Cisco ASA 시리즈 명령 참조, ASASM에 대한 T ~Z 명령 및 IOS 명령

Cisco Systems, Inc.
www.cisco.com

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.
각 지사의 주소, 전화번호 및 팩스 번호는
다음 Cisco 웹사이트에 나와 있습니다.
www.cisco.com/go/offices

텍스트 파트 번호: 해당 사항 없음, 온라인 전용

Cisco ASA 시리즈 명령 참조, ASASM에 대한 T ~Z 명령 및 IOS 명령

파 트　1

T~Z 명령

table-map through title

table-map

IP 라우팅 테이블이 BGP에서 학습한 경로로 업데이트될 때 메트릭 및 태그 값을 수정하려면 주소 패밀리 구성 모드에서 **table-map** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

table-map *map_name*

no table-map *map_name*

구문 설명

map_name	**route-map** 명령에서 맵 이름을 라우팅합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
주소 패밀리 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
9.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 **route-map** 명령으로 정의된 경로 맵 이름을 IP 라우팅 테이블에 추가합니다. 이 명령은 재배포를 구현하기 위해 태그 이름 및 경로 메트릭을 설정하는 데 사용됩니다.

경로 맵의 **match** 절을 **table-map** 명령에서 사용할 수 있습니다. IP 액세스 목록, 자동 시스템 경로 및 다음 홉 일치 절이 지원됩니다.

예

다음 주소 패밀리 구성 모드 예에서는 ASA 소프트웨어가 BGP에서 학습한 경로에 대한 태그 값을 자동으로 계산하고 IP 라우팅 테이블을 업데이트하도록 구성됩니다.

```
ciscoasa(config)# route-map tag
ciscoasa(config-route-map)# match as path 10
ciscoasa(config-route-map)# set automatic-tag

ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# table-map tag
```

관련 명령

Command(명령)	설명
address-family	address-family 구성 모드를 시작합니다.
route-map	라우팅 프로토콜 간에 경로를 재배포하는 조건을 정의합니다.

tcp-inspection

DNS over TCP 검사를 활성화하려면 파라미터 구성 모드에서 **tcp-inspection** 명령을 사용합니다. 프로토콜 적용을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

tcp-inspection

no tcp-inspection

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

DNS over TCP 검사는 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.6(2)	이 명령이 추가되었습니다.

사용 지침

DNS/TCP 포트 53 트래픽을 검사에 포함하려면 이 명령을 DNS 검사 정책 맵에 추가합니다. 이 명령이 없으면 UDP/53 DNS 트래픽만 검사됩니다. DNS/TCP 포트 53 트래픽이 DNS 검사를 적용하는 클래스에 포함되어 있는지 확인합니다. 검사 기본 클래스에는 TCP/53이 포함됩니다.

예

다음 예에서는 DNS 검사 정책 맵에서 DNS over TCP 검사를 활성화하는 방법을 보여 줍니다.

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

관련 명령

Command(명령)	설명
inspect dns	DNS 검사를 활성화합니다.
policy-map type inspect dns	DNS 검사 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

tcp-map

TCP 정규화 작업 집합을 정의하려면 전역 구성 모드에서 **tcp-map** 명령을 사용합니다. TCP 정규화 기능을 사용하면 탐지된 경우 ASA에서 삭제하는 비정상 패킷을 식별하는 조건을 지정할 수 있습니다. TCP 맵을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tcp-map *map_name*

no tcp-map *map_name*

구문 설명

map_name	TCP 맵 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
7.2(4)/8.0(4)	**invalid-ack**, **seq-past-window** 및 **synack-data** 하위 명령이 추가되었습니다.

사용 지침

이 기능은 Modular Policy Framework를 사용합니다. 먼저 **tcp-map** 명령을 사용하여 수행할 TCP 정규화 작업을 정의합니다. **tcp map** 명령은 TCP 정규화 작업을 정의하는 하나 이상의 명령을 입력할 수 있는 tcp-map 구성 모드를 시작합니다. 그런 다음 **class-map** 명령을 사용하여 TCP 맵을 적용할 트래픽을 정의합니다. 그런 다음 **policy-map** 명령을 입력하여 정책을 정의하고, **class** 명령을 입력하여 클래스 맵을 참조합니다. 클래스 구성 모드에서는 **set connection advanced-options** 명령을 입력하여 TCP 맵을 참조합니다. 마지막으로 **service-policy** 명령을 사용하여 정책 맵을 인터페이스에 적용합니다. Modular Policy Framework의 작동 방식에 대한 자세한 내용은 CLI 구성 가이드를 참고하십시오.

tcp-map 구성 모드에서 사용할 수 있는 명령은 다음과 같습니다.

check-retransmission	재전송 데이터 검사를 활성화 및 비활성화합니다.
checksum-verification	체크섬 확인을 활성화 및 비활성화합니다.
exceed-mss	피어에서 설정한 MSS를 초과하는 패킷을 허용하거나 삭제합니다.
invalid-ack	유효하지 않은 ACK가 포함된 패킷에 대한 작업을 설정합니다.

queue-limit	TCP 연결을 대기할 수 있는 비순차적 패킷의 최대 개수를 구성합니다. 이 명령은 ASA 5500 시리즈 적응형 ASA에서만 사용할 수 있습니다. PIX 500 시리즈 ASA에서는 대기열 제한이 3이며, 변경할 수 없습니다.
reserved-bits	ASA에서 예약된 플래그 정책을 설정합니다.
seq-past-window	past-window 시퀀스 번호가 있는 패킷, 즉 받은 TCP 패킷의 시퀀스 번호가 TCP 수신 윈도우의 오른쪽 경계를 초과하는 패킷에 대한 작업을 설정합니다.
synack-data	데이터가 포함된 TCP SYNACK 패킷에 대한 작업을 설정합니다.
syn-data	데이터가 포함된 SYN 패킷을 허용하거나 삭제합니다.
tcp-options	TCP 헤더에 있는 TCP options(TCP 옵션) 필드의 내용에 따라 패킷에 대한 작업을 설정합니다.
ttl-evasion-protection	ASA에서 제공하는 TTL 회피 방지를 활성화하거나 비활성화합니다.
urgent-flag	ASA를 통해 URG 포인터를 허용하거나 지웁니다.
window-variation	해당 창 크기를 예상치 않게 변경하는 연결을 삭제합니다.

예

예를 들어 잘 알려진 FTP 데이터 포트와 텔넷 포트 간의 TCP 포트 범위로 전송된 모든 트래픽에 대해 긴급 플래그 및 긴급 오프셋 패킷을 허용하려면 다음 명령을 입력합니다.

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow

ciscoasa(config-tcp-map)# class-map urg-class
ciscoasa(config-cmap)# match port tcp range ftp-data telnet

ciscoasa(config-cmap)# policy-map pmap
ciscoasa(config-pmap)# class urg-class
ciscoasa(config-pmap-c)# set connection advanced-options tmap

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

관련 명령

Command(명령)	설명
class (policy-map)	트래픽 분류에 사용할 클래스 맵을 지정합니다.
clear configure tcp-map	TCP 맵 구성을 지웁니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
show running-config tcp-map	TCP 맵 구성에 대한 정보를 표시합니다.
tcp-options	selective-ack, timestamps 또는 window-scale TCP 옵션을 허용하거나 지웁니다.

tcp-options

TCP 헤더에서 TCP 옵션을 허용하거나 제거하려면 tcp-map 구성 모드에서 **tcp-options** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tcp-options {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action*

no tcp-options {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range** *lower upper*} *action*

구문 설명

action	옵션에 대해 수행할 작업입니다. 작업은 다음과 같습니다. • **allow** [**multiple**] - 옵션을 포함하는 패킷을 허용합니다. 9.6(2)부터 **allow**는 이 유형의 단일 옵션을 포함하는 패킷을 허용하는 것을 의미합니다. 이는 모든 명명된 옵션에 대한 기본값입니다. 패킷에 둘 이상의 옵션 인스턴스가 포함된 경우에도 패킷을 허용하려면 **multiple** 키워드를 추가합니다. **multiple** 키워드는 **range**에 사용할 수 없습니다. • **maximum** *limit* - **mss**에만 해당합니다. 최대 세그먼트 크기를 지정된 제한(68~65535)으로 설정합니다. 기본 TCP MSS는 **sysopt connection tcpmss** 명령에 정의되어 있습니다. • **clear** - 헤더에서 이 유형의 옵션을 제거하고 패킷을 허용합니다. 이는 **range** 키워드에서 구성할 수 있는 모든 번호 매기기 옵션에 대한 기본값입니다. 타임스탬프 옵션을 지우면 PAWS 및 RTT가 비활성화됩니다. • **drop** - 이 옵션을 포함하는 패킷을 삭제합니다. 이 작업은 **md5** 및 **range**에만 사용할 수 있습니다.
md5	MD5 옵션에 대한 작업을 설정합니다.
mss	최대 세그먼트 크기 옵션에 대한 작업을 설정합니다.
range *lower upper*	범위의 하한 및 상한 내의 번호 매기기 옵션에 대한 작업을 설정합니다. 단일 번호 매기기 옵션에 대한 작업을 설정하려면 하한 및 상한 범위에 대해 동일한 숫자를 입력합니다. (9.6(2) 이상.) 유효한 범위는 6~7, 9~18 및 20~255 이내입니다. (9.6(1) 이하.) 유효한 범위는 6~7 및 9~255 이내입니다.
selective-ack	SACK(Selective Acknowledgement Mechanism) 옵션에 대한 작업을 설정합니다.
timestamp	timestamp 옵션에 대한 작업을 설정합니다. timestamp 옵션을 지우면 PAWS 및 RTT가 비활성화됩니다.
window-scale	창 배율 메커니즘 옵션에 대한 작업을 설정합니다.

기본값

(9.6(1) 이하.) 기본값은 명명된 모든 옵션을 허용하고, 옵션 6~7 및 9~255를 지우는 것입니다.

(9.6(2) 이상.) 기본값은 명명된 각 옵션의 단일 인스턴스를 허용하고, 지정된 명명 옵션 중 두 개 이상의 패킷을 삭제하고, 6~7, 9~18 및 20~155 옵션을 지우는 것입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
tcp-map 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.6(2)	지정된 유형의 단일 옵션을 포함하는 경우 패킷을 허용하도록 명명된 옵션의 기본 처리가 변경되었으며 해당 유형에 대한 옵션이 둘 이상인 경우 패킷을 삭제합니다. 또한 **md5**, **mss**, **allow multiple** 및 **mss maximum** 키워드가 추가되었습니다. MD5 옵션에 대한 기본값이 clear에서 allow로 변경되었습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용됩니다. **class-map** 명령을 사용하여 트래픽의 클래스를 정의하고, **tcp-map** 명령을 사용하여 TCP 검사를 맞춤 설정합니다. **policy-map** 명령을 사용하여 새 TCP 맵을 적용합니다. **service-policy** 명령을 사용하여 TCP 검사를 활성화합니다.

tcp-map 명령을 사용하여 tcp-map 구성 모드를 시작할 수 있습니다. tcp-map 구성 모드에서 **tcp-options** 명령을 사용하여 다양한 TCP 옵션을 처리하는 방법을 정의합니다.

예

다음 예에서는 6~7 및 9~255 범위의 TCP 옵션이 있는 모든 패킷을 삭제하는 방법을 보여 줍니다.

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# tcp-options range 6 7 drop
ciscoasa(config-tcp-map)# tcp-options range 9 18 drop
ciscoasa(config-tcp-map)# tcp-options range 20 255 drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

관련 명령

Command(명령)	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 구성 모드에 대한 액세스를 허용합니다.

telnet

Telnet을 통해 인터페이스에 액세스할 수 있도록 허용하려면 전역 구성 모드에서 **telnet** 명령을 사용합니다. Telnet 액세스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

telnet {*ipv4_address mask* | *ipv6_address*/*prefix*} *interface_name*

no telnet {*ipv4_address mask* | *ipv6_address*/*prefix*} *interface_name*

구문 설명

interface_name	Telnet을 허용할 인터페이스의 이름을 지정합니다. VPN 터널에서 Telnet을 사용하지 않는 한 보안 수준이 가장 낮은 인터페이스에서는 Telnet을 활성화할 수 없습니다. 물리적 또는 가상 인터페이스를 지정당할 수 있습니다.
ipv4_address mask	ASA로 Telnet할 권한이 있는 호스트 또는 네트워크의 IPv4 주소 및 서브넷 마스크를 지정합니다.
ipv6_address/prefix	ASA로 Telnet할 권한이 있는 IPv6 주소/접두사를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.0(2), 9.1(2)	기본 비밀번호인 "cisco"가 제거되었습니다. **password** 명령을 사용하여 로그인 비밀번호를 직접 설정해야 합니다.
9.9.(2)	이제 가상 인터페이스를 지정할 수 있습니다.

사용 지침

telnet 명령을 사용하면 Telnet을 통해 ASA CLI에 액세스할 수 있는 호스트를 지정할 수 있습니다. 모든 인터페이스에서 ASA로의 Telnet을 활성화할 수 있습니다. 그러나 VPN 터널 내에서 Telnet을 사용하지 않는 한 보안 수준이 가장 낮은 인터페이스에는 Telnet을 사용할 수 없습니다. 또한 BVI 인터페이스가 지정된 경우 해당 인터페이스에서 **managenent-access**를 구성해야 합니다.

password 명령을 사용하여 Telnet을 통해 콘솔에 액세스하기 위한 비밀번호를 설정할 수 있습니다. **who** 명령을 사용하여 현재 ASA 콘솔에 액세스 중인 IP 주소를 볼 수 있습니다. **kill** 명령을 사용하여 활성 Telnet 콘솔 세션을 종료할 수 있습니다.

aaa authentication telnet console 명령을 사용하는 경우 Telnet 콘솔에서 인증 서버에 인증해야 합니다.

예

다음 예에서는 호스트 192.168.1.3 및 192.168.1.4에서 Telnet을 통해 ASA CLI에 액세스하도록 허용하는 방법을 보여 줍니다. 또한 192.168.2.0 네트워크의 모든 호스트에 액세스 권한이 부여됩니다.

```
ciscoasa(config)# telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.1.4 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.2.0 255.255.255.0 inside
ciscoasa(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

다음 예에서는 Telnet 콘솔 로그인 세션을 보여 줍니다(비밀번호는 입력 시 표시되지 않음).

```
ciscoasa# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
ciscoasa>
```

no telnet 명령을 사용하여 개별 항목을 제거하거나, **clear configure telnet** 명령을 사용하여 모든 Telnet 명령문을 제거할 수 있습니다.

```
ciscoasa(config)# no telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside

ciscoasa(config)# clear configure telnet
```

관련 명령

Command(명령)	설명
clear configure telnet	구성에서 Telnet 연결을 제거합니다.
kill	Telnet 세션을 종료합니다.
show running-config telnet	Telnet을 사용하여 ASA에 연결할 수 있는 현재 IP 주소 목록을 표시합니다.
telnet timeout	Telnet 시간 초과를 설정합니다.
who	ASA의 활성 Telnet 관리 세션을 표시합니다.

telnet timeout

Telnet 유휴 시간 제한을 설정하려면 전역 구성 모드에서 **telnet timeout** 명령을 사용합니다. 기본 시간 제한을 복원하려면 이 명령의 **no** 형식을 사용합니다.

telnet timeout *minutes*

no telnet timeout *minutes*

구문 설명

minutes	ASA에서 닫기 전에 Telnet 세션이 유휴 상태로 있을 수 있는 기간(분)입니다. 유효한 값은 1~1440분입니다. 기본값은 5분입니다.

기본값

기본적으로 Telnet 세션은 5분 동안 유휴 상태로 유지된 후 ASA에 의해 닫힙니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

telnet timeout 명령을 사용하여 ASA에서 로그오프하기 전에 콘솔 Telnet 세션을 유휴 상태로 유지할 수 있는 최대 시간을 설정할 수 있습니다.

예

다음 예에서는 최대 세션 유휴 기간을 변경하는 방법을 보여 줍니다.

```
ciscoasa(config)# telnet timeout 10
ciscoasa(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

관련 명령

Command(명령)	설명
clear configure telnet	컨피그레이션에서 텔넷 연결을 제거합니다.
kill	Telnet 세션을 종료합니다.
show running-config telnet	텔넷을 사용하여 ASA에 연결할 수 있는 현재 IP 주소 목록을 표시합니다.
telnet	Telnet을 통해 ASA에 액세스할 수 있도록 합니다.
who	ASA의 활성 텔넷 관리 세션을 표시합니다.

terminal interactive

CLI에서 **?**를 입력할 때 현재 CLI 세션에서 도움말을 활성화하려면 특권 EXEC 모드에서 **terminal interactive** 명령을 사용합니다. CLI 도움말을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

terminal interactive

no terminal interactive

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

인터랙티브 CLI 도움말은 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
9.4(1)	이 명령이 추가되었습니다.

사용 지침

일반적으로 ASA CLI에서 **?**를 입력하면 명령 도움말이 표시됩니다. **?**를 명령 내에서 텍스트로 입력하려면 (예를 들어, URL의 일부로 **?** 포함) **no terminal interactive** 명령을 사용하여 인터랙티브 도움말을 비활성화할 수 있습니다.

예

다음 예에서는 콘솔을 비 인터랙티브 모드로 전환했다가 인터랙티브 모드로 전환하는 방법을 보여 줍니다.

```
ciscoasa# no terminal interactive
ciscoasa# terminal interactive
```

관련 명령

Command(명령)	설명
clear configure terminal	터미널 표시 너비 설정을 지웁니다.
pager	"---more---" 프롬프트가 표시되기 전에 텔넷 세션에 표시할 줄 수를 설정합니다. 이 명령은 구성에 저장됩니다.
show running-config terminal	현재 터미널 설정을 표시합니다.

Command(명령)	설명
terminal pager	"---more---" 프롬프트가 표시되기 전에 텔넷 세션에 표시할 줄 수를 설정합니다. 이 명령은 컨피그레이션에 저장되지 않습니다.
terminal width	전역 컨피그레이션 모드에서 터미널 표시 너비를 설정합니다.

terminal monitor

시스템 로그 메시지가 현재 CLI 세션에 표시되도록 허용하려면 특권 EXEC 모드에서 **terminal monitor** 명령을 사용합니다. 시스템 로그 메시지를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

terminal {**monitor** | **no monitor**}

구문 설명

monitor	현재 CLI 세션에서 시스템 로그 메시지 표시를 활성화합니다.
no monitor	현재 CLI 세션에서 시스템 로그 메시지 표시를 비활성화합니다.

