 객체 그룹을 추가하는 기능을 지원합니다.

사용 지침

group-object 명령을 **object-group** 명령과 함께 사용하여 그 자체가 객체 그룹인 객체를 추가할 수 있습니다. 이 하위 명령으로 동일한 유형의 객체를 논리적으로 그룹화하고 구조적 컨피그레이션을 위해 계층 구조 객체 그룹을 구성할 수 있습니다.

중복되는 객체는 그것이 그룹 객체라면 객체 그룹에 허용됩니다. 예를 들어, 객체 1이 그룹 A와 그룹 B 모두에 속해 있다면 A와 B를 모두 포함하는 그룹 C를 정의할 수 있습니다. 그러나 어떤 그룹 객체를 추가함으로써 그룹 계층 구조가 순환형이 되는 것은 허용되지 않습니다. 예를 들어, 그룹 A가 그룹 B를 포함하고 그룹 B 역시 그룹 A를 포함하는 것은 허용되지 않습니다.

계층 구조 객체 그룹에서 허용되는 최대 레벨은 10입니다.

참고 ASA는 IPv6 중첩 네트워크 객체 그룹을 지원하지 않습니다. 따라서 IPv6 항목의 객체를 다른 IPv6 객체 그룹으로 묶을 수 없습니다.

예

다음 예에서는 호스트 중복이 필요하지 않도록 **group-object** 명령을 사용하는 방법을 보여줍니다.

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network)# network-object host 192.168.1.1
ciscoasa(config-network)# network-object host 192.168.1.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network)# network-object host 172.23.56.1
ciscoasa(config-network)# network-object host 172.23.56.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network)# group-object host_grp_1
ciscoasa(config-network)# group-object host_grp_2
ciscoasa(config-network)# 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 w
```

다음 예에서는 사용자 그룹 객체에 로컬 사용자 그룹을 추가하기 위해 **group-object** 명령을 사용하는 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
```

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.

group-policy

그룹 정책을 만들거나 수정하려면 글로벌 컨피그레이션 모드에서 **group-policy** 명령을 사용합니다. 컨피그레이션에서 그룹 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

구문 설명

external server-group *server_group*	그룹 정책을 외부로 지정하고 ASA에서 특성을 찾기 위해 쿼리할 AAA 서버 그룹을 식별합니다.
from *group-policy_name*	이 내부 그룹 정책의 특성을 이미 있는 그룹 정책의 값으로 초기화합니다.
internal	그룹 정책을 내부로 식별합니다.
name	그룹 정책의 이름을 지정합니다. 이 이름은 최대 64자이며 공백을 포함할 수 있습니다. 공백을 포함한 그룹 이름은 큰따옴표로 묶어야 합니다(예: "Sales Group").
password *server_password*	외부 AAA 서버 그룹에서 특성을 검색할 때 사용할 비밀번호를 제공합니다. 이 비밀번호는 최대 128자이며 공백을 포함할 수 없습니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0.1	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드 지원을 추가했습니다.

사용 지침

"DefaultGroupPolicy"라는 기본 그룹 정책은 항상 ASA에 있습니다. 그러나 이 기본 그룹 정책은 ASA에서 사용하도록 구성하지 않는 한 효력이 없습니다. 컨피그레이션에 대한 지침은 CLI 컨피그레이션 가이드를 참조하십시오.

group-policy 컨피그레이션 모드를 시작하려면 **group-policy attributes** 명령을 사용합니다. 이 모드에서는 어떤 group-policy 특성-값 쌍도 구성할 수 있습니다. DefaultGroupPolicy에 이 특성-값 쌍이 있습니다.

특성	기본값
backup-servers	keep-client-config
banner	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

또한 그룹 정책 컨피그레이션 모드에서 **webvpn** 명령을 입력하거나 group-webvpn 컨피그레이션 모드에서 **group-policy attributes** 명령과 **webvpn** 명령을 차례로 입력하는 방법으로 그룹 정책에 대한 webvpn 컨피그레이션 모드 특성을 구성할 수 있습니다. 자세한 내용은 **group-policy attributes** 명령에 대한 설명을 참조하십시오.

예

다음 예에서는 "FirstGroup"이라는 이름으로 내부 그룹 정책을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup internal
```

다음 예에서는 이름이 "ExternalGroup", AAA 서버 그룹이 "BostonAAA", 비밀번호가 "12345678"인 외부 그룹 정책을 만드는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

관련 명령

명령	설명
clear configure group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대한 컨피그레이션을 제거합니다.
group-policy attributes	group-policy 컨피그레이션 모드를 시작합니다. 그러면 지정된 그룹 정책의 특성과 값을 구성하거나 webvpn 컨피그레이션 모드를 시작하여 그룹의 WebVPN 특성을 구성할 수 있습니다.
show running-config group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대해 실행 중인 컨피그레이션을 표시합니다.
webvpn	webvpn 컨피그레이션 모드를 시작합니다. 그러면 지정된 그룹의 WebVPN 특성을 구성할 수 있습니다.

group-policy attributes

group-policy 컨피그레이션 모드를 시작하려면 글로벌 컨피그레이션 모드에서 **group-policy attributes** 명령을 사용합니다. 그룹 정책에서 모든 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

group-policy *name* **attributes**

no group-policy *name* **attributes**

구문 설명

name	그룹 정책의 이름을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

group-policy 컨피그레이션 모드에서 지정된 그룹 정책의 특성-값 쌍을 구성하거나 group-policy webvpn 컨피그레이션 모드를 시작하여 이 그룹의 WebVPN 특성을 구성할 수 있습니다.

특성 모드의 명령 구문은 다음과 같은 공통점을 갖습니다.

- **no** 형식은 실행 중인 컨피그레이션에서 특성을 제거하고 다른 그룹 정책에서 값을 상속할 수 있게 합니다.
- **none** 키워드는 실행 중인 컨피그레이션의 특성을 null 값으로 설정하여 상속할 수 없게 합니다.
- 부울 특성은 활성 및 비활성 설정을 위한 명시적인 구문이 있습니다.

DefaultGroupPolicy라는 기본 그룹 정책은 항상 ASA에 있습니다. 그러나 이 기본 그룹 정책은 ASA에서 사용하도록 구성하지 않는 한 효력이 없습니다. 컨피그레이션에 대한 지침은 CLI 컨피그레이션 가이드를 참조하십시오.

group-policy attributes 명령으로 group-policy 컨피그레이션 모드를 시작합니다. 이 모드에서는 어떤 group-policy 특성-값 쌍도 구성할 수 있습니다. DefaultGroupPolicy에 이 특성-값 쌍이 있습니다.

특성	기본값
backup-servers	keep-client-config
banner	none
client-access-rule	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

또한 그룹 정책에 대한 webvpn-mode 특성을 구성할 수 있습니다. **group-policy attributes** 명령을 입력한 다음 group-policy 컨피그레이션 모드에서 **webvpn** 명령을 입력하면 됩니다. 자세한 내용은 **webvpn** 명령에 대한 설명(group-policy 특성 및 사용자 이름 특성 모드)을 참조하십시오.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 group-policy 특성 모드를 시작하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)#
```

관련 명령

명령	설명
clear configure group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대한 컨피그레이션을 제거합니다.
group-policy	그룹 정책을 만들거나 수정하거나 제거합니다.
show running-config group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대해 실행 중인 컨피그레이션을 표시합니다.
webvpn	group-webvpn 컨피그레이션 모드를 시작합니다. 그러면 지정된 그룹의 WebVPN 특성을 구성할 수 있습니다.

group-prompt

WebVPN 사용자가 ASA에 연결할 때 표시되는 WebVPN 페이지 로그인 상자의 그룹 프롬프트를 사용자 지정하려면 webvpn 사용자 지정 컨피그레이션 모드에서 **group-prompt** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

group-prompt {**text** | **style**} *value*

no group-prompt {**text** | **style**} *value*

구문 설명

text	텍스트의 변경 사항을 지정합니다.
style	스타일의 변경 사항을 지정합니다.
value	표시할 실제 텍스트 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자).

기본값

그룹 프롬프트의 기본 텍스트는 "GROUP"입니다.

그룹 프롬프트의 기본 스타일은 color:black;font-weight:bold;text-align:right입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Webvpn 사용자 지정 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

style 옵션은 임의의 유효한 CSS 매개변수로 표시됩니다. 이 매개변수에 대한 설명은 본 설명서의 범위에 속하지 않습니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹 사이트(www.w3.org)의 CSS 사양을 참조하십시오. CSS 2.1 사양의 부록 F는 편리한 CSS 매개변수 목록을 포함하고 있으며 www.w3.org/TR/CSS21/propidx.html에서 이용할 수 있습니다.

WebVPN 페이지 - 페이지 색상의 가장 대표적인 변경 방법에 대한 몇 가지 팁을 소개합니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 (HTML에서 인식된다면) 색상의 이름을 사용할 수 있습니다.
- RGB 형식은 0,0,0이며, 각 색상(빨강, 녹색, 파랑)을 나타내는 0~255 범위의 10진수입니다. 쉼표로 구분하여 입력한 값은 해당 강도의 각 색상이 나머지 색상과 조합되는 것을 의미합니다.
- HTML 형식은 #000000이며, 6자리의 16진수입니다. 1번째와 2번째 자리는 빨강을, 3번째와 4번째 자리는 녹색을, 5번째와 6번째는 파랑을 나타냅니다.

참고 손쉽게 WebVPN 페이지를 사용자 지정하려면 ASDM을 사용하는 것이 좋습니다. 색 견본, 미리 보기 등 스타일 요소를 편리하게 구성할 수 있는 기능을 제공합니다.

예

다음 예에서는 텍스트가 "Corporate Group:"으로 바뀌며 기본 스타일은 글꼴 두께가 더 굵어지도록 변경됩니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# group-prompt text Corporate Group:
ciscoasa(config-webvpn-custom)# group-prompt style font-weight:bolder
```

관련 명령

명령	설명
password-prompt	WebVPN 페이지의 비밀번호 프롬프트를 사용자 지정합니다.
username-prompt	WebVPN 페이지의 사용자 이름 프롬프트를 사용자 지정합니다.

group-search-timeout

show ad-groups 명령을 사용하여 쿼리한 Active Directory 서버의 응답을 기다리는 시간의 최대값을 지정하려면 aaa-server 호스트 컨피그레이션 모드에서 **group-search-timeout** 명령을 사용합니다. 컨피그레이션에서 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다.

group-search-timeout *seconds*

no group-search-timeout *seconds*

구문 설명

seconds	Active Directory 서버의 응답을 기다리는 시간이며, 범위는 1초~300초입니다.

기본값

기본값은 10초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(4)	이 명령을 도입했습니다.

사용 지침

show ad-groups 명령은 LDAP을 사용하는 Active Directory 서버에만 적용되며, Active Directory 서버에 등록된 그룹을 표시합니다. 서버의 응답을 기다리는 시간을 조정하려면 **group-search-timeout** 명령을 사용합니다.

예

다음 예에서는 시간 초과를 20초로 설정합니다.