기본값

시스템 로그 메시지는 기본적으로 비활성화되어 있습니다. 이 명령은 기본적으로 인터랙티브입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

예

다음 예에서는 현재 세션에서 시스템 로그 메시지를 표시 및 비활성화하는 방법을 보여 줍니다.

```
ciscoasa# terminal monitor
ciscoasa# terminal no monitor
```

관련 명령

Command(명령)	설명
clear configure terminal	터미널 표시 너비 설정을 지웁니다.
pager	"---more---" 프롬프트가 표시되기 전에 Telnet 세션에 표시할 줄 수를 설정합니다. 이 명령은 구성에 저장됩니다.
show running-config terminal	현재 터미널 설정을 표시합니다.
terminal pager	"---more---" 프롬프트가 표시되기 전에 텔넷 세션에 표시할 줄 수를 설정합니다. 이 명령은 구성에 저장되지 않습니다.
terminal width	전역 구성 모드에서 터미널 표시 너비를 설정합니다.

terminal pager

Telnet 세션에 대해 "---More---" 프롬프트가 표시되기 전까지의 페이지의 줄 수를 설정하려면 특권 EXEC 모드에서 **terminal pager** 명령을 사용합니다.

terminal pager [lines] *lines*

구문 설명

[**lines**] *lines*	"---More---" 프롬프트가 표시되기 전까지의 페이지의 줄 수를 설정합니다. 기본값은 24줄이고, 0은 페이지 제한이 없음을 의미합니다. 범위는 0~2147483647줄입니다. **lines** 키워드는 선택 사항이며, 이 명령은 이 키워드의 사용 여부에 상관없이 동일합니다.

기본값

기본값은 24줄입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 현재 Telnet 세션에서만 페이저 줄 설정을 변경합니다. 그러나 ASA는 사용자 EXEC 모드에서 **login** 명령을 입력하거나 **enable** 명령을 입력하여 특권 EXEC 모드를 시작하는 경우에만 실행 중인 구성에서 현재 세션의 페이저 값을 다시 시작합니다. 이는 설계된 것입니다.

참고 ASA가 사용자 프롬프트를 표시하기 전에 예기치 않은 "---More---" 프롬프트가 표시되어 **banner exec** 명령의 출력을 억제했을 수 있습니다. 대신 **banner motd** 명령 또는 **banner login** 명령을 사용합니다.

새 기본 페이저 설정을 구성에 저장하려면 다음을 수행합니다.

1. **login** 명령을 입력하여 사용자 EXEC 모드에 액세스하거나, **enable** 명령을 입력하여 특권 EXEC 모드에 액세스합니다.
2. **pager** 명령을 입력합니다.

Telnet을 사용하여 관리 상황에 액세스한 경우 다른 상황으로 변경하면 페이저 줄 설정이 사용자 세션을 따릅니다. 이는 지정된 상황의 **pager** 명령에 다른 설정이 있는 경우에도 마찬가지입니다. 현재 페이저 설정을 변경하려면 새 설정으로 **terminal pager** 명령을 입력하거나 현재 상황에서 **pager** 명령을 입력합니다. 새 페이저 설정을 상황 구성에 저장하는 것 외에 **pager** 명령은 새 설정을 현재 Telnet 세션에 적용합니다.

예

다음 예에서는 표시되는 줄 수를 20으로 변경합니다.

```
ciscoasa# terminal pager 20
```

관련 명령

Command(명령)	설명
clear configure terminal	터미널 표시 너비 설정을 지웁니다.
pager	"---More---" 프롬프트가 표시되기 전에 Telnet 세션에 표시할 줄 수를 설정합니다. 이 명령은 컨피그레이션에 저장됩니다.
show running-config terminal	현재 터미널 설정을 표시합니다.
terminal	시스템 로그 메시지가 Telnet 세션에 표시되도록 허용합니다.
terminal width	전역 컨피그레이션 모드에서 터미널 표시 너비를 설정합니다.

terminal width

콘솔 세션 중에 정보를 표시할 너비를 설정하려면 전역 구성 모드에서 **terminal width** 명령을 사용합니다. 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

terminal width *columns*

no terminal width *columns*

구문 설명

columns	터미널 너비(열 수)를 지정합니다. 기본값은 80입니다. 범위는 40~511입니다.

기본값

기본 표시 너비는 80열입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

예

다음 예에서는 터미널 표시 너비를 100열로 설정하는 방법을 보여 줍니다.

```
ciscoasa# terminal width 100
```

관련 명령

Command(명령)	설명
clear configure terminal	터미널 표시 너비 설정을 지웁니다.
show running-config terminal	현재 터미널 설정을 표시합니다.
terminal	특권 EXEC 모드에서 터미널 줄 파라미터를 설정합니다.

test aaa-server

ASA에서 특정 AAA 서버에 사용자를 인증하거나 권한을 부여할 수 있는지 확인하려면 특권 EXEC 모드에서 **test aaa-server** 명령을 사용합니다. AAA 서버에 연결하지 못한 경우 이는 ASA의 구성이 잘못되었거나, 네트워크 구성 제한 또는 서버 다운타임과 같은 다른 이유로 AAA 서버에 연결할 수 없기 때문일 수 있습니다.

test aaa-server {**authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*][**ad-agent**]}

구문 설명

ad-agent	AAA AD 에이전트 서버에 대한 연결을 테스트합니다.
authentication	AAA 서버의 인증 기능을 테스트합니다.
authorization	AAA 서버의 레거시 VPN 권한 부여 기능을 테스트합니다.
host *ip_address*	서버 IP 주소를 지정합니다. 명령에서 IP 주소를 지정하지 않으면 IP 주소를 묻는 프롬프트가 표시됩니다.
password *password*	사용자 비밀번호를 지정합니다. 명령에서 비밀번호를 지정하지 않으면 비밀번호를 묻는 프롬프트가 표시됩니다.
server_tag	**aaa-server** 명령에서 설정된 대로 AAA 서버 태그를 지정합니다.
username *username*	AAA 서버 설정을 테스트하는 데 사용된 계정의 사용자 이름을 지정합니다. 사용자 이름이 AAA 서버에 존재해야 합니다. 그렇지 않으면 테스트에 실패합니다. 명령에서 사용자 이름을 지정하지 않으면 사용자 이름을 묻는 프롬프트가 표시됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(4)	이 명령이 추가되었습니다.
8.4(2)	**ad-agent** 키워드가 추가되었습니다.

사용 지침

test aaa-server 명령을 사용하여 ASA가 특정 AAA 서버에 사용자를 인증할 수 있는지 확인하고, 사용자에게 권한을 부여할 수 있는 경우 레거시 VPN 권한 부여를 확인할 수 있습니다. 이 명령을 사용하면 인증 또는 권한 부여를 시도하는 실제 사용자 없이도 AAA 서버를 테스트할 수 있습니다. 또한 AAA 실패 원인을 AAA 서버 파라미터의 잘못된 구성, AAA 서버의 연결 문제 또는 ASA의 기타 구성 오류로 분리할 수 있습니다.

예

다음 예에서는 호스트 192.168.3.4에서 srvgrp1이라는 RADIUS AAA 서버를 구성하고, 시간 제한을 9초로 설정하고, 재시도 간격을 7초로 설정하고, 인증 포트를 1650으로 구성합니다. AAA 서버 파라미터 설정 뒤의 **test aaa-server** 명령은 인증 테스트 시 서버에 연결하지 못했음을 나타냅니다.

```
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)# 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)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

다음은 성공한 **test aaa-server** 명령의 샘플 출력입니다.

```
ciscoasa# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

관련 명령

Command(명령)	설명
aaa authentication console	관리 트래픽에 대한 인증을 구성합니다.
aaa authentication match	통과 트래픽에 대한 인증을 구성합니다.
aaa-server	AAA 서버 그룹을 생성합니다.
aaa-server host	서버 그룹에 AAA 서버를 추가합니다.

test aaa-server ad-agent

Active Directory 에이전트 구성을 구성한 후 테스트하려면 AAA 서버 그룹 구성 모드에서 **test aaa-server ad-agent** 명령을 사용합니다.

test aaa-server ad-agent

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
aaa server group 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

ID 방화벽에 대해 Active Directory 에이전트를 구성하려면 **aaa-server** 명령의 하위 모드인 **ad-agent-mode** 명령을 입력해야 합니다. **ad-agent-mode** 명령을 입력하면 AAA 서버 그룹 구성 모드가 시작됩니다.

Active Directory 에이전트를 구성한 후 **test aaa-server ad-agent** 명령을 입력하여 ASA가 Active Directory 에이전트에 연결되어 있는지 확인합니다.

AD 에이전트는 주기적으로 또는 온디맨드로 WMI를 통해 Active Directory 서버 보안 이벤트 로그 파일을 모니터링하여 사용자 로그인 및 로그오프 이벤트를 확인합니다. AD 에이전트는 사용자 ID와 IP 주소 매핑의 캐시를 유지하며 ASA에 변경 사항을 알려 줍니다.

AD 에이전트 서버 그룹에 대한 기본 및 보조 AD 에이전트를 구성합니다. ASA에서 기본 AD 에이전트가 응답하지 않는 것을 탐지한 경우 보조 에이전트가 지정되어 있으면 ASA는 보조 AD 에이전트로 전환합니다. AD 에이전트의 Active Directory 서버는 RADIUS를 통신 프로토콜로 사용합니다. 따라서 ASA와 AD 에이전트 간의 공유 암호에 대한 키 특성을 지정해야 합니다.

예

다음 예에서는 ID 방화벽에 대해 Active Directory 에이전트를 구성하는 동안 **ad-agent-mode**를 활성화한 다음 연결을 테스트하는 방법을 보여 줍니다.

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

관련 명령

Command(명령)	설명
aaa-server	AAA 서버 그룹을 만들고 그룹별 및 모든 그룹 호스트에 공통적인 AAA 서버 파라미터를 구성합니다.
clear configure user-identity	ID 방화벽 기능에 대한 구성을 지웁니다.

test dynamic-access-policy attributes

dap attributes 모드를 시작하려면 특권 EXEC 모드에서 **test dynamic-access-policy attributes** 명령을 입력합니다. 이렇게 하면 사용자 및 엔드포인트 특성 값 쌍을 지정할 수 있습니다.

dynamic-access-policy attributes

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

일반적으로 ASA는 AAA 서버에서 사용자 권한 부여 특성을 검색하고, Cisco Secure Desktop, Host Scan, CNA 또는 NAC에서 엔드포인트 특성을 검색합니다. 테스트 명령의 경우 이 특성 모드에서 사용자 권한 부여 및 엔드포인트 특성을 지정합니다. ASA는 DAP 레코드에 대한 AAA 선택 특성 및 엔드포인트 선택 특성을 평가할 때 DAP 하위 시스템에서 참조하는 특성 데이터베이스에 이러한 특성을 기록합니다.

이 기능을 사용하여 DAP 레코드 생성을 실험할 수 있습니다.

예

다음 예에서는 **attributes** 명령을 사용하는 방법을 보여 줍니다.

```
ciscoasa # test dynamic-access-policy attributes
ciscoasa(config-dap-test-attr)#
```

관련 명령

Command(명령)	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
attributes	사용자 특성 값 쌍을 지정할 수 있는 특성 모드를 시작합니다.
display	현재 특성 목록을 표시합니다.

test dynamic-access-policy execute

이미 구성된 DAP 레코드를 테스트하려면 특권 EXEC 모드에서 test dynamic-access-policy execute 명령을 사용합니다.

test dynamic-access-policy execute

구문 설명

AAA attribute value	디바이스의 DAP 하위 시스템에서는 각 레코드에 대한 AAA 및 엔드포인트 선택 특성을 평가할 때 이러한 값을 참조합니다. – AAA Attribute - AAA 특성을 식별합니다. – Operation Value - 지정된 값과 =/!=(같음/같지 않음)로 특성을 식별합니다.
endpoint attribute value	엔드포인트 특성을 식별합니다. – Endpoint ID - 엔드포인트 특성 ID를 제공합니다. – Name/Operation/Value—

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(4)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 권한 부여 특성 값 쌍을 지정하여 장치에 구성된 DAP 레코드 집합 검색을 테스트할 수 있습니다.

test regex

정규식을 테스트하려면 특권 EXEC 모드에서 **test regex** 명령을 사용합니다.

test regex *input_text regular_expression*

구문 설명

input_text	정규식과 일치시킬 텍스트를 지정합니다.
regular_expression	100자 이내로 정규식을 지정합니다. 정규식에서 사용할 수 있는 메타 문자 목록은 **regex** 명령을 참고하십시오.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

test regex 명령은 정규식을 테스트하여 일치 여부를 확인합니다.

정규식이 입력 텍스트와 일치하는 경우 다음 메시지가 표시됩니다.

```
INFO: Regular expression match succeeded.
```

정규식이 입력 텍스트와 일치하지 않는 경우 다음 메시지가 표시됩니다.

```
INFO: Regular expression match failed.
```

예

다음 예에서는 정규식에 대해 입력 텍스트를 테스트합니다.

```
ciscoasa# test regex farscape scape
INFO: Regular expression match succeeded.

ciscoasa# test regex farscape scaper

INFO: Regular expression match failed.
```

관련 명령

Command(명령)	설명
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	트래픽 클래스를 하나 이상의 작업과 연결하여 정책 맵을 생성합니다.
policy-map type inspect	애플리케이션 검사를 위한 특수 작업을 정의합니다.
class-map type regex	정규식 클래스 맵을 생성합니다.
regex	정규식을 생성합니다.

test sso-server(사용되지 않음)

참고 마지막으로 이 명령을 지원하는 릴리스는 버전 9.5(1)이었습니다.

평가판 인증 요청으로 SSO 서버를 테스트하려면 특권 EXEC 모드에서 **test sso-server** 명령을 사용합니다.

test sso-server *server-name* **username** *user-name*

구문 설명

server-name	테스트할 SSO 서버 이름을 지정합니다.
user-name	테스트할 SSO 서버의 사용자 이름을 지정합니다.

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
Config-webvpn	• 예	—	• 예	—	—
config-webvpn-sso-saml	• 예	—	• 예	—	—
config-webvpn-sso-siteminder	• 예	—	• 예	—	—
전역 구성 모드	• 예	—	• 예	—	—
특권 실행	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.
9.5(2)	이 명령은 SAML 2.0 지원으로 인해 사용이 중단되었습니다.

사용 지침

SSO(WebVPN에만 제공) 지원을 통해 사용자가 사용자 이름 및 비밀번호를 단 한 번만 입력하여 여러 서버에서 다양한 보안 서비스에 액세스할 수 있습니다. **test sso-server** 명령은 SSO 서버가 인식되고 인증 요청에 응답하는지 테스트합니다.

server-name 인수로 지정된 SSO 서버를 찾을 수 없는 경우 다음 오류가 표시됩니다.

```
ERROR: sso-server server-name does not exist
```

SSO 서버를 찾았지만 *user-name* 인수로 지정된 사용자를 찾을 수 없는 경우에는 인증이 거부됩니다.

인증에서 ASA는 SSO 서버의 WebVPN 사용자를 위한 프록시 역할을 합니다. ASA는 현재 SiteMinder SSO 서버(이전의 Netegrity SiteMinder) 및 SAML POST 유형 SSO 서버를 지원합니다. 이 명령은 두 유형의 SSO 서버 모두에 적용됩니다.

예

특권 EXEC 모드에서 입력된 다음 예에서는 Anyuser라는 사용자 이름을 사용하여 my-sso-server라는 SSO 서버를 성공적으로 테스트합니다.

```
ciscoasa# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
ciscoasa#
```

다음 예에서는 동일한 서버를 테스트하지만 Anotheruser라는 사용자가 인식되지 않아 인증에 실패한 결과를 보여 줍니다.

```
ciscoasa# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
ciscoasa#
```

관련 명령

Command(명령)	설명
max-retry-attempts	실패한 SSO 인증 시도에 대해 ASA에서 재시도할 횟수를 구성합니다.
policy-server-secret	SiteMinder SSO 서버에 대한 인증 요청을 암호화하는 데 사용되는 비밀 키를 생성합니다.
request-timeout	시간 초과로 인해 SSO 인증 시도가 실패하는 시간(초)을 지정합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso-server	SSO(Single Sign-On) 서버를 생성합니다.
web-agent-url	ASA에서 SiteMinder SSO 인증 요청을 작성하는 SSO 서버 URL을 지정합니다.

text-color

로그인, 홈 페이지 및 파일 액세스 페이지의 WebVPN 제목 표시줄에 표시되는 텍스트의 색상을 설정하려면 webvpn 모드에서 **text-color** 명령을 사용합니다. 구성에서 텍스트 색상을 제거하고 기본값을 다시 설정하려면 이 명령의 no 형식을 사용합니다.

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

no text-color

구문 설명

auto	secondary-color 명령에 대한 설정에 따라 검은색 또는 흰색을 선택합니다. 즉, 보조 색상이 검은색인 경우 이 값은 white입니다.
black	제목 표시줄의 기본 텍스트 색상은 흰색입니다.
white	색상을 검은색으로 변경할 수 있습니다.

기본값

제목 표시줄의 기본 텍스트 색상은 흰색입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
config-webvpn	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

예

다음 예에서는 제목 표시줄의 텍스트 색상을 검은색으로 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# text-color black
```

관련 명령

Command(명령)	설명
secondary-text-color	WebVPN 로그인, 홈 페이지 및 파일 액세스 페이지의 보조 텍스트 색상을 설정합니다.

tftp-server

configure net 또는 **write net** 명령에서 사용할 기본 TFTP 서버 및 경로와 파일 이름을 지정하려면 전역 구성 모드에서 **tftp-server** 명령을 사용합니다. 서버 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 명령은 IPv4 및 IPv6 주소를 지원합니다.

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

구문 설명

파일 이름	경로 및 파일 이름을 지정합니다.
interface_name	게이트웨이 인터페이스 이름을 지정합니다. 보안 수준이 가장 높은 인터페이스 이외의 인터페이스를 지정한 경우 인터페이스가 안전하지 않음을 알리는 경고 메시지가 표시됩니다.
server	TFTP 서버 IP 주소 또는 이름을 설정합니다. IPv4 또는 IPv6 주소를 입력할 수 있습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이제 게이트웨이 인터페이스가 필수입니다.

사용 지침

tftp-server 명령은 **configure net** 및 **write net** 명령의 입력을 간소화합니다. **configure net** 또는 **write net** 명령을 입력할 때 **tftp-server** 명령에서 지정된 TFTP 서버를 상속하거나 고유한 값을 제공할 수 있습니다. 또한 **tftp-server** 명령의 경로를 있는 그대로 상속하거나, **tftp-server** 명령 값 끝에 경로 및 파일 이름을 추가하거나, **tftp-server** 명령 값을 재정의할 수 있습니다.

ASA는 하나의 **tftp-server** 명령만 지원합니다.

예

다음 예에서는 TFTP 서버를 지정한 다음 /temp/config/test_config 디렉터리에서 구성을 읽는 방법을 보여 줍니다.