```
ciscoasa(config-aaa-server-host)#group-search-timeout 20
```

관련 명령

명령	설명
ldap-group-base-dn	서버가 동적 그룹 정책에 사용되는 그룹의 검색을 시작하는 Active Directory 계층 구조상의 레벨을 지정합니다.
show ad-groups	Active Directory 서버에 등록된 그룹을 표시합니다.

group-url

그룹에 대해 수신 URL 또는 IP 주소를 지정하려면 tunnel-group webvpn 컨피그레이션 모드에서 **group-url** 명령을 사용합니다. 목록에서 URL을 제거하려면 이 명령의 **no** 형식을 사용합니다.

group-url *url* [**enable** | **disable**]

no group-url *url*

구문 설명

disable	URL을 비활성화합니다. 그러나 목록에서 URL을 제거하지는 않습니다.
enable	URL을 활성화합니다.
url	이 터널 그룹의 URL 또는 IP 주소를 지정합니다.

기본값

기본 URL 또는 IP 주소는 없지만, 사용자가 URL 또는 IP 주소를 지정하면 기본적으로 활성화됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Tunnel-group webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

그룹 URL 또는 IP 주소를 지정하면 사용자가 로그인 시 그룹을 선택할 필요가 없습니다. 사용자가 로그인하면 ASA는 터널 그룹 정책 테이블에서 사용자의 수신 URL/주소를 찾습니다. URL/주소를 찾았고 터널 그룹에서 이 명령이 활성 상태라면 ASA는 자동으로 해당 터널 그룹을 선택하고 사용자에게 로그인 창에서 사용자 이름 및 비밀번호 필드만 표시합니다. 그러면 사용자 인터페이스가 간소화되고 그룹 목록이 사용자에게 노출될 염려가 없다는 장점도 있습니다. 사용자에게 표시되는 로그인 창에서는 그 터널 그룹에 대해 구성된 사용자 지정을 적용합니다.

URL/주소가 비활성화되었고 **group-alias** 명령이 구성된 경우, 그룹의 드롭다운 목록도 표시되며 사용자가 선택해야 합니다.

하나의 그룹에 대해 여러 URL/주소(또는 none)를 구성할 수 있습니다. 각 URL/주소는 개별적으로 활성화하거나 비활성화할 수 있습니다. 지정된 각 URL/주소에 개별적으로 **group-url** 명령을 사용해야 합니다. HTTP 또는 HTTPS 프로토콜을 포함하여 전체 URL/주소를 지정해야 합니다.

동일한 URL/주소를 여러 그룹과 연결할 수 없습니다. ASA는 터널 그룹의 URL/주소를 승인하기 전에 그 고유성을 확인합니다.

예

다음 예에서는 "test"라는 WebVPN 터널 그룹을 구성하고 이 그룹을 위해 2개의 그룹 URL, "http://www.cisco.com"과 "https://supplier.example.com"을 설정하는 명령을 보여줍니다.

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com
ciscoasa(config-tunnel-webvpn)# group-url https://supplier.example.com
ciscoasa(config-tunnel-webvpn)#
```

다음 예에서는 RadiusServer라는 터널 그룹을 위해 그룹 URL, http://www.cisco.com과 http://192.168.10.10을 활성화합니다.

```
ciscoasa(config)# tunnel-group RadiusServer type webvpn
ciscoasa(config)# tunnel-group RadiusServer general-attributes
ciscoasa(config-tunnel-general)# authentication server-group RADIUS
ciscoasa(config-tunnel-general)# accounting-server-group RADIUS
ciscoasa(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com enable
ciscoasa(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

명령	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 명명된 터널 그룹 컨피그레이션을 지웁니다.
show webvpn group-url	지정된 터널 그룹 또는 모든 터널 그룹의 URL을 표시합니다.
tunnel-group webvpn-attributes	WebVPN 터널 그룹 특성을 구성하기 위해 webvpn 컨피그레이션 모드를 시작합니다.

h245-tunnel-block

H.323에서 H.245 터널링을 차단하려면 매개변수 컨피그레이션 모드에서 **h245-tunnel-block** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

h245-tunnel-block action [**drop-connection** | **log**]

no h245-tunnel-block action [**drop-connection** | **log**]

구문 설명

drop-connection	H.245 터널이 탐지되면 통화 설정 연결을 삭제합니다.
log	H.245 터널이 탐지되면 로그를 실행합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 H.323 통화에서 H.245 터널링을 차단하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# h245-tunnel-block action drop-connection
```

관련 명령

명령	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	어떤 애플리케이션과 관련된 트래픽을 매칭하기 위해 검사 클래스 맵을 생성합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

health-check

클러스터 상태 검사 기능을 활성화하려면 클러스터 그룹 컨피그레이션 모드에서 **health-check** 명령을 사용합니다. 상태 검사를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

health-check [**holdtime** *timeout*] [**vss-enabled**]

no health-check [**holdtime** *timeout*] [**vss-enabled**]

구문 설명

holdtime *timeout*	(선택 사항) keepalive 메시지 또는 인터페이스 상태 메시지 간의 간격을 0.8초~45초 범위에서 결정합니다. 기본값은 3초입니다.
vss-enabled	클러스터 제어 링크를 EtherChannel로 구성하고(권장) 이를 VSS 또는 vPC 쌍에 연결한 경우, **vss-enabled** 옵션을 활성화해야 할 수 있습니다. 일부 스위치의 경우 VSS/vPC에서 유닛 하나가 중단되거나 부팅하면 해당 스위치에 연결된 EtherChannel 멤버 인터페이스가 ASA에 대해 가동되는 것으로 표시되지만, 스위치 측의 트래픽을 통과하지 않습니다. ASA 대기 시간 제한을 낮은 값으로 설정한 경우(0.8초) 클러스터에서 ASA가 잘못 제거될 수 있으며 ASA에서는 이러한 EtherChannel 인터페이스 중 하나에 keepalive 메시지를 보냅니다. **vss-enabled**를 활성화할 경우, ASA에서는 하나 이상의 스위치에 keepalive 메시지가 전송되도록 하기 위해 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 대량의 keepalive 메시지를 보냅니다.

명령 기본값

상태 검사는 기본적으로 활성화되며, 대기 시간은 3초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
클러스터 그룹 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.
9.1(4)	**vss-enabled** 키워드를 추가했습니다.

사용 지침

토폴로지 변경이 일어날 경우(예: 데이터 인터페이스를 추가하거나 제거할 때, ASA 또는 스위치에서 인터페이스를 활성화하거나 비활성화할 때, VSS 또는 vPC를 구성하기 위해 스위치를 추가할 때) **no health-check** 명령을 사용하여 잠시 상태 검사를 비활성화하는 것이 좋습니다. 클러스터 토폴로지가 안정화되면 클러스터 상태 검사 기능을 다시 활성화해야 합니다.

멤버 간의 keepalive 메시지로 멤버의 상태를 확인합니다. 피어 유닛의 keepalive 메시지가 대기 시간 내에 유닛에 전송되지 않을 경우, 해당 피어 유닛은 응답하지 않거나 중지된 상태로 간주합니다. 인터페이스 상태 메시지에 링크 장애가 감지됩니다. 특정 유닛의 인터페이스에 오류가 발생하였으나 다른 유닛의 동일한 인터페이스는 활성 상태인 경우, 클러스터에서 해당 특정 유닛이 제거됩니다.

대기 시간 내에 인터페이스 상태 메시지가 유닛에 전송되지 않을 경우, ASA에서 클러스터의 멤버를 제거하기까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 좌우됩니다. EtherChannel(Spanned 또는 일반)의 경우, 설정된 멤버에 대한 인터페이스가 중지될 경우 ASA에서는 9초 후에 해당 멤버를 제거합니다. 유닛이 새 멤버로 클러스터에 참가할 경우 ASA는 45초 기다렸다가 새 유닛을 거부합니다. 비 EtherChannel의 경우, 멤버 상태와 관계없이 500ms 후에 유닛이 제거됩니다.

이 명령은 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.

예

다음 예에서는 상태 검사를 비활성화합니다.

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no health-check
```

관련 명령

명령	설명
clacp system-mac	Spanned EtherChannel을 사용하면 ASA에서는 cLACP를 통해 네이버 스위치와 EtherChannel을 협상합니다.
cluster group	클러스터의 이름을 지정하고 클러스터 컨피그레이션 모드를 시작합니다.
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.
key	클러스터 제어 링크의 제어 트래픽에 대해 인증 키를 설정합니다.
local-unit	클러스터 멤버의 이름을 지정합니다.
mtu cluster-interface	클러스터 제어 링크 인터페이스를 위한 최대 전송 유닛을 지정합니다.
priority (cluster group)	마스터 유닛 선택에서 이 유닛의 우선 순위를 설정합니다.

hello-interval

인터페이스에서 전송된 EIGRP hello 패킷의 간격을 지정하려면 인터페이스 컨피그레이션 모드에서 **hello-interval** 명령을 사용합니다. hello 간격을 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

hello-interval eigrp *as-number seconds*

no hello-interval eigrp *as-number seconds*

구문 설명

as-number	EIGRP 라우팅 프로세스의 자동 시스템 번호를 지정합니다.
seconds	인터페이스에서 전송된 Hello 패킷 간의 간격을 지정합니다. 유효한 값의 범위는 1초~65535초입니다.

기본값

기본값은 5초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

hello 간격이 짧을수록 토폴로지 변경 사항이 더 빨리 탐지되지만 더 많은 라우팅 트래픽이 발생합니다. 이 값은 특정 네트워크의 모든 라우터 및 액세스 서버에서 동일해야 합니다.

예

다음 예에서는 EIGRP hello 간격을 10초로, 대기 시간을 30초로 설정합니다.

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

관련 명령

명령	설명
hold-time	hello 패킷에서 광고하는 EIGRP 대기 시간을 구성합니다.

help

지정된 명령에 대한 도움말 정보를 표시하려면 사용자 EXEC 모드에서 **help** 명령을 사용합니다.

help {*command* | **?**}

구문 설명

?	현재 권한 레벨 및 모드에서 사용 가능한 모든 명령을 표시합니다.
command	CLI 도움말을 표시할 명령을 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
사용자 EXEC	• 예	• 예	• 예	• 예	• 예

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

help 명령은 모든 명령에 대한 도움말 정보를 표시합니다. **help** 명령 다음에 명령 이름을 입력하여 개별 명령의 도움말을 확인할 수 있습니다. 명령 이름을 지정하지 않고 **?**를 입력하면 현재 권한 레벨 및 모드에서 사용 가능한 모든 명령을 표시합니다.

pager 명령을 활성화할 경우 24개 행이 표시된 다음 목록이 일시 중지했다가 다음 프롬프트가 나타납니다.

```
<--- More --->
```

More 프롬프트에서는 다음과 같이 UNIX **more** 명령과 비슷한 구문을 사용합니다.

- 다른 텍스트 화면을 보려면 **스페이스** 바를 누릅니다.
- 다음 행을 보려면 **Enter** 키를 누릅니다.
- 명령줄로 돌아가려면 **q** 키를 누릅니다.

예

다음 예에서는 **rename** 명령에 대해 도움말을 표시하는 방법을 보여줍니다.

```
ciscoasa# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

ciscoasa#
```

다음 예에서는 명령 이름과 물음표를 입력하여 도움말을 표시하는 방법을 보여줍니다.

```
ciscoasa(config)# enable ?
usage: enable password <pwd> [encrypted]
```

show, **no**, **clear** 명령이 아닌 코어 명령에 대한 도움말은 명령 프롬프트에 **?**를 입력하여 표시할 수 있습니다.

```
ciscoasa(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

관련 명령

명령	설명
show version	운영 체제 소프트웨어에 대한 정보를 표시합니다.

hidden-parameter

ASA에서 SSO 인증을 위해 인증 웹 서버에 보내는 HTTP POST 요청의 숨겨진 매개변수를 지정하려면 aaa-server-host 컨피그레이션 모드에서 **hidden-parameter** 명령을 사용합니다. 실행 중인 컨피그레이션에서 숨겨진 매개변수를 모두 제거하려면 이 명령의 **no** 형식을 사용합니다.

hidden-parameter *string*

no hidden-parameter

참고 HTTP 프로토콜을 사용하여 SSO를 올바르게 구성하려면 인증 및 HTTP 프로토콜 교환에 대해 잘 알고 있어야 합니다.

구문 설명

string	양식에 포함된 숨겨진 매개변수로서 SSO 서버에 전송됩니다. 여러 행으로 입력할 수 있습니다. 각 행의 최대 길이는 255자입니다. 전체 행의 최대 길이(숨겨진 매개변수 전체)는 2048자입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

이는 HTTP Forms 명령을 사용하는 SSO입니다.

ASA의 WebVPN 서버는 인증 웹 서버에 SSO 인증 요청을 보내는 데 HTTP POST 요청을 사용합니다. 그 요청에서 사용자에게 표시되지 않는 (사용자 이름 및 비밀번호 이외의) SSO HTML 양식의 숨겨진 매개변수가 필요할 수 있습니다. 웹 서버로부터 받은 양식에 HTTP 헤더 분석기를 사용하면 웹 서버가 POST 요청에서 기대하는 숨겨진 매개변수를 발견할 수 있습니다.

hidden-parameter 명령으로 웹 서버가 인증 POST 요청에서 요구하는 숨겨진 매개변수를 지정할 수 있습니다. 헤더 분석기를 사용할 경우 인코딩된 URL 매개변수를 포함하여 숨겨진 매개변수 문자열 전체를 복사하여 붙여넣을 수 있습니다.

입력의 편의성을 위해 연속적인 여러 행에 숨겨진 매개변수를 입력할 수 있습니다. 그러면 ASA는 이 행들을 하나의 숨겨진 매개변수로 연결합니다. 숨겨진 매개변수 라인별 최대 길이는 255자이지만 각 행에서 더 짧게 입력할 수 있습니다.

참고 문자열에 물음표가 있으면 그 앞에 **Ctrl+v** 이스케이프 시퀀스가 와야 합니다.

예

다음 예에서는 4개의 양식 엔트리와 그 값이 &로 구분된 숨겨진 매개변수를 보여줍니다. POST 요청에서 발췌한 4개의 엔트리와 그 값은 다음과 같습니다.

- 값이 ISO-8859-1인 SMENC
- 값이 US-EN인 SMLOCALE
- 값이 https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG인 target
- 값이 0인 smauthreason

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
ciscoasa(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
ciscoasa(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
ciscoasa(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
ciscoasa(config-aaa-server-host)#
```

관련 명령

명령	설명
action-uri	SSO 인증을 위한 사용자 이름 및 비밀번호를 받을 웹 서버 URI를 지정합니다.
auth-cookie-name	인증 쿠키의 이름을 지정합니다.
password-parameter	SSO 인증을 위해 사용자 비밀번호를 전송해야 하는 HTTP POST 요청 매개변수의 이름을 지정합니다.
start-url	로그인 전 쿠키를 검색할 URL을 지정합니다.
user-parameter	SSO 인증을 위해 사용자 이름을 전송해야 하는 HTTP POST 요청 매개변수의 이름을 지정합니다.

hidden-shares

CIFS 파일에 대한 숨겨진 공유의 가시성을 제어하려면 group-webvpn 컨피그레이션 모드에서 **hidden-shares** 명령을 사용합니다. 컨피그레이션에서 숨겨진 공유 옵션을 제거하려면 이 명령의 **no** 형식을 사용합니다.

hidden-shares {**none** | **visible**}

[no] hidden-shares {**none** | **visible**}

구문 설명

none	사용자에게 표시되거나 사용자 액세스 가능한 구성된 숨겨진 공유가 없도록 지정합니다.
visible	숨겨진 공유를 표시하고 사용자가 액세스할 수 있게 합니다.

기본값

이 명령의 기본 동작은 none입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

숨겨진 공유는 공유 이름의 끝에 달러 기호($)로 표시합니다. 이를테면 드라이브 C는 C$의 형태로 공유됩니다. 숨겨진 공유에서 공유 폴더는 표시되지 않으며, 사용자는 이 숨겨진 리소스를 탐색하거나 액세스할 수 없습니다.

hidden-shares 명령의 **no** 형식은 컨피그레이션에서 이 옵션을 제거하고 그룹 정책 특성인 숨겨진 공유를 비활성화합니다.

예

다음 예에서는 GroupPolicy2와 관련된 WebVPN CIFS 숨겨진 공유를 표시합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-group-policy)# group-policy GroupPolicy2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# hidden-shares visible
ciscoasa(config-group-webvpn)#
```

관련 명령

명령	설명
debug webvpn cifs	CIFS에 대한 디버깅 메시지를 표시합니다.
group-policy attributes	group-policy 컨피그레이션 모드를 시작합니다. 그러면 지정된 그룹 정책의 특성과 값을 구성하거나 webvpn 컨피그레이션 모드를 시작하여 그룹의 WebVPN 특성을 구성할 수 있습니다.
url-list	WebVPN 사용자가 액세스할 URL의 집합을 구성합니다.
url-list	특정 사용자 또는 그룹 정책에 WebVPN 서버 및 URL의 목록을 적용합니다.

hold-time

ASA가 EIGRP hello 패킷에서 광고하는 대기 시간을 지정하려면 인터페이스 컨피그레이션 모드에서 **hold-time** 명령을 사용합니다. hello 간격을 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

hold-time eigrp *as-number seconds*

no hold-time eigrp *as-number seconds*

구문 설명

as-number	EIGRP 라우팅 프로세스의 자율 시스템 번호.
seconds	대기 시간(초)을 지정합니다. 유효한 값의 범위는 1초~65535초입니다.

기본값

기본값은 15초입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.
9.0(1)	다중 컨텍스트 모드가 지원됩니다.

사용 지침

이 값은 ASA에서 보내는 EIGRP hello 패킷에서 광고합니다. 이 인터페이스의 EIGRP 네이버는 ASA의 가용성을 확인하는 데 이 값을 사용합니다. 광고된 대기 시간에 ASA로부터 hello 패킷을 받지 못할 경우 EIGRP 네이버는 ASA가 사용할 수 없는 상태라고 간주합니다.

정체가 심한 대규모 네트워크에서는 모든 라우터와 액세스 서버가 네이버로부터 hello 패킷을 받기에는 기본 대기 시간이 짧을 수 있습니다. 따라서 대기 시간을 늘려야 하는 경우도 있습니다.

대기 시간은 hello 간격의 3배 이상으로 설정하는 것이 좋습니다. ASA에서 지정된 대기 시간 내에 hello 패킷을 받지 못하면 이 네이버를 지나는 경로는 사용할 수 없는 것으로 간주됩니다.

대기 시간을 늘리면 네트워크에서 경로의 통합이 지연됩니다.

예

다음 예에서는 EIGRP hello 간격을 10초로, 대기 시간을 30초로 설정합니다.

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

관련 명령

명령	설명
hello-interval	인터페이스에서 전송된 EIGRP hello 패킷의 간격을 지정합니다.

homepage

이 WebVPN 사용자 또는 그룹 정책을 위해 로그인 시 표시되는 웹 페이지의 URL을 지정하려면 webvpn 컨피그레이션 모드에서 **homepage** 명령을 사용합니다. **homepage none** 명령으로 생성된 null 값을 포함하여 구성된 홈 페이지를 제거하려면 이 명령의 **no** 형식을 사용합니다.

homepage {**value** *url-string* | **none**}

no homepage

구문 설명

none	WebVPN 홈 페이지가 없음을 나타냅니다. null 값을 설정하여 홈 페이지를 허용하지 않습니다. 홈 페이지를 상속할 수 없게 합니다.
value *url-string*	홈 페이지의 URL을 제공합니다. 이 문자열은 http:// 또는 https:// 중 하나로 시작해야 합니다.

기본값

기본 홈 페이지는 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

그룹 정책과 연결된 사용자를 위한 홈 페이지 URL을 지정하려면 이 명령에 URL 문자열의 값을 입력합니다. 기본 그룹 정책에서 홈 페이지를 상속하려면 이 명령의 **no** 형식을 사용합니다. **no** 옵션은 다른 그룹 정책에서 값을 상속하는 것을 허용합니다. 홈 페이지를 상속할 수 없게 하려면 **homepage none** 명령을 사용합니다.