```
ciscoasa(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
ciscoasa(config)# configure net
```

관련 명령

Command(명령)	설명
configure net	지정한 TFTP 서버 및 경로에서 구성을 로드합니다.
show running-config tftp-server	구성 파일의 기본 TFTP 서버 주소 및 디렉터리를 표시합니다.

tftp-server address(사용되지 않음)

클러스터의 TFTP 서버를 지정하려면 phone-proxy 구성 모드에서 **tftp-server address** 명령을 사용합니다. Phone Proxy 구성에서 TFTP 서버를 제거하려면 이 명령의 **no** 형식을 사용합니다.

tftp-server address *ip_address* [*port*] **interface** *interface*

no tftp-server address *ip_address* [*port*] **interface** *interface*

구문 설명

ip_address	TFTP 서버의 주소를 지정합니다.
interface *interface*	TFTP 서버가 상주하는 인터페이스를 지정합니다. 이는 TFTP 서버의 실제 주소여야 합니다.
port	(선택 사항) 이는 TFTP 서버가 TFTP 요청을 수신 대기하는 포트입니다. 기본 TFTP 포트 69가 아닌 경우 구성해야 합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
phone-proxy 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.0(4)	이 명령이 추가되었습니다.
9.4(1)	이 명령은 모든 **phone-proxy** 모드 명령과 함께 사용이 중단되었습니다.

사용 지침

Phone Proxy에는 하나 이상의 CUCM TFTP 서버가 구성되어 있어야 합니다. Phone Proxy당 최대 5개의 TFTP 서버를 구성할 수 있습니다.

TFTP 서버는 신뢰할 수 있는 네트워크의 방화벽 뒤에 있는 것으로 가정합니다. 따라서 Phone Proxy는 IP 전화기와 TFTP 서버 간의 요청을 가로챕니다. TFTP 서버는 CUCM과 동일한 인터페이스에 있어야 합니다.

내부 IP 주소를 사용하여 TFTP 서버를 만들고 TFTP 서버가 상주하는 인터페이스를 지정합니다.

IP 전화기에서 TFTP 서버의 IP 주소를 다음과 같이 구성해야 합니다.

- NAT가 TFTP 서버에 대해 구성된 경우 TFTP 서버의 전역 IP 주소를 사용합니다.
- NAT가 TFTP 서버에 대해 구성되지 않은 경우 TFTP 서버의 내부 IP 주소를 사용합니다.

service-policy가 전역적으로 적용되는 경우 TFTP 서버가 상주하는 인터페이스를 제외하고 모든 이그레스 인터페이스에서 TFTP 서버에 연결하는 모든 TFTP 트래픽을 전달하기 위한 분류 규칙이 생성됩니다. service-policy가 특정 인터페이스에서 적용되는 경우 해당 인터페이스에서 TFTP 서버에 연결하는 모든 TFTP 트래픽을 phone-proxy 모듈로 전달하기 위한 분류 규칙이 생성됩니다.

TFTP 서버에 대해 NAT 규칙을 구성할 경우 분류 규칙을 설치할 때 TFTP 서버의 전역 주소가 사용되도록 service-policy를 적용하기 전에 구성해야 합니다.

예

다음 예에서는 **tftp-server address** 명령을 사용하여 Phone Proxy에 대해 두 개의 TFTP 서버를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.4 interface inside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.25 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa(config-phone-proxy)# ctl-file asactl
ciscoasa(config-phone-proxy)# cluster-mode nonsecure
```

관련 명령

Command(명령)	설명
phone-proxy	전화 프록시 인스턴스를 구성합니다.

threat-detection basic-threat

기본 위협 탐지를 활성화하려면 전역 구성 모드에서 **threat-detection basic-threat** 명령을 사용합니다. 기본 위협 탐지를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

threat-detection basic-threat

no threat-detection basic-threat

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 위협 탐지는 기본적으로 활성화되어 있습니다. 다음 기본 속도 제한이 사용됩니다.

표 1-1 기본 위협 탐지 기본 설정

	트리거 설정	
패킷 삭제 사유	**평균 속도**	**버스트 속도**
• DoS 공격 탐지 • 잘못된 패킷 형식 • 연결 제한 초과 • 의심스러운 ICMP 패킷 탐지	지난 600초 동안 100개/초 삭제	지난 20초 동안 400개/초 삭제
	지난 3600초 동안 80개/초 삭제	지난 120초 동안 320개/초 삭제
검사 공격 탐지	지난 600초 동안 5개/초 삭제	지난 20초 동안 10개/초 삭제
	지난 3600초 동안 4개/초 삭제	지난 120초 동안 8개/초 삭제
TCP SYN 공격 탐지 또는 반환 데이터 없는 UDP 세션 공격 탐지(통합)와 같은 완료되지 않은 세션 탐지.	지난 600초 동안 100개/초 삭제	지난 20초 동안 200개/초 삭제
	지난 3600초 동안 80개/초 삭제	지난 120초 동안 160개/초 삭제
액세스 목록에 의한 거부	지난 600초 동안 400개/초 삭제	지난 20초 동안 800개/초 삭제
	지난 3600초 동안 320개/초 삭제	지난 120초 동안 640개/초 삭제
• 기본 방화벽 확인 실패 • 패킷에서 애플리케이션 검사 실패	지난 600초 동안 400개/초 삭제	지난 20초 동안 1600개/초 삭제
	지난 3600초 동안 320개/초 삭제	지난 120초 동안 1280개/초 삭제
인터페이스 오버로드	지난 600초 동안 2000개/초 삭제	지난 20초 동안 8000개/초 삭제
	지난 3600초 동안 1600개/초 삭제	지난 120초 동안 6400개/초 삭제

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.
8.2(1)	버스트 속도 간격이 평균 속도의 1/60에서 1/30로 변경되었습니다.

사용 지침

기본 위협 탐지를 활성화한 경우 ASA는 다음과 같은 사유로 인해 삭제된 패킷의 속도 및 보안 이벤트를 모니터링합니다.

- 액세스 목록에 의한 거부
- 잘못된 패킷 형식(예: invalid-ip-header 또는 invalid-tcp-hdr-length)
- 연결 제한 초과(시스템 전체 리소스 제한 및 구성에 설정된 제한 모두)
- DoS 공격 탐지(예: 잘못된 SPI, 상태 저장 방화벽 확인 실패)
- 기본 방화벽 검사 실패(이 옵션은 이 글머리 기호 목록의 모든 방화벽 관련 패킷 삭제를 포함하는 통합된 속도입니다. 인터페이스 오버로드, 애플리케이션 검사에 실패한 패킷, 스캔 공격 탐지 등 방화벽과 관련이 없는 삭제는 포함되지 않습니다.)
- 의심스러운 ICMP 패킷 탐지
- 패킷에서 애플리케이션 검사 실패
- 인터페이스 오버로드
- 스캔 공격 탐지(이 옵션은 스캔 공격을 모니터링합니다. 예를 들어 첫 번째 TCP 패킷이 SYN 패킷이 아닌 경우 또는 3방향 핸드셰이크에 실패한 TCP 연결을 모니터링합니다. 전체 스캔 위협 탐지(**threat-detection scanning-threat** 명령 참고)에서는 이 스캔 공격 속도 정보를 가져와 호스트를 공격자로 분류하고 이를 자동으로 차단하는 등의 방식으로 조치를 취합니다.)
- TCP SYN 공격 탐지 또는 반환 데이터 없는 UDP 세션 공격 탐지와 같은 완료되지 않은 세션 탐지.

ASA는 위협을 탐지한 경우 즉시 시스템 로그 메시지(733100)를 보내 ASDM에 알립니다.

기본 위협 탐지는 삭제 또는 잠재적 위협이 있는 경우에만 성능에 영향을 줍니다. 이 경우에도 성능 저하는 미미합니다.

"기본값" 섹션의 표 1-1에 기본 설정이 나와 있습니다. **show running-config all threat-detection** 명령을 사용하여 이 모든 기본 설정을 볼 수 있습니다. **threat-detection rate** 명령을 사용하여 각 이벤트 유형에 대한 기본 설정을 재정의할 수 있습니다.

이벤트 속도를 초과하는 경우 ASA는 시스템 메시지를 보냅니다. ASA는 두 가지 유형의 속도, 즉 간격 동안의 평균 이벤트 속도와 보다 짧은 버스 간격 동안의 버스트 이벤트 속도를 추적합니다. 버스트 이벤트 속도는 평균 속도 간격의 1/30 또는 10초입니다(둘 중 높은 값). 수신된 각 이벤트에 대해 ASA는 평균 및 버스트 속도 제한을 확인합니다. 두 속도 모두 초과하는 경우 ASA는 두 개의 개별 시스템 메시지를 보냅니다(버스트 기간별 각 속도 유형에 대한 최대 하나의 메시지 포함).

예

다음 예에서는 기본 위협 탐지를 활성화하고 DoS 공격에 대한 트리거를 변경합니다.

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

관련 명령

Command(명령)	설명
clear threat-detection rate	기본 위협 탐지 통계를 지웁니다.
show running-config all threat-detection	개별적으로 구성하지 않은 기본 속도 설정을 포함하여 위협 탐지 구성을 표시합니다.
show threat-detection rate	기본 위협 탐지 통계를 표시합니다.
threat-detection rate	이벤트 유형별 위협 탐지 속도 제한을 설정합니다.
threat-detection scanning-threat	스캔 위협 탐지를 활성화합니다.

threat-detection rate

threat-detection basic-threat 명령을 사용하여 기본 위협 탐지를 활성화한 경우 전역 구성 모드에서 **threat-detection rate** 명령을 사용하여 각 이벤트 유형에 대한 기본 속도 제한을 변경할 수 있습니다. **threat-detection scanning-threat** 명령을 사용하여 스캔 위협 탐지를 활성화한 경우 **scanning-threat** 키워드가 포함된 이 명령은 호스트가 공격자 또는 대상으로 간주되는 경우를 설정합니다. 그렇지 않으면 기본 및 스캔 위협 탐지 모두에 기본 **scanning-threat** 값이 사용됩니다. 기본 설정으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

no threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

구문 설명

acl-drop	액세스 목록 거부로 인해 삭제된 패킷의 속도 제한을 설정합니다.
average-rate *av_rate*	0~2147483647의 평균 속도 제한(삭제 수/초)을 설정합니다.
bad-packet-drop	잘못된 패킷 형식(예: invalid-ip-header 또는 invalid-tcp-hdr-length) 거부로 인해 삭제된 패킷의 속도 제한을 설정합니다.
burst-rate *burst_rate*	0~2147483647의 버스트 속도 제한(삭제 수/초)을 설정합니다. 버스트 속도는 *N*초 단위의 평균 속도로 계산됩니다(여기서 *N*은 버스트 속도 간격). 버스트 속도 간격은 **rate-interval** *rate_interval* 값의 1/30 또는 10초입니다(둘 중 높은 값).
conn-limit-drop	연결 제한(시스템 수준 리소스 제한 및 구성에 설정된 제한) 초과로 인해 삭제된 패킷의 속도 제한을 설정합니다.
dos-drop	탐지된 DoS 공격(예: 잘못된 SPI, 상태 저장 방화벽 확인 실패)으로 인해 삭제된 패킷의 속도 제한을 설정합니다.
fw-drop	기본 방화벽 확인 실패로 인해 삭제된 패킷의 속도 제한을 설정합니다. 이 옵션은 이 명령의 모든 방화벽 관련 패킷 삭제를 포함하는 결합된 속도입니다. 방화벽과 관련되지 않은 삭제(예: **interface-drop**, **inspect-drop** 및 **scanning-threat**)는 포함하지 않습니다.
icmp-drop	의심스러운 ICMP 패킷 탐지 거부로 인해 삭제된 패킷의 속도 제한을 설정합니다.
inspect-drop	애플리케이션 검사에 실패한 패킷으로 인해 삭제된 패킷의 속도 제한을 설정합니다.
interface-drop	인터페이스 오버로드로 인해 삭제된 패킷의 속도 제한을 설정합니다.
rate-interval *rate_interval*	600초에서 2592000초(30일) 사이의 평균 속도 간격을 설정합니다. 속도 간격은 삭제 평균을 구할 기간을 결정하는 데 사용됩니다. 또한 버스트 임계값 속도 간격을 결정합니다.

scanning-threat	탐지된 스캔 공격으로 인해 삭제된 패킷의 속도 제한을 설정합니다. 이 옵션은 검사 공격을 모니터링합니다. 예를 들어 첫 번째 TCP 패킷이 SYN 패킷이 아닌 경우 또는 3방향 핸드셰이크에 실패한 TCP 연결을 모니터링합니다. 전체 스캔 위협 탐지(**threat-detection scanning-threat** 명령 참고)에서는 이 스캔 공격 속도 정보를 가져와 호스트를 공격자로 분류하고 이를 자동으로 차단하는 등의 방식으로 조치를 취합니다.
syn-attack	불완전한 세션(예: TCP SYN 공격 또는 반환 데이터 공격 없는 UDP 세션 공격)으로 인해 삭제된 패킷의 속도 제한을 설정합니다.

기본값

threat-detection basic-threat 명령을 사용하여 기본 위협 탐지를 활성화한 경우 다음 기본 속도 제한이 사용됩니다.

표 1-2 기본 위협 탐지 기본 설정

	트리거 설정	
패킷 삭제 사유	**평균 속도**	**버스트 속도**
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	지난 600초 동안 100개/초 삭제	지난 20초 동안 400개/초 삭제
	지난 3600초 동안 100개/초 삭제	지난 120초 동안 400개/초 삭제
scanning-threat	지난 600초 동안 5개/초 삭제	지난 20초 동안 10개/초 삭제
	지난 3600초 동안 5개/초 삭제	지난 120초 동안 10개/초 삭제
syn-attack	지난 600초 동안 100개/초 삭제	지난 20초 동안 200개/초 삭제
	지난 3600초 동안 100개/초 삭제	지난 120초 동안 200개/초 삭제
acl-drop	지난 600초 동안 400개/초 삭제	지난 20초 동안 800개/초 삭제
	지난 3600초 동안 400개/초 삭제	지난 120초 동안 800개/초 삭제
• **fw-drop**	지난 600초 동안 400개/초 삭제	지난 20초 동안 1600개/초 삭제
• **inspect-drop**	지난 3600초 동안 400개/초 삭제	지난 120초 동안 1600개/초 삭제
interface-drop	지난 600초 동안 2000개/초 삭제	지난 20초 동안 8000개/초 삭제
	지난 3600초 동안 2000개/초 삭제	지난 120초 동안 8000개/초 삭제

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.
8.2(1)	버스트 속도 간격이 평균 속도의 1/60에서 1/30로 변경되었습니다.

사용 지침

각 이벤트 유형에 대해 최대 3개의 속도 간격을 구성할 수 있습니다.

기본 위협 탐지를 활성화한 경우 ASA는 "구문 설명" 표에 설명된 이벤트 유형으로 인해 삭제된 패킷의 속도 및 보안 이벤트를 모니터링합니다.

ASA는 위협을 감지한 경우 즉시 시스템 로그 메시지(733100)를 보내 ASDM에 알립니다.

기본 위협 탐지는 삭제 또는 잠재적 위협이 있는 경우에만 성능에 영향을 줍니다. 이 경우에도 성능 저하는 미미합니다.

"기본값" 섹션의 표 1-1에 기본 설정이 나와 있습니다. **show running-config all threat-detection** 명령을 사용하여 이 모든 기본 설정을 볼 수 있습니다.

이벤트 속도를 초과하는 경우 ASA는 시스템 메시지를 보냅니다. ASA는 두 가지 유형의 속도, 즉 간격 동안의 평균 이벤트 속도와 보다 짧은 버스 간격 동안의 버스트 이벤트 속도를 추적합니다. 수신된 각 이벤트에 대해 ASA는 평균 및 버스트 속도 제한을 확인합니다. 두 속도 모두 초과하는 경우 ASA는 두 개의 개별 시스템 메시지를 보냅니다(버스트 기간별 각 속도 유형에 대한 최대 하나의 메시지 포함).

예

다음 예에서는 기본 위협 감지를 활성화하고 DoS 공격에 대한 트리거를 변경합니다.

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

관련 명령

Command(명령)	설명
clear threat-detection rate	기본 위협 탐지 통계를 지웁니다.
show running-config all threat-detection	개별적으로 구성하지 않은 기본 속도 설정을 포함하여 위협 감지 컨피그레이션을 표시합니다.
show threat-detection rate	기본 위협 탐지 통계를 표시합니다.
threat-detection basic-threat	기본 위협 탐지를 활성화합니다.
threat-detection scanning-threat	스캔 위협 탐지를 활성화합니다.

threat-detection scanning-threat

스캔 위협 탐지를 활성화하려면 전역 구성 모드에서 **threat-detection scanning-threat** 명령을 사용합니다. 스캔 위협 탐지를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} | **duration** *seconds*]]

no threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} | **duration** *seconds*]]

구문 설명

duration *seconds*	10초에서 2592000초 사이의 공격 호스트에 대한 차단 기간을 설정합니다. 기본 길이는 3600초(1시간)입니다.
except	IP 주소를 차단에서 제외합니다. 이 명령을 여러 번 입력하여 차단에서 제외할 여러 IP 주소 또는 네트워크 개체 그룹을 식별할 수 있습니다.
ip-address *ip_address mask*	차단에서 제외할 IP 주소를 지정합니다.
object-group *network_object_group_id*	차단에서 제외할 네트워크 개체 그룹을 지정합니다. 객체 그룹을 만드는 방법은 **object-group network** 명령을 참고하십시오.
shun	ASA에서 호스트를 공격자로 식별한 경우 시스템 로그 메시지 733101을 보내는 것 외에, 호스트 연결을 자동으로 종료합니다.

기본값

기본 차단 기간은 3600초(1시간)입니다.

다음 기본 속도 제한은 스캔 공격 이벤트에 사용됩니다.

표 1-3 검사 위협 탐지에 대한 기본 속도 제한

평균 속도	버스트 속도
지난 600초 동안 5개/초 삭제	지난 20초 동안 10개/초 삭제
지난 3600초 동안 5개/초 삭제	지난 120초 동안 10개/초 삭제

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.
8.0(4)	**duration** 키워드가 추가되었습니다.

사용 지침

일반적인 스캐닝 공격은 서브넷의 모든 IP 주소에 대한 액세스 가능성을 테스트하는 호스트로 구성됩니다(서브넷의 여러 호스트를 통해 스캔하거나 호스트 또는 서브넷의 여러 포트를 스위핑함). 스캐닝 위협 감지 기능은 호스트에서 스캔을 수행하는 시점을 결정합니다. 트래픽 시그니처를 기반으로 하는 IPS 스캔 감지와는 달리 ASA 스캔 위협 감지 기능은 스캔 활동을 분석할 수 있는 호스트 통계가 포함된 폭넓은 데이터베이스를 유지 관리합니다.

호스트 데이터베이스는 반환 활동이 없는 연결, 닫힌 서비스 포트 액세스, 취약한 TCP 동작(예: 무작위가 아닌 IPID), 기타 여러 동작 등 의심스러운 활동을 추적합니다.

주의 검사 위협 탐지 기능은 호스트 및 서브넷 기반 데이터 구조 및 정보를 만들고 수집하는 동안 ASA 성능 및 메모리에 상당한 영향을 줄 수 있습니다.

공격자에 대한 시스템 로그 메시지를 보내도록 ASA를 구성하거나 호스트를 자동으로 차단할 수 있습니다. 기본적으로, 호스트가 공격자로 식별되면 시스템 로그 메시지 730101이 생성됩니다.

ASA는 스캔 위협 이벤트 속도가 초과된 경우 공격자 및 대상을 식별합니다. ASA는 두 가지 유형의 속도, 즉 간격 동안의 평균 이벤트 속도와 보다 짧은 버스 간격 동안의 버스트 이벤트 속도를 추적합니다. 검사 공격의 일부로 간주되는 탐지된 각 이벤트에 대해 ASA는 평균 및 버스트 속도 제한을 확인합니다. 호스트에서 전송된 트래픽이 두 속도 중 하나를 초과하는 경우 해당 호스트는 공격자로 간주됩니다. 호스트에서 수신한 트래픽이 두 속도 중 하나를 초과하는 경우 해당 호스트는 대상으로 간주됩니다. **threat-detection rate scanning-threat** 명령을 사용하여 스캔 위협 이벤트에 대한 속도 제한을 변경할 수 있습니다.

공격자 또는 대상으로 분류된 호스트를 보려면 **show threat-detection scanning-threat** 명령을 사용합니다.

차단된 호스트를 보려면 **show threat-detection shun** 명령을 사용합니다. 호스트의 차단을 해제하려면 **clear threat-detection shun** 명령을 사용합니다.

예

다음 예에서는 스캔 위협 탐지를 활성화하고 공격자로 분류된 호스트(10.1.1.0 네트워크의 호스트 제외)를 자동으로 차단합니다. 스캔 위협 탐지에 대한 기본 속도 제한도 변경됩니다.

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20
ciscoasa(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

관련 명령

Command(명령)	설명
clear threat-detection shun	호스트를 차단에서 해제합니다.
show threat-detection scanning-threat	공격자 및 대상으로 분류된 호스트를 표시합니다.
show threat-detection shun	현재 차단된 호스트를 표시합니다.
threat-detection basic-threat	기본 위협 탐지를 활성화합니다.
threat-detection rate	이벤트 유형별 위협 탐지 속도 제한을 설정합니다.

threat-detection statistics

고급 위협 탐지 통계를 활성화하려면 전역 구성 모드에서 **threat-detection statistics** 명령을 사용합니다. 고급 위협 탐지 통계를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

주의 고급 통계를 활성화할 경우 통계 유형에 따라 ASA 성능에 영향이 미칠 수 있습니다. **threat-detection statistics host** 명령은 성능에 상당한 영향을 줍니다. 트래픽 부하가 큰 경우 이 유형의 통계를 일시적으로 활성화하는 것이 좋을 수 있습니다. 그러나 **threat-detection statistics port** 명령은 적당한 영향을 줍니다.

threat-detection statistics [**access-list** | [**host** | **port** | **protocol** [**number-of-rate** {**1** | **2** | **3**}] | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

no threat-detection statistics [**access-list** | **host** | **port** | **protocol | tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

구문 설명

access-list	(선택 사항) 액세스 목록 거부에 대한 통계를 활성화합니다. 액세스 목록 통계는 **show threat-detection top access-list** 명령을 통해서만 표시됩니다.
average-rate *attacks_per_sec*	(선택 사항) TCP 가로채기에 대해 시스템 로그 메시지 생성 평균 속도 임계값(25~2147483647)을 설정합니다. 기본값은 200/초입니다. 평균 속도가 초과되면 시스템 로그 메시지 733105가 생성됩니다.
burst-rate *attacks_per_sec*	(선택 사항) TCP 가로채기에 대해 시스템 로그 메시지 생성 임계값(25~2147483647)을 설정합니다. 기본값은 400/초입니다. 버스트 속도가 초과되면 시스템 로그 메시지 733104가 생성됩니다.
host	(선택 사항) 호스트 통계를 활성화합니다. 호스트 통계는 호스트가 활성화되어 있는 동안 검사 위협 호스트 데이터베이스에서 누적됩니다. 비활성 상태가 10분간 지속된 후에는 데이터베이스에서 호스트가 삭제되고 통계가 지워집니다.
number-of-rate {**1** | **2** | **3**}	(선택 사항) 호스트, 포트 또는 프로토콜 통계에 대해 유지되는 속도 간격 수를 설정합니다. 기본 속도 간격 수는 **1**입니다. 이는 메모리 사용량을 낮게 유지합니다. 추가 속도 간격을 보려면 값을 **2** 또는 **3**으로 설정합니다. 예를 들어 값을 **3**으로 설정하면 지난 1시간, 8시간 및 24시간 동안의 데이터를 볼 수 있습니다. 이 키워드를 **1**(기본값)로 설정하면 가장 짧은 속도 간격 통계가 유지됩니다. 이 값을 **2**로 설정하면 두 개의 가장 짧은 간격이 유지됩니다.
port	(선택 사항) 포트 통계를 활성화합니다.
protocol	(선택 사항) 프로토콜 통계를 활성화합니다.
rate-interval *minutes*	(선택 사항) TCP 가로채기에 대해 기록 모니터링 윈도우 크기(1~1440분)를 설정합니다. 기본값은 30분입니다. 이 간격 동안 ASA는 30회의 공격을 샘플링합니다.
tcp-intercept	(선택 사항) TCP 가로채기에 의해 가로채기된 공격에 대한 통계를 활성화합니다. TCP 가로채기를 활성화하려면 **set connection embryonic-conn-max command** 또는 **nat** 또는 **static** 명령을 참고하십시오.

기본값

액세스 목록 통계는 기본적으로 활성화되어 있습니다. 이 명령에서 옵션을 지정하지 않으면 모든 옵션이 활성화됩니다.

기본 **tcp-intercept rate-interval**은 30분입니다. 기본 **burst-rate**은 400/초입니다. 기본 **average-rate**은 200/초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.
8.0(4), 8.1(2)	**tcp-intercept** 키워드가 추가되었습니다.
8.1(2)	**number-of-rates** 키워드가 호스트 통계에 대해 추가되고, 기본 속도 수가 3에서 1로 변경되었습니다.
8.2(1)	버스트 속도 간격이 평균 속도의 1/60에서 1/30로 변경되었습니다.
8.3(1)	**number-of-rates** 키워드가 포트 및 프로토콜 통계에 대해 추가되고, 기본 속도 수가 3에서 1로 변경되었습니다.

사용 지침

이 명령에서 옵션을 지정하지 않으면 모든 통계가 활성화됩니다. 특정 통계만 활성화하려면 각 통계 유형에 대해 이 명령을 입력하고, 옵션 없이 명령을 입력하지 않습니다. **threat-detection statistics**(옵션 없이)를 입력한 다음 statistics-specific 옵션과 함께 명령을 입력(예: **threat-detection statistics host number-of-rate 2**)하여 특정 통계를 사용자 지정할 수 있습니다. **threat-detection statistics**(옵션 없이)를 입력한 다음 특정 통계에 대한 명령을 통계별 옵션 없이 입력한 경우에는 해당 명령이 이미 활성화되어 있기 때문에 아무 효과가 없습니다.

이 명령의 **no** 형식을 입력한 경우에는 모든 **threat-detection statistics** 명령(기본적으로 활성화되는 **threat-detection statistics access-list** 명령 포함)이 제거됩니다.

show threat-detection statistics 명령을 사용하여 통계를 확인합니다.

threat-detection scanning-threat 명령을 사용하여 스캔 위협 탐지를 활성화하지 않아도 됩니다. 탐지와 통계를 개별적으로 구성할 수 있습니다.

예

다음 예에서는 호스트를 제외하고 모든 유형에 대해 스캔 위협 탐지 및 스캔 위협 통계를 활성화합니다.

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection statistics access-list
ciscoasa(config)# threat-detection statistics port
ciscoasa(config)# threat-detection statistics protocol
ciscoasa(config)# threat-detection statistics tcp-intercept
```

관련 명령

Command(명령)	설명
threat-detection scanning-threat	스캔 위협 탐지를 활성화합니다.
show threat-detection statistics host	호스트 통계를 표시합니다.
show threat-detection memory	고급 위협 탐지 통계의 메모리 사용량을 표시합니다.
show threat-detection statistics port	포트 통계를 표시합니다.
show threat-detection statistics protocol	프로토콜 통계를 표시합니다.
show threat-detection statistics top	상위 10개의 통계를 표시합니다.

threshold

SLA 모니터링 작업에서 임계값 초과 이벤트에 대한 임계값을 설정하려면 SLA 모니터 구성 모드에서 **threshold** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

threshold *milliseconds*

no threshold

구문 설명

milliseconds	선언할 상승 임계값의 밀리초 수를 지정합니다. 유효한 값은 1 ~ 2147483647입니다. 이 값은 시간 초과에 대해 설정된 값보다 클 수 없습니다.

기본값

기본 임계값은 5000밀리초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
SLA 모니터 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

임계값은 연결성에 영향을 주지 않지만 **timeout** 명령에 대한 적절한 설정을 평가하는 데 사용될 수 있는 초과 임계값 이벤트를 나타내는 데에만 사용됩니다.

예

다음 예에서는 ID 123을 사용하여 SLA 작업을 구성하고 ID가 1인 추적 작업을 만들어 SLA 연결성을 추적합니다. SLA 작업의 빈도는 10초, 임계값은 2500밀리초, 시간 초과 값은 4000밀리초로 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)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

Command(명령)	설명
sla monitor	SLA 모니터링 작업을 정의합니다.
timeout	SLA 작업의 응답 대기 시간을 정의합니다.

throughput level

스마트 라이센싱 자격 요청에 대한 처리량 수준을 설정하려면 라이선스 스마트 구성 모드에서 **throughput level** 명령을 사용합니다. 처리량 수준을 제거하고 장치의 라이선스를 해제하려면 이 명령의 **no** 형식을 사용합니다.

참고 이 기능은 ASAv에서만 지원됩니다.

throughput level {100M | 1G | 2G}

no throughput level [100M | 1G | 2G]

구문 설명

100M	처리량 수준을 100Mbps로 설정합니다.
1G	처리량 수준을 1Gbps로 설정합니다.
2G	처리량 수준을 2Gbps로 설정합니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
라이선스 스마트 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
9.3(2)	이 명령이 추가되었습니다.

사용 지침

처리량 수준을 요청하거나 변경한 경우 라이선스 스마트 구성 모드를 종료해야 변경 사항이 적용됩니다.

예

다음 예에서는 기능 계층을 standard로 설정하고, 처리량 수준을 2G로 설정합니다.

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
call-home	Smart Call Home을 구성합니다. Smart Licensing은 Smart Call Home 인프라를 사용합니다.
clear configure license	Smart Licensing 구성을 지웁니다.
feature tier	Smart Licensing에 대한 기능 계층을 설정합니다.
http-proxy	Smart Licensing 및 Smart Call Home에 대한 HTTP(S) 프록시를 설정합니다.
license smart	Smart Licensing에 대한 라이선스 자격을 요청할 수 있습니다.
license smart deregister	라이선스 기관에서 디바이스의 등록을 해제합니다.
license smart register	라이선스 기관에 디바이스를 등록합니다.
license smart renew	등록 또는 라이선스 자격을 갱신합니다.
service call-home	Smart Call Home을 활성화합니다.
show license	Smart Licensing 상태를 표시합니다.
show running-config license	Smart Licensing 구성을 표시합니다.

ticket(사용되지 않음)

Cisco Intercompany Media Engine 프록시에 대한 티켓 에포크 및 비밀번호를 구성하려면 UC-IME 구성 모드에서 **ticket** 명령을 사용합니다. 프록시에서 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ticket epoch *n* **password** *password*

no ticket epoch *n* **password** *password*

구문 설명

n	비밀번호 무결성 확인 간격을 지정합니다. 1~255의 정수를 입력합니다.
password	Cisco Intercompany Media Engine 티켓에 대한 비밀번호를 설정합니다. US-ASCII 문자 집합에서 10~64자의 인쇄 가능한 문자를 입력합니다. 허용되는 문자에는 0x21~0x73이 포함되며, 공백 문자는 제외됩니다. 한 번에 하나의 비밀번호만 구성할 수 있습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
UC-IME 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.3(1)	이 명령이 추가되었습니다.
9.4(1)	이 명령은 모든 **uc-ime** 모드 명령과 함께 사용이 중단되었습니다.

사용 지침

Cisco Intercompany Media Engine에 대한 티켓 에포크 및 비밀번호를 구성합니다.

에포크는 비밀번호가 변경된 각 시점을 업데이트하는 정수를 포함합니다. 프록시를 처음 구성하고 비밀번호를 처음 입력하는 경우 에포크 정수에 1을 입력합니다. 비밀번호를 변경할 때마다 새 비밀번호를 나타내도록 에포크를 증가시킵니다. 비밀번호를 변경할 때마다 에포크 값을 증가시켜야 합니다.

일반적으로 에포크를 순차적으로 증가시킵니다. 그러나 ASA에서는 에포크를 업데이트할 때 원하는 값을 선택할 수 있습니다.

에포크 값을 변경하면 현재 비밀번호가 무효화되므로 새 비밀번호를 입력해야 합니다.

20자 이상의 비밀번호를 사용하는 것이 좋습니다. 한 번에 하나의 비밀번호만 구성할 수 있습니다.

티켓 비밀번호는 플래시에 저장됩니다. **show running-config uc-ime** 명령의 출력에는 비밀번호 문자열 대신 *****가 표시됩니다.

참고 ASA에서 구성한 에포크 및 비밀번호는 Cisco Intercompany Media Engine 서버에서 구성한 에포크 및 비밀번호와 일치해야 합니다. 자세한 내용은 Cisco Intercompany Media Engine 서버 설명서를 참고하십시오.

예

다음 예에서는 Cisco Intercompany Media Engine 프록시에서 티켓 및 에포크를 지정하는 방법을 보여 줍니다.

```
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
hostname(config-uc-ime)# fallback monitoring timer 120
hostname(config-uc-ime)# fallback hold-down timer 30
```

관련 명령

Command(명령)	설명
show running-config uc-ime	Cisco Intercompany Media Engine 프록시의 실행 중인 구성을 표시합니다.
uc-ime	ASA에서 Cisco Intercompany Media Engine 프록시 인스턴스를 생성합니다.

timeout (aaa-server host)

AAA 서버와의 연결 설정을 중단하기 전에 허용되는 호스트별 최대 응답 시간을 구성하려면 aaa-server host 모드에서 **timeout** 명령을 사용합니다. 시간 제한 값을 제거하고 시간 제한을 기본값 10초로 다시 설정하려면 이 명령의 **no** 형식을 사용합니다.

timeout *seconds*

no timeout

구문 설명

seconds	서버에 대한 시간 제한 간격(1~60초)을 지정합니다. 이 값에 실패한 시도의 최대 횟수(AAA 서버 그룹의 **max-failed-attempts** 명령으로 정의)를 곱한 결과가 서버 연결을 성공적으로 시도하는 데 필요한 전체 시간 제한 기간입니다. 전체 시간 제한 기간이 만료되면 ASA에서 기본 AAA 서버에 대한 요청을 제공합니다. 대기 AAA 서버가 있는 경우 ASA는 백업 서버로 요청을 보냅니다.

기본값

기본 시간 제한 값은 10초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
aaa-server host configuration	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 모든 AAA 서버 프로토콜 유형에 사용할 수 있습니다.

timeout 및 **max-failed-attempts** 명령을 사용하여 ASA가 AAA 서버에 연결하려고 시도하는 기간을 지정할 수 있습니다. 이러한 값은 전체 시간 제한을 얻기 위해 곱해집니다. 예를 들어, 시간 제한이 30초이고 최대 실패 시도 횟수가 5회인 경우 시스템은 150초 내에 요청을 완료해야 합니다.

retry-interval 명령을 사용하여 ASA가 연결 시도 간에 대기하는 기간을 지정할 수 있습니다. 이러한 간격은 전체 시간 제한 내에서 발생하므로 재시도 간격이 긴 경우, 시스템은 전체 시간 제한 내에 재시도 횟수를 줄일 수 있습니다. 실제로 재시도 간격은 시간 제한 간격보다 작아야 합니다.

예

다음 예에서는 호스트 1.2.3.4에서 10초의 재시도 간격으로 시간 제한 값 30초를 사용하도록 "svrgrp1" 이라는 RADIUS AAA 서버를 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 30
ciscoasa(config-aaa-server-host)# retry-interval 10
ciscoasa(config-aaa-server-host)#
```

관련 명령

Command(명령)	설명
aaa-server host	호스트별 AAA 서버 파라미터를 구성할 수 있도록 aaa server host 구성 모드를 시작합니다.
clear configure aaa-server	구성에서 모든 AAA 명령문을 제거합니다.
show running-config aaa	현재 AAA 구성 값을 표시합니다.

timeout (dns server-group)

다음 DNS 서버를 시도하기 전에 대기할 기간을 지정하려면 dns server-group 구성 모드에서 **timeout** 명령을 사용합니다. 기본 시간 제한을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timeout *seconds*

no timeout [*seconds*]

구문 설명

seconds	1초에서 30초 사이의 시간 제한(초)을 지정합니다. 기본값은 2초입니다. ASA가 서버 목록을 재시도할 때마다 이 시간 제한이 두 배가 됩니다. dns-server-group 구성 모드에서 **retries** 명령을 사용하여 재시도 횟수를 구성할 수 있습니다.

기본값

기본 시간 초과 값은 2초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
dns server-group 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.