클라이언트리스 사용자는 인증에 성공하면 즉시 이 페이지로 연결됩니다. AnyConnect는 VPN 연결이 성공적으로 설정되면 이 URL로 기본 웹 브라우저를 시작합니다. Linux 플랫폼에서는 현재 AnyConnect가 이 명령을 지원하지 않으므로 무시합니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책의 홈 페이지로 www.example.com을 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
```

관련 명령

명령	설명
webvpn	그룹 정책 또는 사용자 이름에 적용되는 매개변수를 구성하기 위해 webvpn 컨피그레이션 모드를 시작할 수 있게 합니다.

homepage use-smart-tunnel

클라이언트리스 SSL VPN 사용 시 그룹 정책 홈 페이지에서 스마트 터널 기능을 사용할 수 있게 하려면 group-policy webvpn 컨피그레이션 모드에서 **homepage use-smart-tunnel** 명령을 사용합니다.

homepage {**value** *url-string* | **none**}

homepage use-smart-tunnel

구문 설명

none	WebVPN 홈 페이지가 없음을 나타냅니다. null 값을 설정하여 홈 페이지를 허용하지 않습니다. 홈 페이지를 상속할 수 없게 합니다.
value *url-string*	홈 페이지의 URL을 제공합니다. 이 문자열은 http:// 또는 https:// 중 하나로 시작해야 합니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

사용 지침

HTTP 캡처 툴을 사용하여 브라우저 세션을 모니터링하고 WebVPN 연결 과정에서 스마트 터널이 시작했는지 확인할 수 있습니다. 브라우저 캡처에 표시되는 내용에 따라 그 요청이 성능 저하 없이 웹 페이지에 전달될지 여부 및 스마트 터널이 사용되는지 여부가 결정됩니다. https://172.16.16.23/+CSCOE+portal.html과 같은 내용이 표시될 경우 +*CSCO**는 ASA에 의해 콘텐츠의 성능이 저하됨을 의미합니다. 스마트 터널이 시작될 때 +CSCO* 없이 특정 URL로 향하는 **http get** 명령이 표시됩니다(예: GET 200 html http://mypage.example.com).

예

이를테면 벤더 V가 파트너 P에게 내부 재고 서버 페이지에 대한 클라이언트리스 액세스를 제공하려는 경우 벤더 V의 관리자는 다음 사항을 결정해야 합니다.

- 사용자가 클라이언트리스 포털을 거치는가와 상관없이 클라이언트리스 SSL VPN에 로그인한 다음 재고 페이지에 액세스할 것인가?
- 페이지가 Microsoft Silverlight 구성 요소를 포함하고 있으므로 스마트 터널이 액세스에 올바른 선택인가?
- 브라우저가 일단 터널링되면 모든 터널 정책에 따라 모든 브라우저 트래픽이 벤더 V의 ASA를 지나야 하고 파트너 P의 사용자는 내부 리소스에 대한 어떤 액세스 권한도 갖지 않으므로 tunnel-all 정책이 적합한가?

재고 페이지가 inv.example.com(10.0.0.0)에서 호스팅된다는 가정 하에 다음 예에서는 하나의 호스트만 포함하는 터널 정책을 만듭니다.

```
ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.0.0.0
ciscoasa(config-webvpn)# smart-tunnel network inventory host inv.example.com
```

다음 예에서는 파트너의 그룹 정책에 터널 지정 터널 정책을 적용합니다.

```
ciscoasa(config-group-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory
```

다음 예에서는 그룹 정책 홈 페이지를 지정하고 그 페이지에서 스마트 터널을 활성화합니다.

```
ciscoasa(config-group-webvpn)# homepage value http://inv.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
```

host(network object)

네트워크 객체에 대해 호스트를 구성하려면 네트워크 컨피그레이션 모드에서 **host** 명령을 사용합니다. 객체에서 호스트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

host *ip_address*

no host *ip_address*

구문 설명

ip_address	객체의 호스트 IP 주소를 식별합니다. IPv4 또는 IPv6 주소입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
객체 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

사용 지침

기존 네트워크 객체를 다른 IP 주소로 구성할 경우 새 컨피그레이션이 기존 컨피그레이션을 대체합니다.

예

다음 예에서는 호스트 네트워크 객체를 만드는 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.
nat	네트워크 객체를 위한 NAT를 활성화합니다.
object network	네트워크 객체를 만듭니다.
object-group network	네트워크 객체 그룹을 만듭니다.
show running-config object network	네트워크 객체 컨피그레이션을 표시합니다.

host(parameters)

RADIUS 어카운팅을 사용하여 상호 작용할 호스트를 지정하려면 radius-accounting 매개변수 컨피그레이션 모드에서 **host** 명령을 사용합니다. 이는 policy-map type inspect radius-accountin 하위 **모드에서 parameters** 명령을 사용하여 액세스합니다. 지정된 호스트를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

host *address* [**key** *secret*]

no host *address* [**key** *secret*]

구문 설명

host	RADIUS 어카운팅 메시지를 보내는 단일 엔드포인트를 지정합니다.
address	RADIUS 어카운팅 메시지를 보내는 클라이언트 또는 서버의 IP 주소.
key	어카운팅 메시지의 무료(gratuitous) 사본을 보내는 엔드포인트의 암호를 지정하는 선택 사항 키워드.
secret	메시지 검증에 쓰일 어카운팅 메시지를 보내는 엔드포인트의 공유 암호키. 최대 128자의 영숫자입니다.

기본값

no 옵션은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Radius-accounting 매개변수 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령의 다중 인스턴스가 허용됩니다.

예

다음 예에서는 RADIUS 어카운팅으로 호스트를 지정하는 방법을 보여줍니다.

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# host 209.165.202.128 key cisco123
```

관련 명령

명령	설명
inspect radius-accounting	RADIUS 어카운팅에 대한 검사를 설정합니다.
parameters	검사 정책 맵에 대한 매개변수를 설정합니다.

hostname

ASA 호스트 이름을 설정하려면 글로벌 컨피그레이션 모드에서 **hostname** 명령을 사용합니다. 기본 호스트 이름을 복원하려면 이 명령의 **no** 형식을 사용합니다.

hostname *name*

no hostname [*name*]

구문 설명

name	최대 63자의 호스트 이름을 지정합니다. 호스트 이름은 문자 또는 숫자로 시작하고 끝나야 하며 그 밖의 자리에는 문자, 숫자 또는 하이픈만 사용할 수 있습니다.

기본값

기본 호스트 이름은 플랫폼에 따라 달라집니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	(하이픈을 제외하고) 영숫자가 아닌 문자는 더 이상 사용할 수 없습니다.

사용 지침

호스트 이름이 명령줄 프롬프트에 나타나며, 여러 디바이스와의 세션을 설정한 경우 호스트 이름은 명령을 입력할 위치를 파악하는 데 도움이 됩니다. 다중 컨텍스트 모드에서는 시스템 실행 영역에서 설정한 호스트 이름이 모든 컨텍스트의 명령줄 프롬프트에 나타납니다.

어떤 컨텍스트 내에서 선택적으로 설정한 호스트 이름은 명령줄에 나타나지 않지만, **banner** 명령 **$(hostname)** 토큰을 통해 사용할 수 있습니다.

예

다음 예에서는 호스트 이름을 firewall1로 설정합니다.

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

관련 명령

명령	설명
banner	로그인, 오늘의 메시지, 활성 배너를 설정합니다.
domain-name	기본 도메인 이름을 설정합니다.

hpm topn enable

ASA통해 연결되는 최상위 호스트의 ASDM에서 실시간 보고서를 활성화하려면 글로벌 컨피그레이션 모드에서 **hpm topn enable** 명령을 사용합니다. 호스트 보고를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

hpm topn enable

no hpm topn enable

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.3(1)	이 명령을 도입했습니다.

사용 지침

시스템 성능을 극대화하기 위해 이 명령을 비활성화하려는 경우가 있습니다. 이 명령은 ASDM Home > Firewall Dashboard > Top 200 Hosts 창을 채웁니다.

예

다음 예에서는 최상위 호스트 보고를 활성화합니다.

```
ciscoasa(config)# hpm topn enable
```

관련 명령

명령	설명
clear configure hpm	HPM 컨피그레이션을 지웁니다.
show running-config hpm	HPM 컨피그레이션을 표시합니다.

hsi

H.323 프로토콜 검사를 위해 HSI 그룹에 HSI를 추가하려면 hsi 그룹 컨피그레이션 모드에서 **hsi** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

hsi *ip_address*

no hsi *ip_address*

구문 설명

ip_address	추가할 호스트의 IP 주소. HSI 그룹당 최대 5개의 HSI가 허용됩니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Hsi 그룹 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 H.323 검사 정책 맵에서 HSI 그룹에 HSI를 추가하는 방법을 보여줍니다.

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

관련 명령

명령	설명
class-map	레이어 3/4 클래스 맵을 만듭니다.
endpoint	HSI 그룹에 엔드포인트를 추가합니다.
hsi-group	HSI 그룹을 만듭니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

hsi-group

H.323 프로토콜 검사를 위해 HSI 그룹을 정의하고 hsi 그룹 컨피그레이션 모드를 시작하려면 매개변수 컨피그레이션 모드에서 **hsi-group** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

hsi-group *group_id*

no hsi-group *group_id*

구문 설명

group_id	HSI 그룹 ID 번호이며, 범위는 0~2147483647입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 H.323 검사 정책 맵에서 HSI 그룹을 구성하는 방법을 보여줍니다.

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

관련 명령

명령	설명
class-map	레이어 3/4 클래스 맵을 만듭니다.
endpoint	HSI 그룹에 엔드포인트를 추가합니다.
hsi	HSI 그룹에 HSI를 추가합니다.
policy-map	레이어 3/4 정책 맵을 만듭니다.
show running-config policy-map	현재 정책 맵 컨피그레이션을 모두 표시합니다.

html-content-filter

이 사용자 또는 그룹 정책에 대해 WebVPN 세션에서 Java, ActiveX, 이미지, 스크립트, 쿠키를 필터링하려면 webvpn 컨피그레이션 모드에서 **html-content-filter** 명령을 사용합니다. 콘텐츠 필터를 제거하려면 이 명령의 **no** 형식을 사용합니다.

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

구문 설명

cookies	이미지에서 쿠키를 제거하여 제한적인 광고 필터링 및 개인 정보 보호를 제공합니다.
images	이미지 참조를 제거합니다(<IMG> 태그 제거).
java	Java 및 ActiveX 참조를 제거합니다(<EMBED>, <APPLET>, <OBJECT> 태그 제거).
none	필터링이 없음을 나타냅니다. null 값을 설정하여 필터링을 허용하지 않습니다. 필터링 값을 상속할 수 없게 합니다.
scripts	스크립팅 참조를 제거합니다(<SCRIPT> 태그 제거).

기본값

필터링이 일어나지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

html-content-filter none 명령을 통해 생성된 null 값을 포함하여 모든 콘텐츠 필터를 제거하려면 이 명령의 **no** 형식을 인수 없이 사용합니다. **no** 옵션은 다른 그룹 정책에서 값을 상속하는 것을 허용합니다. HTML 콘텐츠 필터를 상속할 수 없게 하려면 **html-content-filter none** 명령을 사용합니다.