예

다음 예에서는 DNS 서버 그룹 "dnsgroup1" 의 시간 제한을 1초로 설정합니다.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# dns timeout 1
```

관련 명령

Command(명령)	설명
clear configure dns	사용자가 만든 모든 DNS 서버 그룹을 제거하고 기본 서버 그룹의 특성을 기본값으로 재설정합니다.
domain-name	기본 도메인 이름을 설정합니다.
retries	ASA가 응답을 받지 못한 경우 DNS 서버 목록을 재시도할 횟수를 지정합니다.
show running-config dns server-group	현재 실행 중인 DNS 서버 그룹 구성을 표시합니다.

timeout (global)

여러 기능에 대한 전역 최대 유휴 시간을 설정하려면 전역 구성 모드에서 **timeout** 명령을 사용합니다. 모든 시간 제한을 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다. 단일 기능을 해당 기본값으로 재설정하려면 기본값과 함께 **timeout** 명령을 다시 입력합니다.

timeout {**conn** | **conn-holddown** | **floating-conn** | **h225** | **h323** | **half-closed** | **icmp** | **icmp-error** | **igp stale-route** | **mgcp** | **mgcp-pat** | **pat-xlate** | **sctp** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **sip-provisional-media** | **sunrpc** | **tcp-proxy-reassembly** | **udp** | **xlate**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

no timeout

구문 설명

absolute	(**uauth**의 경우 선택 사항) uauth 시간 제한이 만료된 후 재인증을 요구합니다. **absolute** 키워드는 기본적으로 활성화되어 있습니다. 비활성 기간 후 시간 초과되도록 uauth 타이머를 설정하려면 대신 **inactivity** 키워드를 입력합니다.
conn	연결이 닫히기 전에 경과해야 하는 유휴 시간(0:5:0~1193:0:0)을 지정합니다. 기본값은 1시간(1:0:0)입니다. 연결이 시간 초과되지 않도록 하려면 **0**을 사용합니다.
conn-holddown	이제 더 이상 존재하지 않거나 비활성 상태인 연결에서 경로를 사용할 경우, 시스템이 연결을 유지해야 하는 기간입니다. 경로가 이 보류 기간 이내에 활성화되지 않으면 연결이 해제됩니다. 연결 보류 타이머의 목적은 경로 플래핑의 효과를 줄이기 위한 것입니다. 여기서 경로는 빠르게 설정되었다가 해제될 수 있습니다. 경로 통합이 더 신속하게 발생하도록 보류 타이머를 줄일 수 있습니다. 기본값은 15초이고 범위는 00:00:00~00:00:15입니다.
floating-conn	여러 경로가 서로 다른 메트릭으로 네트워크에 존재하는 경우 ASA는 연결 생성 시 최상의 메트릭이 있는 경로를 사용합니다. 더 나은 경로를 사용할 수 있게 되면 연결을 다시 설정하여 해당 경로를 사용할 수 있도록 이 시간 제한을 통해 연결을 닫을 수 있습니다. 기본값은 0(연결이 시간 초과되지 않음)입니다. 더 나은 경로를 사용하려면 타임아웃 값을 0:0:30~1193:0:0로 설정합니다.
hh:*mm*:*ss*	시간, 분, 초 단위로 시간 제한을 지정합니다. 연결이 시간 초과되지 않도록 하려면 **0**을 사용합니다(사용 가능한 경우).
h225	H.225 신호 처리 연결이 닫히기 전에 경과해야 하는 유휴 시간(0:0:0~1193:0:0)을 지정합니다. 기본값은 1시간(1:0:0)입니다. 시간 제한 값 0:0:1은 모든 호출이 지워지는 즉시 타이머를 비활성화하고 TCP 연결을 닫습니다.
h323	H.245(TCP) 및 H.323(UDP) 미디어 연결이 닫히기 전에 경과해야 하는 유휴 시간(0:0:0~1193:0:0)을 지정합니다. 기본값은 5분(0:5:0)입니다. H.245 및 H.323 미디어 연결 모두에 동일한 연결 플래그가 설정되어 있으므로 H.245(TCP) 연결에서 H.323(RTP 및 RTCP) 미디어 연결과 유휴 시간 제한을 공유합니다.

half-closed	TCP 반 닫힘 연결이 해제되기 전에 경과해야 하는 유휴 시간을 0:5:0(9.1(1) 이하) 또는 0:0:30(9.1(2) 이상)에서 1193:0:0 사이로 지정합니다. 기본값은 10분(0:10:0)입니다. 연결이 시간 초과되지 않도록 하려면 **0**을 사용합니다.
icmp	ICMP에 대한 유휴 시간(0:0:2~1193:0:0)을 지정합니다. 기본값은 2초(0:0:2)입니다.
icmp-error	ASA에서 ICMP 에코-응답 패킷을 수신한 후 ICMP 연결을 제거하기 전까지 유휴 시간을 지정합니다. 이는 0:0:0에서 0:1:0 사이 또는 **timeout icmp** 값 중 더 낮은 값입니다. 기본값은 **0**(비활성화됨)입니다. 이 시간 제한이 비활성화된 경우와 사용자가 ICMP 검사를 활성화한 경우, ASA가 에코-응답을 수신하는 즉시 ICMP 연결을 제거하므로 연결(현재 닫힘)에 대해 생성된 모든 ICMP 오류가 삭제됩니다. 이 시간 제한은 ICMP 연결 제거를 지연시키므로 중요한 ICMP 오류를 수신할 수 있습니다.
igp stale-route	라우터 정보 기반에서 제거하기 전에 오래된 경로를 유지할 수 있는 유휴 시간을 지정합니다. 이러한 경로는 OSPF와 같은 내부 게이트웨이 프로토콜에 대한 것입니다. 기본값은 70초(00:01:10)이고 범위는 00:00:10~00:01:40입니다.
inactivity	(**uauth**의 경우 선택 사항) 비활성 시간 제한 만료 후 uauth 재인증을 요구합니다.
mgcp	MGCP 미디어 연결이 제거되기 전에 경과해야 하는 유휴 시간(0:0:0~1193:0:0)을 설정합니다. 기본값은 5분(0:5:0)입니다.
mgcp-pat	MGCP PAT 변환이 제거되기 전에 경과해야 하는 절대 간격(0:0:0~1193:0:0)을 설정합니다. 기본값은 5분(0:5:0)입니다.
pat-xlate	PAT 변환 슬롯이 확보될 때까지 경과해야 하는 유휴 시간(0:0:30~0:5:0)을 설정합니다. 기본값은 30초입니다. 이전 연결이 업스트림 디바이스에서 여전히 열려 있을 수 있기 때문에 업스트림 라우터가 확보된 PAT 포트를 사용하는 새 연결을 거부하는 경우 시간 제한을 늘릴 수 있습니다.
sctp	SCTP(Stream Control Transmission Protocol) 연결이 닫힐 때까지의 유휴 시간(0:1:0~1193:0:0)을 지정합니다. 기본값은 2분(0:2:0)입니다.
sip	SIP 제어 연결이 닫히기 전까지 경과해야 하는 유휴 시간(0:5:0~1193:0:0)을 지정합니다. 기본값은 30분(0:30:0)입니다. 연결이 시간 초과되지 않도록 하려면 **0**을 사용합니다.
sip-disconnect	CANCEL 또는 BYE 메시지에 대해 200 OK가 수신되지 않은 경우 SIP 세션이 삭제되기 전까지 경과해야 하는 유휴 시간(0:0:1~00:10:0)을 지정합니다. 기본값은 2분(0:2:0)입니다.
sip-invite	(선택 사항) PROVISIONAL 메시지 및 미디어 xlate에 대한 핀홀이 닫히기 전까지 경과해야 하는 유휴 시간(0:1:0~1193:0:0)을 지정합니다. 기본값은 3분(0:3:0)입니다.
sip_media	SIP 미디어 연결이 닫히기 전까지 경과해야 하는 유휴 시간(0:1:0~1193:0:0)을 지정합니다. 기본값은 2분(0:2:0)입니다. 연결이 시간 초과되지 않도록 하려면 **0**을 사용합니다. SIP 미디어 타이머는 UDP 비활성 시간 제한 대신 SIP UDP 미디어 패킷이 있는 SIP RTP/RTCP에 사용됩니다.
sip-provisional-media	SIP 프로비전 미디어 연결의 시간 제한 값(0:1:0~1193:0:0)을 지정합니다. 기본값은 2분(0:2:0)입니다.

sunrpc	SUNRPC 슬롯이 닫히기 전까지 경과해야 하는 유휴 시간(0:1:0~1193:0:0)을 지정합니다. 기본값은 10분(0:10:0)입니다. 연결이 시간 초과되지 않도록 하려면 **0**을 사용합니다.
tcp-proxy-reassembly	재어셈블을 대기하는 버퍼된 패킷이 삭제되기 전까지 경과해야 하는 유휴 시간 제한(0:0:10~1193:0:0)을 구성합니다. 기본값은 1분(0:1:0)입니다.
uauth	인증 및 권한 부여 캐시가 시간 초과되어 사용자가 다음 연결을 재인증해야 하기 전까지 경과해야 하는 기간(0:0:0~1193:0:0)을 지정합니다. 기본값은 5분(0:5:0)입니다. 기본 타이머는 **absolute**입니다. **inactivity** 키워드를 입력하여 비활성 기간 이후에 시간 제한이 발생하도록 설정할 수 있습니다. **uauth** 기간은 **xlate** 기간보다 짧아야 합니다. 캐싱을 비활성화하려면 **0**으로 설정합니다. 수동 FTP가 연결에 사용되거나 **virtual http** 명령이 웹 인증에 사용되는 경우에는 **0**을 사용하지 마십시오.
udp	UDP 슬롯이 확보될 때까지 경과해야 하는 유휴 시간(0:1:0~1193:0:0)을 설정합니다. 기본값은 2분(0:2:0)입니다. 연결이 시간 초과되지 않도록 하려면 **0**을 사용합니다.
xlate	변환 슬롯이 확보될 때까지 경과해야 하는 유휴 시간(0:1:0~1193:0:0)을 설정합니다. 기본값은 3시간(3:0:0)입니다.

기본값

기본값은 다음과 같습니다.

- **conn**은 1시간(**1:0:0**)입니다.
- **conn-holddown**은 15초(**0:0:15**)입니다.
- **floating-conn**은 시간 초과되지 않습니다(**0**).
- **h225**는 1시간(**1:0:0**)입니다.
- **h323**은 5분(**0:5:0**)입니다.
- **half-closed**는 10분(**0:10:0**)입니다.
- **icmp**는 2초(**0:0:2**)입니다.
- **icmp-error**는 시간 초과되지 않습니다(**0**).
- **igp stale-route**는 70초(**00:01:10**)입니다.
- **mgcp**는 5분(**0:5:0**)*입니다.*
- **mgcp-pat**는 5분(**0:5:0**)*입니다.*
- **rpc**는 5분(**0:5:0**)입니다.
- **sctp**는 2분(**0:2:0**)입니다.
- **sip**는 30분(**0:30:0**)입니다.
- **sip-disconnect**는 2분(**0:2:0**)입니다.
- **sip-invite**는 3분(**0:3:0**)입니다.
- **sip_media**는 2분(**0:2:0**)입니다.
- **sip-provisional-media**는 2분(**0:2:0**)입니다.
- **sunrpc**는 10분(**0:10:0**)입니다.
- **tcp-proxy-reassembly**는 1분(**0:1:0**)입니다.

- **uauth**는 5분(**0:5:0**)입니다(**절대값**).
- **udp**는 2분(**0:02:0**)입니다.
- **xlate**는 3시간(**3:0:0**)입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성 모드	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	**mgcp-pat**, **sip-disconnect** 및 **sip-invite** 키워드가 추가되었습니다.
7.2(4)/8.0(4)	**sip-provisional-media** 키워드가 추가되었습니다.
7.2(5)/8.0(5)/8.1(2)/8.2(1)	**tcp-proxy-reassembly** 키워드가 추가되었습니다.
8.2(5)/8.4(2)	**floating-conn** 키워드가 추가되었습니다.
8.4(3)	**pat-xlate** 키워드가 추가되었습니다.
9.1(2)	최소 **half-closed** 값이 30초(0:0:30)로 낮아졌습니다.
9.4(3)/9.6(2)	**conn-holddown** 키워드가 추가 되었습니다.
9.5(2)	**sctp** 키워드가 추가되었습니다.
9.7(1)	**igp stale-route** 키워드가 추가되었습니다.
9.8(1)	**icmp-error** 키워드가 추가되었습니다.

사용 지침

timeout 명령을 사용하여 전역 시간 제한을 설정할 수 있습니다. 일부 기능의 경우 **set connection timeout** 명령은 해당 명령에서 식별된 트래픽에 대해 우선적으로 적용됩니다.

timeout 명령 뒤에 여러 키워드 및 값을 입력할 수 있습니다.

연결 타이머(**conn**)가 변환 타이머(**xlate**)보다 우선합니다. 변환 타이머는 모든 연결이 시간 초과된 후에만 작동합니다.

예

다음 예에서는 최대 유휴 시간을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
ciscoasa(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

관련 명령

Command(명령)	설명
clear configure timeout	시간 제한 구성을 지우고 기본값으로 다시 설정합니다.
set connection timeout	MPF(Modular Policy Framework)를 사용하여 연결 시간 제한을 설정합니다.
show running-config timeout	지정된 프로토콜의 시간 제한 값을 표시합니다.

timeout (policy-map type inspect gtp > parameters)

GTP 세션에 대한 비활성 타이머를 변경하려면 파라미터 구성 모드에서 **timeout** 명령을 사용합니다. 먼저 **policy-map type inspect gtp** 명령을 입력하여 파라미터 구성 모드에 액세스할 수 있습니다. 이러한 간격을 해당 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

timeout {**endpoint** | **gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *hh*:*mm*:*ss*

no timeout {**endpoint** | **gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel**} *hh*:*mm*:*ss*

구문 설명

hh:*mm*:*ss*	지정된 서비스에 대한 유휴 시간 제한(시간:분:초 형식)입니다. 시간 제한을 없애려면 숫자에 0을 지정합니다.
endpoint	GTP 엔드포인트를 제거하기까지의 최대 비활성 상태 기간입니다.
gsn	GSN을 제거하기까지의 최대 비활성 상태 기간입니다. 9.5(1)부터는 이 키워드가 제거되고 **endpoint** 키워드로 대체됩니다.
pdp-context	GTP 세션 중에 PDP 컨텍스트를 제거하기까지의 최대 비활성 상태 기간입니다. GTPv2에서 이는 베어러 컨텍스트입니다.
request	요청 대기열에서 요청이 제거된 후의 최대 비활성 기간입니다. 폐기된 요청에 대한 후속 응답도 모두 손실됩니다.
signaling	GTP 신호를 제거하기까지의 최대 비활성 상태 기간입니다.
t3-response	연결을 제거하기까지의 최대 응답 대기 시간입니다.
tunnel	GTP 터널이 해제되기까지의 최대 비활성 상태 기간입니다.

기본값

기본값은 **endpoint**, **gsn**, **pdp-context** 및 **signaling**의 경우 30분입니다.

request에 대한 기본값은 1분입니다.

tunnel에 대한 기본값은 1시간입니다(PDP 상황 삭제 요청이 수신되지 않은 경우).

t3-response에 대한 기본값은 20초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.5(1)	**gsn** 키워드가 **endpoint**로 대체되었습니다.

사용 지침

GTP 검사에서 사용되는 기본 시간 제한을 변경하려면 이 명령을 사용합니다.

예

다음 예에서는 요청 대기열에 대한 시간 제한 값을 2분으로 설정합니다.

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout request 00:02:00
```

관련 명령

명령	설명
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
inspect gtp	애플리케이션 검사에 사용할 특정 GTP 맵을 적용합니다.
show service-policy inspect gtp	GTP 구성을 표시합니다.

timeout (policy-map type inspect m3ua > parameters)

M3UA 세션에 대한 비활성 타이머를 변경하려면 파라미터 구성 모드에서 **timeout** 명령을 사용합니다. 먼저 **policy-map type inspect m3ua** 명령을 입력하여 파라미터 구성 모드에 액세스할 수 있습니다. 이러한 간격을 해당 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

timeout {**endpoint | session}** *hh*:*mm*:*ss*

no timeout {**endpoint | session}** *hh*:*mm*:*ss*

구문 설명

hh:*mm*:*ss*	지정된 서비스에 대한 유휴 시간 제한(시간:분:초 형식)입니다. 시간 제한을 없애려면 숫자에 0을 지정합니다.
endpoint	M3UA 엔드포인트에 대한 통계를 제거하기까지의 최대 비활성 상태 기간입니다. 기본값은 30분입니다.
session	엄격한 ASP 상태 검증을 활성화한 경우 M3UA 세션을 제거할 유휴 시간 제한(hh:mm:ss 형식)입니다. 기본값은 30분(00:30:00)입니다. 이 시간 제한을 비활성화하면 시스템이 오래된 세션을 제거하는 것을 방지할 수 있습니다.

기본값

endpoint 및 **session**의 경우 기본값은 30분입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.6(2)	이 명령이 추가되었습니다.
9.7(1)	**session** 키워드가 추가되었습니다.

사용 지침

M3UA 검사에서 사용되는 기본 시간 제한을 변경하려면 이 명령을 사용합니다.

예

다음 예에서는 엔드포인트의 시간 제한을 45분으로 설정합니다.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
```

관련 명령

명령	설명
inspect m3ua	M3UA 검사를 활성화합니다.
policy-map type inspect	검사 정책 맵을 만듭니다.
show service-policy inspect m3ua	M3UA 통계를 표시합니다.
strict-asp-state	엄격한 M3UA ASP 상태 검증을 활성화합니다.

timeout (policy-map type inspect radius-accounting > parameters)

RADIUS 어카운트 관리 사용자에 대한 비활성 타이머를 변경하려면 파라미터 구성 모드에서 **timeout** 명령을 사용합니다. 먼저 **policy-map type inspect radius-accounting** 명령을 입력하여 파라미터 구성 모드에 액세스할 수 있습니다. 이러한 간격을 해당 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

구문 설명

hh:*mm*:*ss*	시간 제한입니다. 여기서 *hh*는 시간을 지정하고, *mm*은 분을 지정하며, *ss*는 초를 지정하고, 콜론(:)은 이 세 구성요소를 구분합니다. 0 값은 즉시 중지되지 않음을 의미합니다. 기본값은 1시간입니다.
users	사용자에 대한 시간 제한을 지정합니다.

기본값

사용자에 대한 기본 시간 제한은 1시간입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

예

다음 예에서는 사용자에 대한 시간 제한 값을 10분으로 설정합니다.

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout user 00:10:00
```

관련 명령

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

timeout (type echo)

SLA 작업이 요청 패킷에 대한 응답을 기다리는 시간을 설정하려면 유형 에코 구성 모드에서 **timeout** 명령을 사용합니다. 먼저 **sla monitor** 명령을 입력하여 유형 에코 구성 모드에 액세스할 수 있습니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timeout *milliseconds*

no timeout

구문 설명

milliseconds	0~604800000입니다.

기본값

기본 시간 제한 값은 5000밀리초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
type echo 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

frequency 명령을 사용하여 SLA 작업이 요청 패킷을 보내는 빈도를 설정하고, **timeout** 명령을 사용하여 SLA 작업이 해당 요청에 대한 응답을 기다리는 기간을 설정할 수 있습니다. **timeout** 명령에 지정된 값은 **frequency** 명령에 지정된 값보다 클 수 없습니다.

예

다음 예에서는 ID 123을 사용하여 SLA 작업을 구성하고 ID가 1인 추적 작업을 만들어 SLA 연결성을 추적합니다. SLA 작업의 빈도는 10초, 임계값은 2500밀리초, 시간 초과 값은 4000밀리초로 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)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

Command(명령)	설명
frequency	SLA 작업이 반복되는 빈도를 지정합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.

timeout assertion

SAML 시간 제한을 구성하려면 webvpn 구성 모드에서 **timeout assertion** 명령을 사용합니다.

timeout assertion *number of seconds*

구문 설명

number of seconds	SAML IdP 시간 제한(초)입니다.

기본값

기본값은 none입니다. 즉, 어설션의 NotBefore 및 NotOnOrAfter가 유효성을 확인함을 의미합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
config webVPN	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.5.2	이 명령이 추가되었습니다.

사용 지침

지정된 경우 이 구성은 NotBefore의 합계와 시간 제한(초 단위)이 NotOnOrAfter 이전인 경우 NotOnOrAfter를 재정의합니다. 지정되지 않은 경우 어설션에서 NotBefore 및 NotOnOrAfter가 유효성을 확인하는 데 사용됩니다. config-webvpn-saml-idp에서 시간 제한 값을 입력하는 경우 어설션과 초 수 값 모두 필수입니다.

예

다음 예에서는 클라이언트리스 VPN 기반 URL, SAML 요청 서명 및 SAML 어설션 시간 제한을 구성합니다.

```
ciscoasa(config-webvpn-saml-idp)# base url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

timeout edns

서버에서 응답이 없는 경우 클라이언트에서 Umbrella 서버로의 연결을 제거하기 전의 유휴 시간 제한을 구성하려면 Umbrella 구성 모드에서 **timeoutedns** 명령을 사용합니다. 기본 설정으로 돌아가려면 이 명령의 **no** 형식을 사용합니다.

timeout edns *hh*:*mm*:*ss*

no timeout edns *hh*:*mm*:*ss*

구문 설명

hh:*mm*:*ss*	클라이언트에서 Umbrella 서버로의 연결에 대한 유휴 시간 제한(시간:분:초 형식)으로, 0:0:0~1193:0:0입니다. 기본값은 0:02:00(2분)입니다. 시간 제한을 없애려면 숫자에 0을 지정합니다.

기본값

기본값은 0:02:00(2분)입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
Umbrella 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.10(1)	이 명령이 추가되었습니다.

예

다음 예에서는 클라이언트에서 Umbrella 서버로의 연결에 대해 1분의 유휴 시간 제한을 설정합니다.

```
ciscoasa(config)# umbrella-global
ciscoasa(config)# timeout edns 0:1:0
```

관련 명령

명령	설명
public-key	Cisco Umbrella와 함께 사용 되는 공개 키를 구성 합니다.
token	Cisco Umbrella에 등록하는 데 필요한 API 토큰을 식별합니다.
umbrella-global	Cisco Umbrella 전역 파라미터를 구성합니다.

timeout pinhole

DCERPC 핀홀에 대한 시간 제한을 구성하고 전역 시스템 핀홀 시간 제한(2분)을 재정의하려면 파라미터 구성 모드에서 **timeout pinhole** 명령을 사용합니다. 파라미터 구성 모드는 정책 맵 구성 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

timeout pinhole *hh:mm:ss*

no timeout pinhole

구문 설명

hh:mm:ss	핀홀 연결에 대한 시간 제한입니다. 값은 0:0:1~1193:0:0입니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

예

다음 예에서는 DCERPC 검사 정책 맵에서 핀홀 연결에 대한 핀홀 시간 제한을 구성하는 방법을 보여 줍니다.

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

관련 명령

Command(명령)	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	Layer 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

timeout secure-phones (사용되지 않음)

secure-phone 항목이 Phone Proxy 데이터베이스에서 제거될 때까지의 유휴 시간 제한을 구성하려면 phone-proxy 구성 모드에서 **timeout secure-phones** 명령을 사용합니다. 시간 제한 값을 기본값인 5분으로 다시 설정하려면 이 명령의 **no** 형식을 사용합니다.

timeout secure-phones *hh:mm:ss*

no timeout secure-phones *hh:mm:ss*

구문 설명

hh:mm:ss	개체가 제거될 때까지의 유휴 시간 제한을 지정합니다. 기본값은 5분입니다.

기본값

보안 전화기 시간 제한에 대한 기본값은 5분입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.0(4)	이 명령이 추가되었습니다.
9.4(1)	이 명령은 모든 **phone-proxy** 모드 명령과 함께 사용이 중단되었습니다.

사용 지침

보안 전화기는 부팅 시 항상 CTL 파일을 요청하기 때문에 Phone Proxy는 전화기를 안전한 것으로 표시하는 데이터베이스를 생성합니다. 보안 전화기 데이터베이스의 항목은 구성된(**timeout secure-phones** 명령을 통해) 시간 제한 후 제거됩니다. 이 항목의 타임스탬프는 SIP 전화기의 경우 Phone Proxy에서 받은 각 등록 새로 고침, SCCP 전화기의 경우 KeepAlive에 대해 업데이트됩니다.

timeout secure-phones 명령의 기본값은 5분값입니다. SCCP KeepAlive 및 SIP 등록 새로 고침에 대한 최대 시간 제한 값보다 큰 값을 지정합니다. 예를 들어 SCCP Keepalive가 1분 간격으로 구성되고 SIP 등록 새로 고침이 3분으로 구성된 경우 이 시간 제한 값을 3분보다 큰 값으로 구성합니다.

예

다음 예에서는 **timeout secure-phones** 명령을 사용하여 3분 후 보안 전화기 데이터베이스의 항목이 시간 초과되도록 Phone Proxy를 구성합니다.

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
ciscoasa(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
ciscoasa(config-phone-proxy)# media-termination address 192.168.1.4
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
```

```
ciscoasa(config-phone-proxy)# ctl-file asactl
ciscoasa(config-phone-proxy)# timeout secure-phones 00:03:00
```

관련 명령

Command(명령)	설명
phone-proxy	전화 프록시 인스턴스를 구성합니다.

time-range

time-range 구성 모드를 시작하고 트래픽 규칙 또는 작업에 연결할 수 있는 시간 범위를 정의하려면 전역 구성 모드에서 **time-range** 명령을 사용합니다. 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

time-range *name*

no time-range *name*

구문 설명

name 시간 범위의 이름입니다. 이름은 64자 이하여야 합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

시간 범위 생성은 디바이스에 대한 액세스를 제한하지 않습니다. **time-range** 명령은 시간 범위만을 정의합니다. 시간 범위를 정의한 후에는 트래픽 규칙 또는 작업에 연결할 수 있습니다.

시간 기반 ACL을 구현하려면 **time-range** 명령을 사용하여 하루 및 주중의 특정 시간을 정의합니다. 그런 다음 **access-list extended time-range** 명령을 사용하여 시간 범위를 ACL에 바인딩합니다.

시간 범위는 ASA의 시스템 클럭을 기반으로 합니다. 그러나 이 기능은 NTP 동기화에서 가장 효과적으로 작동합니다.

예

다음 예에서는 "New_York_Minute" 이라는 시간 범위를 만들고 시간 범위 구성 모드를 시작합니다.

```
ciscoasa(config)# time-range New_York_Minute
ciscoasa(config-time-range)#
```

시간 범위를 만들고 time-range 구성 모드를 시작한 후에는 **absolute** 및 **periodic** 명령을 사용하여 시간 범위 파라미터를 정의할 수 있습니다. **time-range** 명령의 **absolute** 및 **periodic** 키워드에 대한 기본 설정을 복원하려면 time-range 구성 모드에서 **default** 명령을 사용합니다.

시간 기반 ACL을 구현하려면 **time-range** 명령을 사용하여 하루 및 주중의 특정 시간을 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
ciscoasa(config)#
```

ACL에 대한 자세한 내용은 **access-list extended** 명령을 참고하십시오.

관련 명령

Command(명령)	설명
absolute	시간 범위가 적용되는 절대 시간을 정의합니다.
access-list extended	ASA를 통해 IP 트래픽을 허용하거나 거부하는 정책을 구성합니다.
default	**time-range** 명령의 **absolute** 및 **periodic** 키워드에 대한 기본 설정을 복원합니다.
periodic	time-range 기능을 지원하는 기능에 대한 되풀이(매주) 시간 범위를 지정합니다.

timers bgp

BGP 네트워크 타이머를 조정하려면 router bgp구성 모드에서 **timers bgp** 명령을 사용합니다. BGP 타이밍 기본값을 재설정하려면 이 명령의 **no** 형식을 사용합니다.

timers bgp *keepalive holdtime* [*min-holdtime*]

no timers bgp *keepalive holdtime* [*min-holdtime*]

구문 설명

keepalive	Cisco IOS 소프트웨어가 해당 피어로 *keepalive* 메시지를 보내는 빈도(초)입니다. 기본값은 60초입니다. 범위는 0~65535입니다.
holdtime	소프트웨어가 *keepalive* 메시지를 받지 못한 후 피어를 정지된 것으로 선언할 때까지의 간격(초)입니다. 기본값은 180초입니다. 범위는 0~65535입니다.
min-holdtime	(선택 사항) BGP 네이버에서 허용되는 최소 보류 시간을 지정하는 간격(초)입니다. 허용되는 최소 보류 시간은 *holdtime* 인수에 지정된 간격보다 작거나 같아야 합니다. 범위는 0~65535입니다.

기본값

keepalive: 60초
holdtime: 180초

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
router bgp 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
9.2(1)	이 명령이 추가되었습니다.

사용 지침

holdtime 인수 값을 20초 미만으로 구성하면 다음 경고가 표시됩니다. A hold time of less than 20 seconds increases the chances of peer flapping

허용되는 최소 보류 시간이 지정된 보류 시간보다 큰 경우 다음 알림이 표시됩니다. Minimum acceptable hold time should be less than or equal to the configured hold time

참고 허용되는 최소 보류 시간이 BGP 라우터에 구성된 경우 원격 BGP 피어 세션은 원격 피어가 허용되는 최소 보류 시간 간격보다 크거나 같은 보류 시간을 전달하는 경우에만 설정됩니다. 허용되는 최소 보류 시간이 구성된 보류 시간보다 큰 경우에는 다음에 원격 세션을 설정하려고 할 때 설정에 실패하고 로컬 라우터가 "unacceptable hold time" 이라는 알림을 보냅니다.

예

다음 예에서는 keepalive 타이머를 70초로 변경하고 hold-time 타이머를 130초로 변경하며, 허용되는 최소 보류 시간 간격을 100초로 변경합니다.

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# timers bgp 70 130 100
```

timers lsa arrival

ASA가 OSPFv3 네이버의 동일한 LSA를 허용하는 최소 간격을 설정하려면 IPv6 라우터 구성 모드에서 **timers lsa arrival** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timers lsa arrival *milliseconds*

no timers lsa arrival *milliseconds*

구문 설명

milliseconds	네이버에서 수신되는 동일한 LSA를 허용하기 위해 경과해야 하는 최소 지연 시간(밀리초)을 지정합니다. 유효한 값은 0~600,000밀리초입니다.

기본값

기본값은 1000밀리초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
IPv6 라우터 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하여 네이버에서 수신되는 동일한 LSA를 허용하기 위해 경과해야 하는 최소 간격을 나타낼 수 있습니다.

예

다음 예에서는 동일한 LSA를 허용하기 위한 최소 간격을 2000밀리초로 설정합니다.

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# timers lsa arrival 2000
```

관련 명령

Command(명령)	설명
ipv6 router ospf	OSPFv3에 대한 라우터 구성 모드를 시작합니다.
show ipv6 ospf	OSPFv3 라우팅 프로세스에 대한 일반 정보를 표시합니다.
timers pacing flood	OSPFv3 라우팅 프로세스에 대한 LSA 플러드 패킷 속도 조절을 구성합니다.

timers lsa-group-pacing

OSPF LSA(링크 상태 알림)를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격을 지정하려면 라우터 구성 모드에서 **timers lsa-group-pacing** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing [*seconds*]

구문 설명

seconds	OSPF LSA(링크 상태 알림)를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격입니다. 유효한 값은 10~1800초입니다.

기본값

기본 간격은 240초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
라우터 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

OSPF LSA(링크 상태 알림)를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격을 변경하려면 라우터 구성 모드에서 **timers lsa-group-pacing** *seconds* 명령을 사용합니다. 기본 타이머 값으로 되돌리려면 **no timers lsa-group-pacing** 명령을 사용합니다.

예

다음 예에서는 LSA의 그룹 처리 간격을 500초로 설정합니다.

```
ciscoasa(config-rtr)# timers lsa-group-pacing 500
ciscoasa(config-rtr)#
```

관련 명령

Command(명령)	설명
router ospf	라우터 컨피그레이션 모드를 시작합니다.
show ospf	OSPF 라우팅 프로세스에 대한 일반 정보를 표시합니다.
timers spf	SPF(최단 경로 우선) 계산 지연 및 보류 시간을 지정합니다.

timers pacing flood

LSA 플러드 패킷 속도 조절을 구성하려면 IPv6 라우터 구성 모드에서 **timers pacing flood** 명령을 사용합니다. 기본 플러드 패킷 속도 조절 값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timers pacing flood *milliseconds*

no timers pacing flood *milliseconds*

구문 설명

milliseconds	플러딩 대기열의 LSA가 업데이트 간격 사이에서 속도 조절되는 시간(밀리초)을 지정합니다. 컨피그레이션 가능한 범위는 5밀리초 ~ 100밀리초입니다.

기본값

기본값은 33밀리초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
IPv6 라우터 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하여 LSA 플러드 패킷 속도 조절을 구성할 수 있습니다.

예

다음 예에서는 LSA 플러드 패킷 속도 조절 업데이트가 OSPFv3에 대해 20밀리초 간격으로 발생하도록 구성합니다.

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

관련 명령

Command(명령)	설명
ipv6 router ospf	IPv6 라우터 구성 모드를 시작합니다.
timers pacing lsa-group	OSPFv3 LSA(링크 상태 알림)를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격을 지정합니다.

timers pacing lsa-group

OSPFv3 LSA(링크 상태 알림)를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격을 지정하려면 IPv6 라우터 구성 모드에서 **timers lsa-group-pacing** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timers pacing lsa-group *seconds*

no timers pacing lsa-group [*seconds*]

구문 설명

seconds	LSA를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격(초)을 지정합니다. 유효한 값은 10~1800초입니다.

기본값

기본 간격은 240초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
IPv6 라우터 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하여 OSPFv3 LSA를 그룹으로 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격을 나타낼 수 있습니다.

예

다음 예에서는 LSA 그룹 간의 OSPFv3 그룹 패킷 속도 조절 업데이트가 OSPFv3 라우팅 프로세스 1에 대해 300초 간격으로 발생하도록 설정합니다.

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

관련 명령

Command(명령)	설명
ipv6 router ospf	IPv6 라우터 컨피그레이션 모드를 시작합니다.
show ipv6 ospf	OSPFv3 라우팅 프로세스에 대한 일반 정보를 표시합니다.
timers pacing flood	OSPFv3 라우팅 프로세스에 대한 LSA 플러드 패킷 속도 조절을 구성합니다.
timers pacing retransmission	LSA 재전송 패킷 속도 조절을 구성합니다.

timers pacing retransmission

LSA(링크 상태 알림) 재전송 패킷 속도 조절을 구성하려면 라우터 구성 모드에서 **timers pacing retransmission** 명령을 사용합니다. 기본 재전송 패킷 속도 조절 값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timers pacing retransmission *milliseconds*

no timers pacing retransmission

구문 설명

milliseconds	재전송 대기열의 LSA가 속도 조절되는 시간 간격(밀리초)을 지정합니다. 유효한 값은 5~200밀리초입니다.

기본값

기본 간격은 66밀리초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
IPv6 라우터 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.2(1)	이 명령이 추가되었습니다.

사용 지침

OSPF(Open Shortest Path First: 최단 경로 우선 프로토콜) 재전송 속도 조절 타이머를 구성하면 OSPF 재전송 대기열에 있는 연속된 링크 상태 업데이트 패킷 간의 간격을 제어할 수 있습니다. 이 명령을 통해 LSA 업데이트가 발생하는 속도를 제어하여 많은 LSA로 인해 영역이 플러딩될 때 발생할 수 있는 높은 CPU 또는 버퍼 사용률을 줄일 수 있습니다. OSPF 패킷 재전송 속도 조절 타이머의 기본 설정은 대부분의 OSPF 배포에 적합합니다.

참고 OSPF 패킷 플러딩 요구 사항을 충족하는 다른 옵션을 모두 사용하지 않은 한 패킷 재전송 속도 조절 타이머를 변경하지 마십시오. 특히, 네트워크 사업자는 기본 플러딩 타이머를 변경하기 전에 요약, 스텁 영역 사용, 대기열 조정 및 버퍼 조정을 먼저 수행해야 합니다.

또한 타이머 값 변경에 대한 지침은 없습니다. 각 OSPF 배포는 고유하며, 사례별로 고려해야 합니다. 네트워크 운영자는 기본 패킷 재전송 속도 조절 타이머 값을 변경할 경우의 위험을 가정합니다.

예

다음 예에서는 LSA 플러드 속도 조절 업데이트가 OSPF 라우팅 프로세스 1에 대해 55밀리초 간격으로 발생하도록 구성합니다.

```
hostname(config)# router ospf 1
hostname(config-router)# timers pacing retransmission 55
```

관련 명령

Command(명령)	설명
ipv6 router ospf	IPv6 라우터 컨피그레이션 모드를 시작합니다.
show ipv6 ospf	OSPFv3 라우팅 프로세스에 대한 일반 정보를 표시합니다.
timers pacing flood	OSPFv3 라우팅 프로세스에 대한 LSA 플러드 패킷 속도 조절을 구성합니다.

timers spf

SPF(최단 경로 우선) 계산 지연 및 보류 시간을 지정하려면 라우터 구성 모드에서 **timers spf** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

구문 설명

delay	OSPF가 토폴로지 변경 사항을 받은 때부터 SPF(최단 경로 우선) 계산을 시작할 때까지의 지연 시간(1~65535초)을 지정합니다.
holdtime	연속된 두 SPF 계산 사이의 보류 시간(초)입니다. 유효한 값은 1~65535입니다.

기본값

기본값은 다음과 같습니다.

- *delay*는 5초입니다.
- *holdtime*은 10초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
라우터 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

OSPF 프로토콜이 토폴로지 변경 사항을 받은 때부터 계산을 시작할 때까지의 지연 시간 및 연속된 두 SPF 계산 사이의 보류 시간을 구성하려면 **timers spf** 명령을 사용합니다. 기본 타이머 값으로 되돌리려면 **no timers spf** 명령을 사용합니다.

예

다음 예에서는 SPF 계산 지연을 10초로 설정하고, SPF 계산 보류 시간을 20초로 설정합니다.