이 명령을 2번째 사용하면 이전의 설정을 재정의합니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 Java 및 Active X, 쿠키, 이미지의 필터링을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# html-content-filter java cookies images
```

관련 명령

명령	설명
webvpn	그룹 정책 또는 사용자 이름에 적용되는 매개변수를 구성하기 위해 webvpn 컨피그레이션 모드를 시작할 수 있게 합니다. 글로벌 컨피그레이션 모드를 시작하여 WebVPN을 위한 전역 설정을 구성할 수 있습니다.

http

ASA의 내부에 있는 HTTP 서버에 액세스할 수 있는 호스트를 지정하려면 글로벌 컨피그레이션 모드에서 **http** 명령을 사용합니다. 하나 이상의 호스트를 제거하려면 이 명령의 **no** 형식을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 형식을 인수 없이 사용합니다.

http *ip_address subnet_mask interface_name*

no http

구문 설명

interface_name	호스트가 HTTP 서버에 액세스하기 위해 거치는 ASA 인터페이스의 이름을 제공합니다.
ip_address	HTTP 서버에 액세스할 수 있는 호스트의 IP 주소를 제공합니다.
subnet_mask	HTTP 서버에 액세스할 수 있는 호스트의 서브넷 마스크를 제공합니다.

기본값

어떤 호스트도 HTTP 서버에 액세스할 수 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 IP 주소가 10.10.99.1, 서브넷 마스크가 255.255.255.255인 호스트가 외부 인터페이스를 통해 HTTP 서버에 액세스하도록 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# http 10.10.99.1 255.255.255.255 outside
```

다음 예에서는 임의의 호스트가 외부 인터페이스를 통해 HTTP 서버에 액세스하도록 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

관련 명령

명령	설명
clear configure http	HTTP 컨피그레이션을 제거합니다. HTTP 서버를 비활성화하고 HTTP 서버에 액세스할 수 있는 호스트를 제거합니다.
http authentication-certificate	ASA와의 HTTPS 연결을 설정하는 사용자에게 인증서를 통한 인증을 요구합니다.
http redirect	ASA에서 HTTPS에 HTTP 연결을 리디렉션하도록 지정합니다.
http server enable	HTTP 서버를 활성화합니다.
show running-config http	HTTP 서버에 액세스할 수 있는 호스트 및 HTTP 서버의 활성화 여부를 표시합니다.

http authentication-certificate

ASDM HTTPS 연결에서 인증을 위한 인증서를 요구하려면 글로벌 컨피그레이션 모드에서 **http authentication-certificate** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이 명령의 **no** 버전을 사용합니다. 컨피그레이션에서 모든 **http authentication-certificate** 명령을 제거하려면 **no** 버전을 인수 없이 사용합니다.

ASA는 PKI 신뢰 지점을 대상으로 인증서를 검증합니다. 인증서가 검증을 통과하지 못하면 ASA는 SSL 연결을 종료합니다.

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

구문 설명

interface	인증서 인증을 요구하는 ASA의 인터페이스를 지정합니다.

기본값

HTTP 인증서 인증은 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0.3	**ssl certificate-authentication** 명령을 우선적으로 사용함에 따라 이 명령은 사용 중단했습니다.
8.2.1	이 명령을 다시 추가했습니다. 전역 **ssl certificate-authentication** 명령은 역호환성을 위해 유지했습니다.
8.4.7, 9.1.3	인증서 전용 인증을 활성화했습니다. 이전에는 **aaa authentication http console** 명령을 활성화한 경우에만 사용자 인증에 인증서 인증을 추가했습니다.

사용 지침

각 인터페이스에 대해 인증서 인증을 구성함으로써 신뢰받는/내부 인터페이스의 연결은 인증서를 제공할 필요 없습니다. 이 명령을 여러 번 사용하여 여러 인터페이스에서 인증서 인증을 활성화할 수 있습니다.

예

다음 예에서는 outside 및 external이라는 인터페이스와 연결하는 클라이언트에 대해 인증서 인증을 요구하는 방법을 보여줍니다.

```
ciscoasa(config)# http authentication-certificate inside
ciscoasa(config)# http authentication-certificate external
```

관련 명령

명령	설명
clear configure http	HTTP 컨피그레이션을 제거합니다. HTTP 서버를 비활성화하고 HTTP 서버에 액세스할 수 있는 호스트를 제거합니다.
HTTP	HTTP 서버에 액세스할 수 있는 호스트를 IP 주소 및 서브넷 마스크로 지정합니다. 호스트가 HTTP 서버에 액세스하기 위해 지나는 ASA 인터페이스를 지정합니다.
http redirect	ASA에서 HTTPS에 HTTP 연결을 리디렉션하도록 지정합니다.
http server enable	HTTP 서버를 활성화합니다.
show running-config http	HTTP 서버에 액세스할 수 있는 호스트 및 HTTP 서버의 활성화 여부를 표시합니다.
ssl authentication-certificate	SSL 연결에 대해 인증서를 요구합니다.

http[s](parameters)

scansafe 검사 정책 맵에 대해 서비스 유형을 지정하려면 매개변수 컨피그레이션 모드에서 **http**[**s**] 명령을 사용합니다. 서비스 유형을 제거하려면 이 명령의 **no** 형식을 사용합니다. 먼저 **policy-map type inspect scansafe** 명령을 입력하여 매개변수 컨피그레이션 모드에 액세스할 수 있습니다.

{**http** | **https**}

no {**http** | **https**}

구문 설명

이 명령은 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
9.0(1)	이 명령을 도입했습니다.

사용 지침

Scansafe 검사 정책 맵에 대해 서비스 유형을 하나만(**http** 또는 **https**) 지정할 수 있습니다. 기본값은 없습니다. 유형을 지정해야 합니다.

예

다음 예에서는 검사 정책 맵을 만들고 서비스 유형을 HTTP로 설정합니다.

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
```

관련 명령

명령	설명
class-map type inspect scansafe	화이트리스트에 있는 사용자 및 그룹에 대한 검사 클래스 맵을 만듭니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없을 경우 기본 사용자 이름 및/또는 그룹을 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	어떤 화이트리스트에 대해 사용자 또는 그룹을 매칭합니다.
policy-map type inspect scansafe	규칙에 대한 필수 매개변수를 구성하고 선택적으로 화이트리스트를 식별할 수 있도록 검사 정책 맵을 만듭니다.
retry-count	재시도 카운터 값을 입력합니다. 이는 ASA에서 Cloud Web Security 프록시 서버의 가용성을 확인하기 위해 폴링할 때까지 기다리는 시간입니다.
scansafe	다중 컨텍스트 모드에서 컨텍스트별 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN 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 연결할 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.

http-comp

특정 그룹 또는 사용자에 대해 WebVPN 연결을 통한 HTTP 데이터의 압축을 활성화하려면 group-policy webvpn 및 username webvpn 컨피그레이션 모드에서 **http-comp** 명령을 사용합니다. 컨피그레이션에서 이 명령을 제거하고 값이 상속되게 하려면 이 명령의 **no** 형식을 사용합니다.

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

구문 설명

gzip	그룹 또는 사용자에 대해 압축을 활성화하도록 지정합니다.
none	그룹 또는 사용자에 대해 압축을 비활성화하도록 지정합니다.

기본값

기본적으로 압축을 활성 상태로 설정됩니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Group-policy webvpn 컨피그레이션	• 예	—	• 예	—	—
사용자 이름 webvpn 컨피그레이션	• 예	—	• 예	—	—

명령 기록

릴리스	수정 사항
7.1(1)	이 명령을 도입했습니다.

사용 지침

WebVPN 연결에서는 글로벌 컨피그레이션 모드에서 구성된 **compression** 명령이 그룹 정책 및 사용자 이름 webvpn 컨피그레이션 모드에서 구성된 **http-comp** 명령을 재정의합니다.

예

다음 예에서는 sales라는 그룹 정책에 대해 압축을 비활성화합니다.

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# http-comp none
```

관련 명령

명령	설명
compression	모든 SVC, WebVPN, IPsec VPN 연결에 대해 압축을 활성화합니다.

http-proxy(call-home)

스마트 라이센스 및 Smart Call Home을 위한 HTTP(S) 프록시를 설정하려면 call-home 컨피그레이션 모드에서 **http-proxy** 명령을 사용합니다. 프록시를 제거하려면 이 명령의 **no** 형식을 사용합니다.

http-proxy *ip_address* **port** *port*

no http-proxy [*ip_address* **port** *port*]

구문 설명

ip_address	HTTP 프록시 서버의 IP 주소를 설정합니다.
port *port*	HTTP 프록시의 포트 번호를 설정합니다. 예를 들어, HTTPS 서버는 443을 사용합니다.

명령 기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Call-home 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

릴리스	수정 사항
9.3(2)	이 명령을 도입했습니다.

사용 지침

이 명령은 Smart Call Home 및 스마트 라이센스를 위해 전역에서 HTTP 또는 HTTPS 프록시를 설정합니다.

예

다음 예에서는 HTTP 프록시를 설정합니다.

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

관련 명령

명령	설명
call-home	Smart Call Home을 구성합니다. 스마트 라이센스에서는 Smart Call Home 인프라를 사용합니다.
clear configure license	스마트 라이센스 컨피그레이션을 지웁니다.
feature tier	스마트 라이센스의 기능 계층을 설정합니다.
license smart	스마트 라이센스를 위해 라이센스 자격을 요청할 수 있습니다.
license smart deregister	License Authority에서 디바이스의 등록을 취소합니다.
license smart register	License Authority에 디바이스를 등록합니다.
license smart renew	등록 또는 라이센스 자격을 갱신합니다.
service call-home	Smart Call Home을 활성화합니다.
show license	스마트 라이센스 상태를 표시합니다.
show running-config license	스마트 라이센스 컨피그레이션을 표시합니다.
throughput level	스마트 라이센스를 위한 처리량 레벨을 설정합니다.

http-proxy(dap)

HTTP 프록시 포트 전달을 활성화하거나 비활성화하려면 dap-webvpn 컨피그레이션 모드에서 **http-proxy** 명령을 사용합니다. 컨피그레이션에서 특성을 제거하려면 이명령의 **no** 형식을 사용합니다.

http-proxy {**enable** | **disable** | **auto-start**}

no http-proxy

구문 설명

auto-start	DAP 레코드에 대해 HTTP 프록시 포트 전달을 활성화하고 자동으로 시작합니다.
enable/disable	DAP 레코드에 대해 HTTP 프록시 포트 전달을 활성화하거나 비활성화합니다.

기본값

기본값 또는 기본 동작이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

	방화벽 모드		보안 컨텍스트		
				다중	
명령 모드	라우팅	투명	단일	컨텍스트	시스템
Dap webvpn 컨피그레이션	• 예	• 예	• 예	—	—

명령 기록

릴리스	수정 사항
8.0(2)	이 명령을 도입했습니다.

사용 지침

ASA는 다양한 소스의 특성 값을 적용할 수 있습니다. 다음 계층 구조에 따라 적용합니다.

1. DAP 레코드
2. 사용자 이름
3. 그룹 정책
4. 터널 그룹에 대한 그룹 정책
5. 기본 그룹 정책

특성의 DAP 값은 사용자, 그룹 정책 또는 터널 그룹에 대해 구성된 값보다 우선순위가 높습니다.