```
ciscoasa(config-router)# timers spf 10 20
ciscoasa(config-router)#
```

관련 명령

Command(명령)	설명
router ospf	라우터 구성 모드를 시작합니다.
show ospf	OSPF 라우팅 프로세스에 대한 일반 정보를 표시합니다.
timers lsa-group-pacing	OSPF LSA(링크 상태 알림)를 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격을 지정합니다.

타이머 스로틀

OSPF(Open Shortest Path First: 최단 경로 우선 프로토콜) LSA(링크 상태 알림) 생성 또는 SPF 생성에 대한 속도 제한 값을 설정하려면 router ospf 또는 ipv6 router ospf 구성 모드에서 **timers throttle** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

timers throttle {**lsa | spf**} *start-interval hold-interval max-interval*

no timers throttle {**lsa | spf**}

구문 설명

lsa	LSA 제한을 구성합니다.
start-interval	LSA의 첫 번째 발생을 생성할 지연 시간(밀리초)을 지정합니다. SPF 계산에 변경 사항을 수신할 지연 시간(밀리초)을 지정합니다. LSA의 첫 번째 발생을 생성할 최소 지연 시간(밀리초)을 지정합니다. **참고** LSA의 첫 번째 인스턴스는 로컬 OSPF 토폴로지가 변경된 즉시 생성됩니다. 다음 LSA는 *start-interval* 이후에만 생성됩니다. 유효한 값은 0~600,000밀리초입니다. 기본값은 0밀리초입니다. LSA가 즉시 전송됩니다.
hold-interval	동일한 LSA를 시작할 최대 지연 시간(밀리초)을 지정합니다. 첫 번째와 두 번째 SPF 계산 사이의 지연 시간(밀리초)을 지정합니다. LSA를 다시 생성할 최소 지연 시간(밀리초)을 지정합니다. 이 값은 LSA 생성에 대한 이후의 속도 제한 값을 계산하는 데 사용됩니다. 유효한 값은 1~600,000밀리초입니다. 기본값은 5000밀리초입니다.
max-interval	동일한 LSA를 시작할 최소 지연 시간(밀리초)을 지정합니다. SPF 계산에 대한 최대 대기 시간(밀리초)을 지정합니다. LSA를 다시 생성할 최대 지연 시간(밀리초)을 지정합니다. 유효한 값은 1~600,000밀리초입니다. 기본값은 5000밀리초입니다.
spf	SPF 제한을 구성합니다.

기본값

LSA 제한:

- *start-interval*의 경우 기본값은 0밀리초입니다.
- *hold-interval*의 경우 기본값은 5000밀리초입니다.
- *max-interval*의 경우 기본값은 5000밀리초입니다.

SPF 제한:

- *start-interval*의 경우 기본값은 5000밀리초입니다.
- *hold-interval*의 경우 기본값은 10000밀리초입니다.
- *max-interval*의 경우 기본값은 10000밀리초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
ipv6 router ospf 구성	• 예	—	• 예	• 예	—
router ospf 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
9.0(1)	이 명령이 추가되었습니다.
9.2(1)	IPv6에 대한 지원이 추가되었습니다.

사용 지침

LSA 및 SPF 제한은 네트워크가 불안정한 동안 OSPF에서 LSA 업데이트 속도를 늦추는 동적 메커니즘을 제공하며, LSA 속도 제한(밀리초)을 제공하여 OSPF를 보다 빠르게 통합할 수 있도록 합니다.

LSA 제한의 경우 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPF가 첫 번째 어커런스 값으로 자동으로 수정됩니다. 마찬가지로 지정된 최대 지연 시간이 최소 지연 시간보다 작으면 OSPF가 최소 지연 시간 값으로 자동으로 수정됩니다.

SPF 제한의 경우 *hold-interval* 또는 *max-interval*이 *start-interval*보다 작은 경우 OSPF는 *start-interval* 값을 자동으로 수정합니다. 마찬가지로, *max-interval*이 *hold-interval*보다 작은 경우 OSPF는 *hold-interval* 값을 자동으로 수정합니다.

예

다음 예에서는 OSPFv3 LSA 제한(밀리초)을 구성합니다.

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 4000 5000
```

LSA 제한의 경우 다음 예에서는 지정된 최대 지연 시간 값이 최소 지연 시간 값보다 작은 경우에 발생하는 자동 수정을 보여 줍니다.

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6
ipv6 router ospf 10
 timers throttle lsa 100 100 100
```

다음 예에서는 OSPFv3 SPF 제한(밀리초)을 구성합니다.

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

SPF 제한의 경우 다음 예에서는 지정된 최대 지연 시간 값이 최소 지연 시간 값보다 작은 경우에 발생하는 자동 수정을 보여 줍니다.

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6
ipv6 router ospf 10
 timers throttle spf 100 100 100
```

관련 명령

Command(명령)	설명
ipv6 router ospf	IPv6 라우터 컨피그레이션 모드를 시작합니다.
show ipv6 ospf	OSPFv3 라우팅 프로세스에 대한 일반 정보를 표시합니다.
timers lsa-group-pacing	OSPFv3 LSA(링크 상태 알림)를 수집하고 새로 고치거나, 체크섬하거나, 기간 경과로 설정할 간격을 지정합니다.

timestamp

IP 옵션 검사를 통해 패킷 헤더에서 TS(Time Stamp) 옵션이 발생하는 경우 작업을 정의하려면 파라미터 구성 모드에서 **timestamp** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

timestamp action {allow | clear}

no timestamp action {allow | clear}

구문 설명

허용	타임스탬프 IP 옵션을 포함하는 패킷을 허용합니다.
clear	패킷 헤더에서 Time Stamp(타임스탬프) 옵션을 제거한 다음 해당 패킷을 허용합니다.

기본값

기본적으로 IP 옵션 검사에서는 타임스탬프 IP 옵션을 포함하는 패킷을 삭제합니다.

IP Options 검사 정책 맵에서 **default** 명령을 사용하여 기본값을 변경할 수 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.5(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 IP 옵션 검사 정책 맵에서 구성할 수 있습니다.

ASA를 통과하도록 허용할 특정 IP 옵션의 IP 패킷을 제어하려면 IP 옵션 검사를 구성할 수 있습니다. 지정된 IP 옵션을 변경하거나 삭제한 다음 패킷이 통과하도록 허용하지 않고도 패킷이 통과하도록 허용할 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)# timestamp action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

관련 명령

Command(명령)	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	Layer 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

title

WebVPN 사용자가 보안 어플라이언스에 연결할 때 표시되는 WebVPN 페이지의 제목을 사용자 지정하려면 webvpn customization 모드에서 **title** 명령을 사용합니다.

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

구성에서 명령을 제거하고 값을 상속받도록 하려면 **no** 형식의 다음 명령을 사용합니다.

구문 설명

text	텍스트를 변경하도록 지정합니다.
style	스타일을 변경하도록 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자)입니다.

기본값

기본 제목 텍스트는 "WebVPN Service" 입니다.

기본 제목 스타일은 다음과 같습니다.

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger; vertical-align:middle;text-align:left;font-weight:bold

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
webvpn customization	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.

사용 지침

제목을 없애려면 *value* 인수 없이 **title text** 명령을 사용합니다.

style 옵션은 유효한 모든 CSS(Cascading Style Sheet) 매개변수로 표현됩니다. 이러한 매개변수에 대한 설명은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트(www.w3.org)에서 CSS 사양을 참고하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수 목록이 포함되어 있습니다.

다음은 WebVPN 페이지에서 수행할 수 있는 가장 일반적인 변경(페이지 색상 변경) 작업에 대한 몇 가지 팁입니다.

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

참고 WebVPN 페이지를 쉽게 사용자 지정하려면 색상 견본 및 미리보기 기능 등 스타일 요소 컨피그레이션에 대한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예에서는 "Cisco WebVPN Service" 라는 텍스트로 제목을 맞춤 설정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# title text Cisco WebVPN Service
```

관련 명령

Command(명령)	설명
logo	WebVPN 페이지의 로고를 맞춤 설정합니다.
page style	CSS(Cascading Style Sheet) 파라미터를 사용하여 WebVPN 페이지를 맞춤 설정합니다.

tls-proxy through type echo 명령

tls-proxy

TLS 구성 모드에서 TLS 프록시 인스턴스를 구성하거나 최대 세션을 설정하려면 전역 구성 모드에서 **tls-proxy** 명령을 사용합니다. 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

구문 설명

max_sessions *max_sessions*	플랫폼에서 지원할 최대 TLS 프록시 세션 수를 지정합니다.
noconfirm	확인 없이 **tls-proxy** 명령을 실행합니다.
proxy_name	TLS 프록시 인스턴스의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

TLS 프록시 구성 모드를 시작하여 TLS 프록시 인스턴스를 생성하거나 플랫폼에서 지원되는 최대 세션을 설정하려면 **tls-proxy** 명령을 사용합니다.

예

다음 예에서는 TLS 프록시 인스턴스를 생성하는 방법을 보여 줍니다.

```
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
client	암호 그룹을 정의하고 로컬 동적 인증서 발급자 또는 키 쌍을 설정합니다.
ctl-provider	CTL 공급자 인스턴스를 정의하고 공급자 구성 모드를 시작합니다.
server trust-point	TLS 핸드셰이크 중에 제공할 프록시 트러스트 포인트 인증서를 지정합니다.
show tls-proxy	TLS 프록시를 표시합니다.

토큰

Cisco Umbrella에 등록하는 데 필요한 API 토큰을 구성하려면 Umbrella 구성 모드에서 **token** 명령을 사용합니다. 토큰을 제거하려면 이 명령의 **no** 형식을 사용합니다.

token *api_token*

no token *api_token*

구문 설명

api_token	Cisco Umbrella에 등록하는 데 필요한 API 토큰입니다. Cisco Umbrella 네트워크 디바이스 대시보드(https://login.umbrella.com/)에서 토큰을 가져와야 합니다. 토큰은 16 진수 문자열(예: AABBA59A0BDE1485C912AFE)이 됩니다.

기본값

기본 API 토큰이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
Umbrella 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.10(1)	이 명령이 추가되었습니다.

사용 지침

Cisco Umbrella에 디바이스를 올바르게 등록하려면 API 토큰을 구성해야 합니다. 토큰은 고객별로 고유하지만 디바이스 별로는 고유하지 않습니다.

등록은 독립형 디바이스, 클러스터 또는 장애 조치 그룹에 대한 것입니다. 클러스터 또는 장애 조치 그룹 내의 각 디바이스를 개별적으로 등록하지 마십시오. 다중 컨텍스트 모드에서 각 컨텍스트는 독립형이든 클러스터 또는 장애 조치 그룹 내에 있든 관계없이 디바이스입니다.

예

다음 예에서는 Cisco Umbrella 등록을 위해 API 토큰을 구성합니다.

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

관련 명령

명령	설명
public-key	Cisco Umbrella에서 사용되는 공개 키를 구성합니다.
timeout edns	서버에서 응답이 없는 경우 클라이언트에서 Umbrella 서버로의 연결을 제거하기 전의 유휴 시간 제한을 구성합니다.
umbrella-global	Cisco Umbrella 전역 파라미터를 구성합니다.

tos

SLA 작업 요청 패킷의 IP 헤더에서 서비스 바이트의 유형을 정의하려면 SLA 모니터 프로토콜 구성 모드에서 **tos** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

tos *number*

no tos

구문 설명

number	IP 헤더에서 사용할 서비스 유형 값입니다. 유효한 값은 0 ~ 255입니다.

기본값

기본 서비스 유형 값은 0입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
SLA 모니터 프로토콜 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 필드에는 지연, 우선 순위, 신뢰성 등의 정보가 포함됩니다. 네트워크의 다른 라우터가 정책 라우팅 및 기능(예: Committed Access Rate)에 이를 사용할 수 있습니다.

예

다음 예에서는 ICMP 에코 요청/응답 시간 프로브 작업을 사용하는 ID가 123인 SLA 작업을 구성합니다. 에코 요청 패킷의 페이로드 크기를 48바이트로 설정하고, SLA 작업 중에 전송되는 에코 요청 수를 5로 설정하며, 서비스 바이트 유형을 80으로 설정합니다.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# tos 80
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

Command(명령)	설명
num-packets	SLA 작업 중에 전송할 요청 패킷 수를 지정합니다.
request-data-size	요청 패킷 페이로드의 크기를 지정합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.
type echo	SLA 작업을 에코 응답 시간 프로브 작업으로 구성합니다.

traceroute

패킷이 대상에 도달하는 경로를 확인하려면 **traceroute** 명령을 사용합니다.

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

구문 설명

destination_ip	traceroute의 대상 IP 주소를 지정합니다. IPv4 및 IPv6 주소를 모두 지원합니다.
hostname	경로를 추적해야 하는 호스트의 호스트 이름입니다. 호스트 대상은 IPv4 또는 IPv6 주소일 수 있습니다. 호스트 이름을 지정하는 경우 **name** 명령으로 정의하거나 traceroute를 사용하여 호스트 이름을 IP 주소로 확인하도록 DNS 서버를 구성합니다. www.example.com과 같은 DNS 도메인 이름을 지원합니다.
max-ttl	사용할 수 있는 최대 TTL 값입니다. 기본값은 30입니다. 이 명령은 traceroute 패킷이 대상에 도달하거나 값에 도달한 경우 종료됩니다.
min_ttl	첫 번째 프로브의 TTL 값입니다. 기본값은 1이지만 더 높은 값으로 설정하여 알려진 홉 표시를 무시할 수 있습니다.
numeric	중간 게이트웨이의 IP 주소만 인쇄하도록 출력을 지정합니다. 이 키워드를 지정하지 않으면 traceroute에서 추적 중에 도달한 게이트웨이의 호스트 이름을 조회하려고 시도합니다.
port *port_value*	UDP(사용자 데이터그램 프로토콜) 프로브 메시지에서 사용하는 대상 포트입니다. 기본값은 33434입니다.
probe *probe_num*	각 TTL 수준에서 전송할 프로브 수입니다. 기본 count는 3입니다.
source	추적 패킷의 소스로 사용되는 IP 주소 또는 인터페이스를 지정합니다. IPv6은 IPv6 소스 주소만 허용합니다.
source_interface	패킷 추적의 소스 인터페이스를 지정합니다. 지정하면 소스 인터페이스의 IP 주소가 사용됩니다.
source_ip	패킷 추적의 소스 IP 주소를 지정합니다. 이 IP 주소는 인터페이스 중 하나의 IP 주소여야 합니다. 투명 모드에서는 ASA의 관리 IP 주소여야 합니다.
timeout	시간 초과 값을 사용하도록 지정합니다.
timeout_value	연결 시간이 초과되기 전에 응답을 대기할 기간(초)을 지정합니다. 기본값은 3초입니다.
ttl	프로브에서 사용할 TTL 값의 범위를 지정하는 키워드입니다.
use-icmp	UDP 프로브 패킷 대신 ICMP 프로브 패킷을 사용하도록 지정합니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.
9.7.(1)	이 명령은 IPv6 주소를 허용하도록 업데이트되었습니다.

사용 지침

traceroute 명령은 전송된 각 프로브의 결과를 인쇄합니다. 출력 화면의 각 줄은 TTL 값에 해당합니다(오름차순). 다음은 **traceroute** 명령에서 인쇄되는 출력 기호입니다.

출력 기호	설명
*	프로브에 대한 응답을 받지 못한 채 시간이 초과되었습니다.
U	대상에 대한 경로가 없습니다.
nn msec	각 노드에서 지정된 수의 프로브가 왕복하는 데 걸린 시간(밀리초)입니다.
!N.	연결 불가한 ICMP 네트워크입니다. ICMPv6에 대한 주소 범위를 벗어났습니다.
!H	연결 불가한 ICMP 호스트입니다.
!P	ICMP 프로토콜에 연결할 수 없습니다. ICMPv6에 포트를 연결할 수 없습니다.
!A	관리자가 ICMP를 금지했습니다.
?	알 수 없는 ICMP 오류입니다.

예

다음 예에서는 대상 IP 주소가 지정된 경우 traceroute의 출력 결과를 보여 줍니다.

```
ciscoasa# traceroute 209.165.200.225

Tracing the route to 209.165.200.225

 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec

ciscoasa/admin(config)# traceroute 2002::130
Type escape sequence to abort.
Tracing the route to 2002::130
 1  5000::2 0 msec 0 msec 0 msec
 2  2002::130 10 msec 0 msec 0 msec
```

관련 명령

Command(명령)	설명
capture	추적 패킷을 포함하여 패킷 정보를 캡처합니다.
show capture	옵션을 지정하지 않은 경우의 캡처 구성을 표시합니다.
packet-tracer	패킷 추적 기능을 활성화합니다.

track rtr

SLA 작업의 연결성을 추적하려면 전역 구성 모드에서 **track rtr** 명령을 사용합니다. SLA 추적을 제거하려면 이 명령의 **no** 형식을 사용합니다.

track *track-id* **rtr** *sla-id* **reachability**

no track *track-id* **rtr** *sla-id* **reachability**

구문 설명

연결성	개체의 연결성을 추적하도록 지정합니다.
sla-id	추적 항목에서 사용되는 SLA의 ID입니다.
track-id	추적 항목 개체 ID를 생성합니다. 유효한 값은 1 ~ 500입니다.

기본값

SLA 추적은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		**보안 상황**		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	**수정 사항**
7.2(1)	이 명령이 추가되었습니다.

사용 지침

track rtr 명령은 추적 항목 개체 ID를 만들고 해당 추적 항목에서 사용하는 SLA를 지정합니다.

각 SLA 작업은 추적 프로세스에서 해석되는 작업 반환 코드 값을 유지 관리합니다. 반환 코드는 OK, Over Threshold 또는 기타 여러 반환 코드일 수 있습니다. 표 2-1 에는 이러한 반환 코드에 대한 개체의 연결성 상태가 나와 있습니다.

표 2-1 SLA 추적 반환 코드

Tracking	**반환 코드**	**추적 상태**
연결 가능성	OK 또는 Over Threshold	Up(위로)
	다른 코드	중단

예

다음 예에서는 ID 123을 사용하여 SLA 작업을 구성하고 ID가 1인 추적 작업을 생성하여 SLA 연결성을 추적합니다.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
```

```
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

Command(명령)	설명
route	고정 경로를 구성합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.

traffic-forward

모듈에 트래픽을 직접 전달하고 액세스 제어 및 기타 처리를 우회하려면 인터페이스 구성 모드에서 **traffic-forward** 명령을 사용합니다. 트래픽 전달을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

traffic-forward *module_type* **monitor-only**

no traffic-forward *module_type* **monitor-only**

구문 설명

module_type	모듈의 유형입니다. 지원되는 모듈은 다음과 같습니다. • **sfr** - ASA FirePOWER 모듈 • **cxsc** - ASA CX 모듈
monitor-only	모듈을 모니터 전용 모드로 설정합니다. 모니터링 전용 모드에서 모듈은 트래픽을 처리한 다음 트래픽을 삭제할 수 있습니다. 사용법은 모듈 유형에 따라 다릅니다. • ASA FirePOWER - 패시브 모드를 구성하려면 이 명령을 사용합니다. 프로덕션 목적으로 이 모드를 사용할 수 있습니다. • ASA CX - 이는 엄격히 데모 모드입니다. 트래픽 전달 인터페이스 또는 장치를 프로덕션에 사용할 수 없습니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
인터페이스 구성	—	• 예	• 예	—	—

명령 기록

Release	수정 사항
9.1(2)	이 명령이 추가되었습니다.
9.2(1)	**sfr** 키워드가 추가되었습니다.
9.3(2)	**sfr** 키워드와 함께 프로덕션 사용에 대한 지원이 추가되었습니다.