DAP 레코드에 대한 특성을 활성화하거나 비활성화하면 ASA는 그 값을 강제적으로 적용합니다. 이를테면 dap webvpn 컨피그레이션 모드에서 HTTP 프록시를 비활성화하면 ASA는 더 이상 값을 찾지 않습니다. 그 대신 **http-proxy** 명령에 대해 **no** 값을 사용하면 그 특성은 DAP 레코드에 없으므로, ASA는 사용자 이름, 필요하다면 그룹 정책의 AAA 특성까지 내려와 적용할 값을 찾습니다.

예

다음 예에서는 Finance라는 DAP 레코드에 대해 HTTP 프록시 포트 전달을 활성화하는 방법을 보여줍니다.

```
ciscoasa (config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# http-proxy enable
ciscoasa(config-dap-webvpn)#
```

관련 명령

명령	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
show running-config dynamic-access-policy-record	모든 DAP 레코드 또는 명명된 DAP 레코드에 대해 실행 중인 컨피그레이션을 표시합니다.

http-proxy(webvpn)

ASA에서 HTTP 요청 처리에 외부 프록시 서버를 사용하도록 구성하려면 webvpn 컨피그레이션 모드에서 **http-proxy** 명령을 사용합니다. 컨피그레이션에서 HTTP 프록시 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

http-proxy {*host* [*port*] [**exclude** `url`] | **pac** *pacfile*} [**username** *username* {**password** *password*}]

no http-proxy

구문 설명

host	외부 HTTP 프록시 서버의 호스트 이름 또는 IP 주소.
pac *pacfile*	하나 이상의 프록시를 지정하는 JavaScript 기능을 포함한 PAC 파일을 나타냅니다.
password	(선택 사항이며, 사용자 이름을 지정할 경우에만 사용 가능) 기본적인 프록시 인증을 제공하기 위해 각 HTTP 프록시 요청에 비밀번호를 추가하려면 이 키워드를 사용합니다.
password	각 HTTP 요청에서 프록시 서버에 보낼 비밀번호.
port	(선택 사항) HTTP 프록시 서버에서 사용하는 포트 번호. 기본 포트는 80입니다. 사용자가 값을 제공하지 않으면 ASA는 이 포트를 사용합니다. 범위는 1~65535입니다.
url	프록시 서버에 전송될 수 있는 URL에서 제외할 URL 또는 쉼표로 구분된 여러 URL의 목록을 입력합니다. 이 문자열은 길이 제한이 없지만, 전체 명령이 512자를 초과해서는 안 됩니다. 리터럴 URL을 지정하거나 다음 와일드카드를 사용할 수 있습니다. • *****는 슬래시(/), 마침표(.)를 포함한 어떤 문자열과도 매칭합니다. 이 와일드카드는 영숫자 문자열과 함께 사용해야 합니다. • **?** 슬래시, 마침표를 포함하여 단일 문자와 매칭합니다. • [*x*-*y*]는 *x*~*y* 범위에 속한 임의의 단일 문자와 매칭합니다. 여기서 *x*는 ANSI 문자 세트의 한 문자, *y* 역시 이 세트의 또 다른 문자를 나타냅니다. • [**!***x*-*y*]는 이 범위에 속하지 않는 단일 문자와 매칭합니다.
username	(선택 사항) 기본적인 프록시 인증을 제공하기 위해 각 HTTP 프록시 요청에 사용자 이름을 추가하려면 이 키워드를 입력합니다.
username	각 HTTP 요청에서 프록시 서버에 보낼 사용자 이름.

기본값

기본적으로 어떤 HTTP 프록시 서버도 구성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0(2)	**exclude**, **username**, **password** 키워드를 추가했습니다.

사용 지침

조직에서 제어하는 서버를 통한 인터넷 액세스를 요구함으로써 추가적인 필터링을 통해 안전한 인터넷 액세스 및 관리 제어를 보장할 수 있습니다.

ASA는 **http-proxy** 명령의 단일 인스턴스만 지원합니다. 이 명령의 어떤 인스턴스가 이미 실행 중인 컨피그레이션에 있는 상태에서 또 다른 인스턴스를 입력할 경우 CLI는 이전의 인스턴스를 덮어씁니다. **show running-config webvpn** 명령을 입력할 경우 CLI는 실행 중인 컨피그레이션의 모든 **http-proxy** 명령을 나열합니다. 이 응답에 어떤 **http -proxy** 명령도 포함되지 않는다면 아무 것도 없는 것입니다.

참고 Proxy NTLM 인증은 **http-proxy**에서 지원되지 않습니다. 인증 없는 프록시와 기본 인증의 프록시만 지원됩니다.

예

다음 예에서는 IP 주소가 209.165. 201.2이고 기본 포트 443을 사용하는 HTTP 프록시 서버의 사용을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# http-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

다음 예에서는 동일한 프록시 서버의 사용을 구성하고 각 HTTP 요청과 함께 사용자 이름과 비밀번호를 보내는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

다음 예에서는 동일한 명령을 보여주지만, ASA에서 HTTP 요청에서 www.example.com이라는 특정 URL을 수신할 경우 이를 프록시 서버에 전달하지 않고 그 요청을 확인합니다.

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
ciscoasa(config-webvpn)
```

다음 예에서는 **exclude** 옵션을 사용하는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
12345678
ciscoasa(config-webvpn)
```

다음 예에서는 **pac** 옵션을 사용하는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

관련 명령

명령	설명
https-proxy	HTTPS 요청을 처리하기 위해 외부 프록시 서버를 사용하도록 구성합니다.
show running-config webvpn	HTTP 및 HTTPS 프록시 서버를 포함하여 SSL VPN을 위해 실행 중인 컨피그레이션을 표시합니다.

http redirect

ASA에서 HTTPS에 HTTP를 리디렉션하도록 지정하려면 글로벌 컨피그레이션 모드에서 **http redirect** 명령을 사용합니다. 컨피그레이션에서 지정된 **http redirect** 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다. 컨피그레이션에서 모든 **http redirect** 명령을 제거하려면 이 명령의 **no** 형식을 인수 없이 사용합니다.

http redirect *interface* [*port*]

no http redirect [*interface*]

구문 설명

interface	ASA에서 HTTP 요청을 HTTPS로 리디렉션해야 하는 인터페이스를 식별합니다.
port	ASA에서 HTTP 요청을 수신하는 포트를 식별합니다. 그 다음에는 이를 HTTPS로 리디렉션합니다. 기본적으로 포트 80에서 수신합니다.

기본값

HTTP 리디렉션은 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

인터페이스에서는 HTTP를 허용하는 액세스 목록이 필요합니다. 그렇지 않으면 ASA는 포트 80 또는 HTTP를 위해 구성하는 다른 어떤 포트에서도 수신하지 않습니다.

http redirect 명령이 실패할 경우 다음 메시지가 나타납니다.

```
"TCP port <port_number> on interface <interface_name> is in use by another feature. Please
choose a different port for the HTTP redirect service"
```

HTTP 리디렉션 서비스에 다른 포트를 사용합니다.

예

다음 예에서는 내부 인터페이스에 대해 HTTP 리디렉션을 구성하고 기본 포트 80을 유지하는 방법을 보여줍니다.

```
ciscoasa(config)# http redirect inside
```

관련 명령

명령	설명
clear configure http	HTTP 컨피그레이션을 제거합니다. HTTP 서버를 비활성화하고 HTTP 서버에 액세스할 수 있는 호스트를 제거합니다.
HTTP	HTTP 서버에 액세스할 수 있는 호스트를 IP 주소 및 서브넷 마스크로 지정합니다. 호스트가 HTTP 서버에 액세스하기 위해 지나는 ASA 인터페이스를 지정합니다.
http authentication-certificate	ASA와의 HTTPS 연결을 설정하는 사용자에게 인증서를 통한 인증을 요구합니다.
http server enable	HTTP 서버를 활성화합니다.
show running-config http	HTTP 서버에 액세스할 수 있는 호스트 및 HTTP 서버의 활성화 여부를 표시합니다.

http server enable

ASA HTTP 서버를 활성화하려면 글로벌 컨피그레이션 모드에서 **http server enable** 명령을 사용합니다. HTTP 서버를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

http server enable [*port*]

구문 설명

port	HTTP 연결에 사용할 포트. 범위는 1~65535입니다. 기본 포트는 443입니다.

기본값

HTTP 서버가 비활성화되어 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

예

다음 예에서는 HTTP 서버를 활성화하는 방법을 보여줍니다.

```
ciscoasa(config)# http server enable
```

관련 명령

명령	설명
clear configure http	HTTP 컨피그레이션을 제거합니다. HTTP 서버를 비활성화하고 HTTP 서버에 액세스할 수 있는 호스트를 제거합니다.
HTTP	HTTP 서버에 액세스할 수 있는 호스트를 IP 주소 및 서브넷 마스크로 지정합니다. 호스트가 HTTP 서버에 액세스하기 위해 지나는 ASA 인터페이스를 지정합니다.
http authentication-certificate	ASA와의 HTTPS 연결을 설정하는 사용자에게 인증서를 통한 인증을 요구합니다.
http redirect	ASA에서 HTTPS에 HTTP 연결을 리디렉션하도록 지정합니다.
show running-config http	HTTP 서버에 액세스할 수 있는 호스트 및 HTTP 서버의 활성화 여부를 표시합니다.

http server idle-timeout

ASA와의 ASDM 연결에 대한 유휴 타이머를 설정하려면 글로벌 컨피그레이션 모드에서 **http server idle-timeout** 명령을 사용합니다. 타이머를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

http server idle-timeout [*minutes*]

no http server idle-timeout [*minutes*]

구문 설명

minutes	유휴 타이머이며, 범위는 1분~1440분입니다.

기본값

기본 설정은 20분입니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 ASDM 세션의 유휴 타이머를 500분으로 설정합니다.

```
ciscoasa(config)# http server idle-timeout 500
```

관련 명령

명령	설명
clear configure http	HTTP 컨피그레이션을 제거합니다. HTTP 서버를 비활성화하고 HTTP 서버에 액세스할 수 있는 호스트를 제거합니다.
HTTP	HTTP 서버에 액세스할 수 있는 호스트를 IP 주소 및 서브넷 마스크로 지정하고 호스트가 HTTP 서버에 액세스하기 위해 지날 인터페이스를 지정합니다.
http authentication-certificate	ASA와의 HTTPS 연결을 설정하는 사용자에게 인증서를 통한 인증을 요구합니다.
http server enable	ASDM 세션을 위해 HTTP 서버를 활성화합니다.
http server session-timeout	ASA에 대한 ASDM 세션의 세션 시간을 제한합니다.
http redirect	ASA에서 HTTPS에 HTTP 연결을 리디렉션하도록 지정합니다.
show running-config http	HTTP 서버에 액세스할 수 있는 호스트 및 HTTP 서버의 활성화 여부를 표시합니다.

http server session-timeout

ASA와의 ASDM 연결에 대한 세션 시간 초과를 설정하려면 글로벌 컨피그레이션 모드에서 **http server session-timeout** 명령을 사용합니다. 타이머를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

http server session-timeout [*minutes*]

no http server session-timeout [*minutes*]

구문 설명

minutes	세션 시간 초과이며, 범위는 1분~1440분입니다.

기본값

세션 시간 초과는 비활성화되어 있습니다. ASDM 연결은 세션 시간 제한이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

예

다음 예에서는 ASDM 연결에 대한 세션 시간 초과를 1000분으로 설정합니다.

```
ciscoasa(config)# http server session-timeout 1000
```

관련 명령

명령	설명
clear configure http	HTTP 컨피그레이션을 제거합니다. HTTP 서버를 비활성화하고 HTTP 서버에 액세스할 수 있는 호스트를 제거합니다.
HTTP	HTTP 서버에 액세스할 수 있는 호스트를 IP 주소 및 서브넷 마스크로 지정하고 호스트가 HTTP 서버에 액세스하기 위해 지날 인터페이스를 지정합니다.
http authentication-certificate	ASA와의 HTTPS 연결을 설정하는 사용자에게 인증서를 통한 인증을 요구합니다.
http server enable	ASDM 세션을 위해 HTTP 서버를 활성화합니다.
http server idle-timeout	ASA에 대한 ASDM 세션의 유휴 시간을 제한합니다.
http redirect	ASA에서 HTTPS에 HTTP 연결을 리디렉션하도록 지정합니다.
show running-config http	HTTP 서버에 액세스할 수 있는 호스트 및 HTTP 서버의 활성화 여부를 표시합니다.

https-proxy

ASA에서 HTTPS 요청 처리에 외부 프록시 서버를 사용하도록 구성하려면 webvpn 컨피그레이션 모드에서 **https-proxy** 명령을 사용합니다. 컨피그레이션에서 HTTPS 프록시 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

https-proxy {*host* [*port*] [**exclude** *url*] | [**username** *username* {**password** *password*}]

no https-proxy

구문 설명

host	외부 HTTPS 프록시 서버의 호스트 이름 또는 IP 주소.
password	(선택 사항이며, 사용자 이름을 지정할 경우에만 사용 가능) 기본적인 프록시 인증을 제공하기 위해 각 HTTPS 프록시 요청에 비밀번호를 추가하려면 이 키워드를 사용합니다.
password	각 HTTPS 요청에서 프록시 서버에 보낼 비밀번호.
port	(선택 사항) HTTPS 프록시 서버에서 사용하는 포트 번호. 기본 포트는 443입니다. 사용자가 값을 제공하지 않으면 ASA는 이 포트를 사용합니다. 범위는 1~65535입니다.
url	프록시 서버에 전송될 수 있는 URL에서 제외할 URL 또는 쉼표로 구분된 여러 URL의 목록을 입력합니다. 이 문자열은 길이 제한이 없지만, 전체 명령이 512자를 초과해서는 안 됩니다. 리터럴 URL을 지정하거나 다음 와일드카드를 사용할 수 있습니다. • *는 슬래시(/), 마침표(.)를 포함한 어떤 문자열과도 매칭합니다. 이 와일드카드는 영숫자 문자열과 함께 사용해야 합니다. • **?** 슬래시, 마침표를 포함하여 단일 문자와 매칭합니다. • [*x*-*y*]는 *x*~*y* 범위에 속한 임의의 단일 문자와 매칭합니다. 여기서 *x*는 ANSI 문자 세트의 한 문자, *y* 역시 이 세트의 또 다른 문자를 나타냅니다. • [**!***x*-*y*]는 이 범위에 속하지 않는 단일 문자와 매칭합니다.
username	(선택 사항) 기본적인 프록시 인증을 제공하기 위해 각 HTTPS 프록시 요청에 사용자 이름을 추가하려면 이 키워드를 입력합니다.
username	각 HTTPS 요청에서 프록시 서버에 보낼 사용자 이름.

기본값

기본적으로 어떤 HTTPS 프록시 서버도 구성되지 않습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.0(2)	**exclude**, **username**, **password** 키워드를 추가했습니다.

사용 지침

조직에서 제어하는 서버를 통한 인터넷 액세스를 요구함으로써 추가적인 필터링을 통해 안전한 인터넷 액세스 및 관리 제어를 보장할 수 있습니다.

ASA는 **https-proxy** 명령의 단일 인스턴스만 지원합니다. 이 명령의 어떤 인스턴스가 이미 실행 중인 컨피그레이션에 있는 상태에서 또 다른 인스턴스를 입력할 경우 CLI는 이전의 인스턴스를 덮어씁니다. **show running-config webvpn** 명령을 입력할 경우 CLI는 실행 중인 컨피그레이션의 모든 **https-proxy** 명령을 나열합니다. 이 응답에 어떤 **https-proxy** 명령도 포함되지 않는다면 아무 것도 없는 것입니다.

예

다음 예에서는 IP 주소가 209.165. 201.2이고 기본 포트 443을 사용하는 HTTPS 프록시 서버의 사용을 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# https-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

다음 예에서는 동일한 프록시 서버의 사용을 구성하고 각 HTTPS 요청과 함께 사용자 이름과 비밀번호를 보내는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

다음 예에서는 동일한 명령을 보여주지만, ASA에서 HTTPS 요청에서 www.example.com이라는 특정 URL을 수신할 경우 이를 프록시 서버에 전달하지 않고 그 요청을 확인합니다.

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
ciscoasa(config-webvpn)
```

다음 예에서는 **exclude** 옵션을 사용하는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
ciscoasa(config-webvpn)
```

다음 예에서는 **pac** 옵션을 사용하는 방법을 보여줍니다.

```
ciscoasa(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

관련 명령

명령	설명
http-proxy	HTTP 요청을 처리하기 위해 외부 프록시 서버를 사용하도록 구성합니다.
show running-config webvpn	HTTP 및 HTTPS 프록시 서버를 포함하여 SSL VPN을 위해 실행 중인 컨피그레이션을 표시합니다.

hw-module module allow-ip

ASA 5505의 AIP SSC에서 관리 IP 주소에 액세스할 수 있는 호스트를 설정하려면 특별 권한 EXEC 모드에서 **hw-module module allow-ip** 명령을 사용합니다.

hw-module module 1 allow-ip *ip_address netmask*

구문 설명

1	슬롯 번호를 지정하는데, 항상 1입니다.
ip_ address	호스트 IP 주소를 지정합니다.
netmask	서브넷 마스크를 지정합니다.

기본값

공장 기본 컨피그레이션에서 192.168.1.5~192.168.1.254의 호스트는 IPS 모듈을 관리할 수 있습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

이 명령은 SSC 상태가 UP일 때만 유효합니다.

이러한 설정은 ASA 컨피그레이션이 아닌 IPS 애플리케이션 컨피그레이션에 기록됩니다. ASA에서 **show module details** 명령을 사용하여 이 설정을 볼 수 있습니다.

또는 IPS 애플리케이션 **setup** 명령을 사용하여 IPS CLI에서 이 설정을 구성할 수도 있습니다.

예

다음 예에서는 SSC에서 호스트 매개변수를 구성하는 방법을 보여줍니다.

```
ciscoasa# hw-module module 1 allow-ip 209.165.201.29 255.255.255.0
```

관련 명령

명령	설명
hw-module module ip	AIP SSC 관리 주소를 구성합니다.
show module	모듈 상태 정보를 표시합니다.

hw-module module ip

ASA 5505의 AIP SSC에서 관리 IP 주소를 구성하려면 특별 권한 EXEC 모드에서 **hw-module module ip** 명령을 사용합니다.

hw-module module 1 ip *ip_address netmask gateway*

구문 설명

1	슬롯 번호를 지정하는데, 항상 1입니다.
gateway	게이트웨이 IP 주소를 지정합니다.
ip_address	관리 IP 주소를 지정합니다.
netmask	서브넷 마스크를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
8.2(1)	이 명령을 도입했습니다.

사용 지침

이 주소가 ASA VLAN IP 주소와 동일한 서브넷에 있어야 합니다. 예를 들어, ASA용 VLAN에 10.1.1.1을 지정한 경우 IPS 관리 주소로 10.1.1.2와 같은 다른 주소를 네트워크에 지정합니다.

관리 스테이션이 직접 연결된 ASA 네트워크에 있을 경우 게이트웨이가 IPS 관리 VLAN에 지정된 ASA IP 주소가 되도록 설정합니다. 설명한 예에서는 게이트웨이를 10.1.1.1로 설정합니다. 관리 스테이션이 원격 네트워크에 있을 경우 게이트웨이는 IPS 관리 VLAN 업스트림 라우터의 주소가 되도록 설정합니다.

참고 이러한 설정은 ASA 컨피그레이션이 아닌 IPS 애플리케이션 컨피그레이션에 기록됩니다. ASA에서 **show module details** 명령을 사용하여 이 설정을 볼 수 있습니다.

또는 IPS 애플리케이션 **setup** 명령을 사용하여 IPS CLI에서 이 설정을 구성할 수도 있습니다.

예

다음 예에서는 IPS 모듈의 관리 주소를 구성하는 방법을 보여줍니다.

```
ciscoasa# hw-module module 1 ip 209.165.200.254 255.255.255.224 209.165.200.225
```

관련 명령

명령	설명
hw-module module allow-ip	AIP SSC 관리 호스트 주소를 구성합니다.
show module	모듈 상태 정보를 표시합니다.

hw-module module password-reset

하드웨어 모듈의 기본 관리 사용자를 위한 비밀번호를 기본값으로 재설정하려면 특별 권한 EXEC 모드에서 **hw-module module password-reset** 명령을 사용합니다.

hw-module module 1 password-reset

구문 설명

1	슬롯 번호를 지정하는데, 항상 1입니다.

기본값

기본 사용자 이름과 비밀번호는 모듈에 따라 달라집니다.

- IPS 모듈—사용자 이름: **cisco**, 비밀번호: **cisco**
- CSC 모듈—사용자 이름: **cisco**, 비밀번호: **cisco**
- ASA CX 모듈—사용자 이름: **admin**, 비밀번호: **Admin123**

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.2(2)	이 명령을 도입했습니다.
8.4(4.1)	ASA CX 모듈에 대한 지원을 추가했습니다.

사용 지침

이 명령은 하드웨어 모듈이 작동(Up) 상태에 있고 비밀번호 재설정을 지원하는 경우에만 유효합니다. IPS에서는 이 모듈이 IPS Version 6.0 이상을 실행하는 경우에 비밀번호 재설정이 지원됩니다. 비밀번호를 재설정한 후 모듈 애플리케이션을 사용하여 고유한 값으로 변경해야 합니다. 모듈 비밀번호를 재설정하면 모듈이 재부팅됩니다. 모듈이 재부팅하는 동안에는 서비스를 사용할 수 없습니다. 여기에 몇 분이 걸릴 수 있습니다. **show module** 명령을 실행하여 모듈 상태를 모니터링할 수 있습니다.

이 명령은 항상 확인 프롬프트를 표시합니다. 명령이 성공하면 다른 출력은 나타나지 않습니다. 명령이 실패하면 실패 원인을 설명하는 오류 메시지가 나타납니다. 다음과 같은 오류 메시지가 표시될 수 있습니다.

```
Unable to reset the password on the module in slot 1

Unable to reset the password on the module in slot 1 - unknown module state

Unable to reset the password on the module in slot 1 - no module installed

Failed to reset the password on the module in slot 1 - module not in Up state

Unable to reset the password on the module in slot 1 - unknown module type

The module in slot 1 does not support password reset

Unable to reset the password on the module in slot 1 - no application found

The SSM application version does not support password reset

Failed to reset the password on the module in slot 1
```

예

다음 예에서는 슬롯 1의 하드웨어 모듈에서 비밀번호를 재설정합니다.

```
ciscoasa(config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

관련 명령

명령	설명
hw-module module recover	TFTP 서버에서 복구 이미지를 로드하여 모듈을 복구합니다.
hw-module module reload	모듈 소프트웨어를 다시 로드합니다.
hw-module module reset	모듈 하드웨어를 종료하고 재설정합니다.
hw-module module shutdown	컨피그레이션 데이터를 잃지 않고 전원을 끄기 위한 준비 단계로 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

hw-module module recover

TFTP 서버에서 설치된 모듈로 복구 소프트웨어 이미지를 로드하거나 TFTP 서버에 액세스하기 위해 네트워크 설정을 구성하려면 특별 권한 EXEC 모드에서 **hw-module module recover** 명령을 사용합니다. 이를테면 모듈에서 로컬 이미지를 로드할 수 없는 경우에 이 명령을 사용하여 모듈을 복구해야 합니다.

hw-module module 1 recover {**boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *module_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*]}

구문 설명

1	슬롯 번호를 지정하는데, 항상 1입니다.
boot	이 모듈의 복구를 시작하고 **configure** 키워드 설정에 따라 복구 이미지를 다운로드합니다. 그러면 새 이미지에서 모듈이 재부팅됩니다.
configure	복구 이미지를 다운로드하기 위해 네트워크 매개변수를 구성합니다. **configure** 키워드 다음에 네트워크 매개변수를 입력하지 않을 경우 전체 매개변수에 대한 프롬프트가 나타납니다. 이 명령에서는 TFTP 서버의 URL, 관리 인터페이스 IP 주소 및 넷마스크, 게이트웨이 주소, VLAN ID를 묻습니다. 이러한 네트워크 매개변수는 ROMMON에서 구성합니다. 모듈 애플리케이션에서 구성한 네트워크 매개변수는 ROMMON에서 사용할 수 없으므로 여기서 별도로 설정해야 합니다.
gateway *gateway_ip_address*	(선택 사항) SSM 관리 인터페이스를 통해 TFTP 서버에 액세스하기 위한 게이트웨이 IP 주소.
ip *module_address*	(선택 사항) 모듈 관리 인터페이스의 IP 주소.
stop	복구 작업을 중지하고 복구 이미지의 다운로드를 중지합니다. 모듈은 원래의 이미지에서 부팅합니다. **hw-module module recover boot** 명령을 사용하여 복구를 시작하고 30초~45초 내에 이 명령을 입력해야 합니다. 이 기간이 지난 후에 **stop** 명령을 실행하면 모듈이 응답하지 않는 등의 예기치 않은 결과가 생길 수 있습니다.
url *tfp_url*	(선택 사항) TFTP 서버에 있는 이미지의 URL이며, 그 형식은 다음과 같습니다. **tftp://***server*/[*path*/]*filename*
vlan *vlan_id*	(선택 사항) 관리 인터페이스의 VLAN ID를 지정합니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.

사용 지침

모듈에 오류가 발생하고 모듈 애플리케이션 이미지가 실행되지 않을 경우 TFTP 서버에서 모듈에 새 이미지를 재설치할 수 있습니다.

참고 이미지를 설치하기 위해 모듈 소프트웨어 내에서 **upgrade** 명령을 사용하지 마십시오.

지정한 TFTP 서버가 최대 60MB 크기의 파일을 전송할 수 있는지 확인합니다. 네트워크 및 이미지 크기에 따라 이 프로세스를 완료하는 데 약 15분 정도 걸릴 수 있습니다.

이 명령은 모듈이 작동(Up), 중지(Down), 무응답(Unresponsive) 또는 복구(Recovery) 상태일 때만 사용 가능합니다. 상태 정보는 **show module** 명령을 참조하십시오.

show module 1 recover 명령을 사용하여 복구 컨피그레이션을 볼 수 있습니다.

참고 이 명령은 ASA CX, ASA FirePOWER 모듈에서는 지원되지 않습니다.

예

다음 예에서는 모듈이 TFTP 서버로부터 이미지를 다운로드하도록 설정합니다.

```
ciscoasa# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

다음 예에서는 모듈을 복구합니다.

```
ciscoasa# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버그 정보를 표시합니다.
hw-module module reset	모듈을 종료하고 하드웨어 재설정을 수행합니다.
hw-module module reload	모듈 소프트웨어를 다시 로드합니다.
hw-module module shutdown	컨피그레이션 데이터를 잃지 않고 전원을 끄기 위한 준비 단계로 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

hw-module module reload

물리적 모듈을 위해 모듈 소프트웨어를 다시 로드하려면 특별 권한 EXEC 모드에서 **hw-module module reload** 명령을 사용합니다.

hw-module module 1 reload

구문 설명

1	슬롯 번호를 지정하는데, 항상 1입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.4(4.1)	ASA CX 모듈에 대한 지원을 추가했습니다.
9.2(1)	ASA FirePOWER 모듈에 대한 지원을 추가했습니다.

사용 지침

이 명령은 모듈을 다시 로드하기 전에 하드웨어 재설정도 수행하는 **hw-module module reset** 명령과 다릅니다.

이 명령은 모듈 상태가 작동(Up)일 때만 유효합니다. 상태 정보는 **show module** 명령을 참조하십시오.

예

다음 예에서는 슬롯 1에 모듈을 다시 로드합니다.

```
ciscoasa# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버깅 정보를 표시합니다.
hw-module module recover	TFTP 서버에서 복구 이미지를 로드하여 모듈을 복구합니다.
hw-module module reset	모듈을 종료하고 하드웨어 재설정을 수행합니다.
hw-module module shutdown	컨피그레이션 데이터를 잃지 않고 전원을 끄기 위한 준비 단계로 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

hw-module module reset

모듈 하드웨어를 재설정하고 모듈 소프트웨어를 다시 로드하려면 특별 권한 EXEC 모드에서 **hw-module module reset** 명령을 사용합니다.

hw-module module 1 reset

구문 설명

1	슬롯 번호를 지정하는데, 항상 1입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.4(4.1)	ASA CX 모듈에 대한 지원을 추가했습니다.
9.2(1)	ASA FirePOWER 모듈에 대한 지원을 추가했습니다.

사용 지침

모듈이 작동(Up) 상태일 때 **hw-module module reset** 명령은 재설정하기 전에 소프트웨어를 종료하라고 안내합니다.

hw-module module recover 명령을 사용하여 모듈을 복구할 수 있습니다(지원되는 경우). 모듈이 복구(Recover) 상태일 때 **hw-module module reset** 명령을 입력하면 모듈은 복구 프로세스를 중단하지 않습니다. **hw-module module reset** 명령은 모듈의 하드웨어 재설정을 수행하며, 하드웨어 재설정 후 모듈 복구가 계속됩니다. 모듈이 멈출 경우 복구 과정에서 모듈의 재설정이 필요할 수 있습니다. 하드웨어 재설정으로 문제가 해결될 수도 있습니다.

이 명령은 소프트웨어만 다시 로드할 뿐 하드웨어 재설정을 수행하지 않는 **hw-module module reload** 명령과 다릅니다.

이 명령은 모듈이 작동(Up), 중단(Down), 무응답(Unresponsive) 또는 복구(Recover) 상태일 때만 유효합니다. 상태 정보는 **show module** 명령을 참조하십시오.

예

다음 예에서는 작동(Up) 상태인 슬롯 1의 모듈을 재설정합니다.

```
ciscoasa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버깅 정보를 표시합니다.
hw-module module recover	TFTP 서버에서 복구 이미지를 로드하여 모듈을 복구합니다.
hw-module module reload	모듈 소프트웨어를 다시 로드합니다.
hw-module module shutdown	컨피그레이션 데이터를 잃지 않고 전원을 끄기 위한 준비 단계로 모듈 소프트웨어를 종료합니다.
show module	모듈 정보를 표시합니다.

hw-module module shutdown

모듈 소프트웨어를 종료하려면 특별 권한 EXEC 모드에서 **hw-module module shutdown** 명령을 사용합니다.

hw-module module 1 shutdown

구문 설명

1	슬롯 번호를 지정하는데, 항상 1입니다.

기본값

기본 동작 또는 값이 없습니다.

명령 모드

다음 표에서는 명령을 입력할 수 있는 모드를 보여줍니다.

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

명령 기록

릴리스	수정 사항
7.0(1)	이 명령을 도입했습니다.
8.4(4.1)	ASA CX 모듈에 대한 지원을 추가했습니다.
9.2(1)	ASA FirePOWER 모듈에 대한 지원을 추가했습니다.

사용 지침

모듈 소프트웨어를 종료하면 컨피그레이션 데이터를 잃지 않은 채 모듈의 전원을 안전하게 끌 수 있습니다.

이 명령은 모듈 상태가 작동(Up) 또는 무응답(Unresponsive)일 때만 유효합니다. 상태 정보는 **show module** 명령을 참조하십시오.

예

다음 예에서는 슬롯 1의 모듈을 종료합니다.

```
ciscoasa# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
ciscoasa#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

관련 명령

명령	설명
debug module-boot	모듈 부팅 프로세스에 대한 디버깅 정보를 표시합니다.
hw-module module recover	TFTP 서버에서 복구 이미지를 로드하여 모듈을 복구합니다.
hw-module module reload	모듈 소프트웨어를 다시 로드합니다.
hw-module module reset	모듈을 종료하고 하드웨어 재설정을 수행합니다.
show module	모듈 정보를 표시합니다.