사용 지침

이 명령은 서비스 정책 **sfr** 또는 **cxsc** 명령을 **monitor-only** 키워드와 함께 사용하여 트래픽을 모듈로 리디렉션하는 대신 사용할 수 있습니다. 서비스 정책을 사용하는 경우 트래픽은 계속해서 ASA 처리를 수행하며 이를 통해 액세스 규칙 및 TCP 정규화 등의 트래픽을 삭제할 수 있습니다. 또한, ASA는 단순히 트래픽의 복사본을 모듈에 전송하고 궁극적으로는 자체 정책에 따라 트래픽을 전송합니다.

반면 **traffic-forward** 명령은 ASA 처리를 완전히 우회하여 단순히 모듈에 트래픽을 전달합니다. 그런 다음 모듈에서 트래픽을 검사하고, 정책을 결정하고, 이벤트를 생성하여 인라인 모드에서 작동한 경우 트래픽에 수행된 작업을 보여 줍니다. 모듈이 트래픽 사본에서 작동하지만 ASA는 ASA 또는 모듈의 정책 결정에 상관없이 트래픽을 즉시 삭제합니다. 모듈은 블랙홀 역할을 합니다.

네트워크의 스위치에 있는 SPAN 포트에 트래픽 전달 인터페이스를 연결합니다.

트래픽 전달 인터페이스 구성에는 다음과 같은 제한 사항이 있습니다.

- ASA에서 모니터링 전용 모드와 일반 인라인 모드를 동시에 구성할 수는 없습니다. 한 가지 유형의 보안 정책만 허용됩니다.
- ASA는 단일 컨텍스트 모드여야 합니다.
- 트래픽 전달 인터페이스는 VLAN 또는 BVI가 아니라 물리적 인터페이스입니다. 물리적 인터페이스에는 VLAN을 연결할 수 없습니다.
- 트래픽 전달 인터페이스는 ASA 트래픽에 사용할 수 없습니다. 인터페이스 이름을 지정하거나 장애 조치 또는 관리 전용을 포함하여 ASA 기능에 대해 구성할 수 없습니다.

예

다음 예에서는 GigabitEthernet 0/5를 트래픽 전용 인터페이스로 만듭니다.

```
interface gigabitethernet 0/5
 no nameif
 traffic-forward sfr monitor-only
 no shutdown
```

관련 명령

Command(명령)	설명
interface	인터페이스 구성 모드를 시작합니다.
cxsc	ASA CX 모듈로 트래픽을 리디렉션하는 서비스 정책 명령입니다.
sfr	ASA FirePOWER 모듈로 트래픽을 리디렉션하는 서비스 정책 명령입니다.

traffic-non-sip

잘 알려진 SIP 신호 처리 포트를 사용하여 비 SIP 트래픽을 허용하려면 파라미터 구성 모드에서 **traffic-non-sip** 명령을 사용합니다. 파라미터 구성 모드는 정책 맵 구성 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

traffic-non-sip

no traffic-non-sip

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령은 기본적으로 사용됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

예

다음 예에서는 SIP 검사 정책 맵에서 잘 알려진 SIP 신호 처리 포트를 사용하여 비 SIP 트래픽을 허용하는 방법을 보여 줍니다.

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

관련 명령

Command(명령)	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	Layer 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

transfer-encoding

전송 인코딩 유형을 지정하여 HTTP 트래픽을 제한하려면 HTTP 맵 구성 모드에서 **transfer-encoding** 명령을 사용합니다. 이 모드는 **http-map** 명령을 사용하여 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

구문 설명

action	지정된 전송 인코딩 유형을 사용하는 연결이 탐지된 경우 수행할 작업을 지정합니다.
allow	메시지를 허용합니다.
chunked	메시지 본문이 일련의 청크로 전송되는 전송 인코딩 유형을 식별합니다.
compress	메시지 본문이 UNIX 파일 압축을 사용하여 전송되는 전송 인코딩 유형을 식별합니다.
default	트래픽에 구성된 목록에 없는 지원되는 요청 방법이 포함된 경우 ASA에서 수행하는 기본 작업을 지정합니다.
deflate	메시지 본문이 zlib 형식(RFC 1950) 및 수축 압축(RFC 1951)을 사용하여 전송되는 전송 인코딩 유형을 식별합니다.
drop	연결을 닫습니다.
gzip	메시지 본문이 GNU zip(RFC 1952)을 사용하여 전송되는 전송 인코딩 유형을 식별합니다.
ID	메시지 본문에서 전송 인코딩이 수행되지 않는 연결을 식별합니다.
log	(선택 사항) 시스템 로그를 생성합니다.
reset	TCP 재설정 메시지를 클라이언트 및 서버로 전송합니다.
type	HTTP 애플리케이션 검사를 통해 제어할 전송 인코딩 유형을 지정합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다. 이 명령을 활성화하고 지원되는 전송 인코딩 유형을 지정하지 않은 경우 기본 동작은 기록 없이 연결을 허용하는 것입니다. 기본 동작을 변경하려면 **default** 키워드를 사용하고 다른 기본 동작을 지정합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
HTTP 맵 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

transfer-encoding 명령을 활성화한 경우 ASA는 각 지원 및 구성된 전송 인코딩 유형에 대한 HTTP 연결에 지정된 동작을 적용합니다.

ASA는 구성된 목록에 있는 전송 인코딩 유형과 일치하지 *않는* 모든 트래픽에 **default** 동작을 적용합니다. 사전 구성된 **default** 동작은 기록 없이 연결을 **allow**하는 것입니다.

예를 들어 미리 구성된 기본 동작이 있는 경우 **drop** 및 **log**를 사용하여 하나 이상의 인코딩 유형을 지정하면 ASA는 구성된 인코딩 유형이 포함된 연결을 삭제하고, 각 연결을 기록하며, 지원되는 다른 인코딩 유형에 대한 모든 연결을 허용합니다.

보다 엄격한 정책을 구성하려면 기본 동작을 **drop**(또는 **reset**) 및 **log**(이벤트를 기록하려는 경우)로 변경합니다. 그런 다음 **allow** 동작으로 허용되는 각 인코딩 유형을 구성합니다.

적용할 각 설정에 대해 **transfer-encoding** 명령을 한 번씩 입력합니다. **transfer-encoding** 명령의 인스턴스를 하나를 사용하여 기본 동작을 변경하고 또 하나의 인스턴스를 사용하여 각 인코딩 유형을 구성된 전송 인코딩 유형 목록에 추가합니다.

구성된 애플리케이션 유형 목록에서 애플리케이션 카테고리를 제거하기 위해 이 명령의 **no** 형식을 사용하는 경우 명령줄에서 애플리케이션 카테고리 키워드 뒤의 문자는 모두 무시됩니다.

예

다음 예에서는 특별히 금지되지 않은 지원되는 모든 애플리케이션 유형을 허용하는 사전 구성된 기본값으로 허용 정책을 제공합니다.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# transfer-encoding gzip drop log
ciscoasa(config-http-map)#
```

이 경우 GNU zip을 사용하는 연결만 삭제되고 이벤트가 기록됩니다.

다음 예에서는 연결을 재설정하고 특별히 허용되지 않은 인코딩 유형에 대한 이벤트를 기록하도록 기본 동작이 변경된 제한 정책을 제공합니다.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# port-misuse default action reset log
ciscoasa(config-http-map)# port-misuse identity allow
ciscoasa(config-http-map)#
```

이 경우 전송 인코딩을 사용하지 않는 연결만 허용됩니다. 지원되는 다른 인코딩 유형에 대한 HTTP 트래픽을 받은 경우 ASA는 연결을 재설정하고 시스템 로그 항목을 생성합니다.

관련 명령

명령	설명
class-map	보안 작업을 적용할 트래픽 클래스를 정의합니다.
debug appfw	고급 HTTP 검사와 관련된 트래픽에 대한 자세한 정보를 표시합니다.
http-map	고급 HTTP 검사를 구성하기 위한 HTTP 맵을 정의합니다.
inspect http	애플리케이션 검사에 사용할 특정 HTTP 맵을 적용합니다.
policy-map	클래스 맵을 특정 보안 작업과 연결합니다.

trustpoint (saml idp)

idp 인증 또는 sp 인증용 인증서를 포함하는 트러스트 포인트를 구성하려면 saml idp 구성 모드에서 **trustpoint** 명령을 사용합니다. 먼저 **webvpn** 명령을 입력하여 saml idp 구성 모드에 액세스할 수 있습니다. 트러스트 포인트를 제거하려면 이 명령의 **no** 형식을 사용합니다.

trustpoint {**idp** | **sp**} *trustpoint-name*

no trustpoint {**idp** | **sp**} *trustpoint-name*

구문 설명

trustpoint_name	사용할 트러스트 포인트의 이름을 지정합니다.
sp	이 트러스트 포인트는 IdP에서 ASA의 서명 또는 암호화된 SAML 어설션을 확인할 수 있는 ASA(SP)의 인증서를 포함하고 있습니다.
idp	이 트러스트 포인트는 ASA에서 SAML 어설션을 확인할 수 있는 IdP 인증서를 포함하고 있습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
Saml idp 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.5(2)	이 명령이 추가되었습니다.

사용 지침

트러스트 포인트는 검증 테스트 없이 유효한 것으로 간주될 수 있는 CA 발급 인증서, 특히 인증 경로에서 첫 번째 공개 키를 제공하는 데 사용되는 공개 키 인증서를 기반으로 하는 인증 기관 ID를 나타냅니다.

관련 명령

Command(명령)	설명
saml idp	서드파티 Idp에 대한 구성을 생성하며, SAML 속성을 구성할 수 있도록 saml Idp 모드로 전환합니다.

trustpoint (sso server)(사용되지 않음)

참고 마지막으로 이 명령을 지원하는 릴리스는 버전 9.3(1)이었습니다.

SAML POST 유형 SSO 서버로 전송할 인증서를 식별하는 트러스트 포인트의 이름을 지정하려면 sso server 모드에서 **trustpoint** 명령을 사용합니다. 트러스트 포인트 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

trustpoint *trustpoint-name*

no trustpoint *trustpoint-name*

구문 설명

trustpoint_name	사용할 트러스트 포인트의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
Config webvpn sso saml	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.
9.5(2)	이 명령은 SAML 2.0 지원으로 인해 사용이 중단되었습니다.

사용 지침

SSO(WebVPN에만 제공) 지원을 통해 사용자가 사용자 이름 및 비밀번호를 단 한 번만 입력하여 여러 서버에서 다양한 보안 서비스에 액세스할 수 있습니다. 현재 ASA는 SAML POST 유형의 SSO 서버 및 SiteMinder 유형의 SSO 서버를 지원합니다.

이 명령은 SAML 유형의 SSO 서버에만 적용됩니다.

트러스트 포인트는 검증 테스트 없이 유효한 것으로 간주될 수 있는 CA 발급 인증서, 특히 인증 경로에서 첫 번째 공개 키를 제공하는 데 사용되는 공개 키 인증서를 기반으로 하는 인증 기관 ID를 나타냅니다.

예

다음 예에서는 config-webvpn-sso-saml 모드를 시작하고 SAML POST 유형의 SSO 서버로 전송할 인증서를 식별하는 트러스트 포인트의 이름을 지정합니다.

```
ciscoasa(config-webvpn)# sso server
ciscoasa(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

관련 명령

Command(명령)	설명
crypto ca trustpoint	트러스트 포인트 정보를 관리합니다.
show webvpn sso server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
sso server	SSO 서버를 생성하고, 이름을 지정하고, 유형을 지정합니다.

trust-verification-server

HTTPS를 설정하는 동안 Cisco Unified IP Phone이 애플리케이션 서버를 인증할 수 있도록 해주는 Trust Verification Services 서버를 식별하려면 SIP 검사에 대한 파라미터 구성 모드에서 **trust-verification-server** 명령을 사용합니다. 파라미터 구성 모드는 정책 맵 구성 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

trust-verification-server {**ip** *address* | **port** *number*}

no trust-verification-server {**ip** *address* | **port** *number*}

구문 설명

ip *address*	Trust Verification Services 서버의 IP 주소를 지정합니다. SIP 검색 정책 맵에서 이 인수와 함께 명령을 최대 4번 입력할 수 있습니다. SIP 검사는 등록된 각 전화기에 대해 각 서버에 대한 핀홀을 열며, 전화기는 사용할 핀홀을 결정합니다. CUCM(Cisco Unified Communications Manager) 서버에서 Trust Verification Services 서버를 구성합니다.
port *number*	서버에서 사용하는 포트 번호를 지정합니다. 기본 포트 범위는 1026~32768입니다.

기본값

기본 포트는 2445입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.3(2)	이 명령이 추가되었습니다.

예

다음 예에서는 SIP 검사 정책 맵에서 4개의 Trust Verification Services 서버를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.1
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.2
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.3
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.4
ciscoasa(config-pmap-p)# trust-verification-server port 2445
```

관련 명령

Command(명령)	설명
policy-map type inspect	검사 정책 맵을 만듭니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

tsig enforced

TSIG 리소스 레코드를 제공하도록 요구하려면 파라미터 구성 모드에서 **tsig enforced** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

tsig enforced action {**drop** [**log**] | **log**}

no tsig enforced [**action** {**drop** [**log**] | **log**}]

구문 설명

drop	TSIG가 없는 경우 패킷을 삭제합니다.
log	시스템 메시지 로그를 생성합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 DNS 트랜잭션에서 TSIG 존재에 대한 모니터링 및 적용을 활성화합니다.

예

다음 예에서는 DNS 검사 정책 맵에서 TSIG 적용을 활성화하는 방법을 보여 줍니다.

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

관련 명령

Command(명령)	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	Layer 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

ttl-evasion-protection

TTL(Time-To-Live) 회피 방지를 활성화하려면 tcp-map 구성 모드에서 **ttl-evasion-protection** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

ttl-evasion-protection

no ttl-evasion-protection

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

TTL 회피 방지는 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
tcp-map 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용됩니다. **class-map** 명령을 사용하여 트래픽의 클래스를 정의하고, **tcp-map** 명령을 사용하여 TCP 검사를 맞춤 설정합니다. **policy-map** 명령을 사용하여 새 TCP 맵을 적용합니다. **service-policy** 명령을 사용하여 TCP 검사를 활성화합니다.

tcp-map 명령을 사용하여 tcp-map 구성 모드를 시작할 수 있습니다. tcp-map 구성 모드에서 **ttl-evasion-protection** 명령을 사용하여 보안 정책을 회피하려는 공격을 방지할 수 있습니다. TTL 회피 방지를 사용하는 경우 연결에 대한 최대 TTL은 초기 패킷의 TTL이 결정합니다. 후속 패킷에 대한 TTL은 줄일 수는 있지만 늘릴 수는 없습니다. 시스템은 TTL을 해당 연결에 대해 목격된 최저 TTL로 재설정합니다.

예를 들어 공격자는 TTL이 매우 짧은 정책을 전달하는 패킷을 전송할 수 있습니다. TTL이 0이 되면 ASA와 엔드포인트 사이의 라우터가 패킷을 삭제합니다. 이때 공격자는 ASA에 재전송으로 표시되어 전달되는 TTL이 긴 악성 패킷을 전송할 수 있습니다. 그러나 엔드포인트 호스트에는 이것이 공격자가 받은 첫 번째 패킷이 됩니다. 이 경우 공격자는 공격을 방지하는 보안 없이 성공할 수 있습니다. 이 기능을 활성화하면 이러한 공격이 방지됩니다.

예

다음 예에서는 네트워크 10.0.0.0에서 20.0.0.0으로의 흐름에 대해 TTL 회피 방지를 비활성화하는 방법을 보여 줍니다.

```
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)# no ttl-evasion-protection
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

Command(명령)	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 구성 모드에 대한 액세스를 허용합니다.

tunnel destination

VTI 터널 대상의 IP 주소를 지정하려면 인터페이스 구성 모드에서 **tunnel destination** 명령을 사용합니다. VTI 터널 대상의 IP 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel destination {*IP address* | *hostname*}

no tunnel destination {*IP address* | *hostname*}

구문 설명

IP address	VTI 터널 대상의 IP 주소(IPv4)를 지정합니다.
hostname	VTI 터널 대상의 호스트 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
interface 구성	• 예	• 아니요	• 예	• 아니요	—

명령 기록

Release	수정 사항
9.7(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 전역 구성 모드에서 **interface tunnel** 명령을 사용한 후에 인터페이스 구성 모드에서 사용할 수 있습니다.

예

다음 예에서는 VTI 터널 대상의 IP 주소를 지정합니다.

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel destination 10.2.2.3
```

관련 명령

Command(명령)	설명
interface tunnel	새 VTI 터널 인터페이스를 생성합니다.
tunnel source interface	VTI 터널을 생성하기 위한 소스 인터페이스를 지정합니다.
tunnel mode	IPsec이 터널 보호에 사용되도록 지정합니다.
tunnel protection ipsec	터널 보호에 사용할 IPsec 프로파일을 지정합니다.

터널 모드

VTI 터널에 대한 터널 보호 모드를 지정하려면 인터페이스 구성 모드에서 **tunnel mode** 명령을 사용합니다. VTI 터널 보호를 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel mode *ipsec IPv4*

no tunnel mode *ipsec IPv4*

구문 설명

ipsec	터널에서 터널 보호 표준으로 IPsec을 사용하도록 지정합니다.
IPv4	터널에서 IPv4를 통한 IPsec을 사용하도록 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
interface 구성	• 예	• 아니요	• 예	• 아니요	—

명령 기록

Release	수정 사항
9.7(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 전역 구성 모드에서 **interface tunnel** 명령을 사용한 후에 인터페이스 구성 모드에서 사용할 수 있습니다.

예

다음 예에서는 IPsec을 보호 모드로 지정합니다.

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel mode ipsec ipv4
```

관련 명령

Command(명령)	설명
interface tunnel	새 VTI 터널 인터페이스를 생성합니다.
tunnel source interface	VTI 터널을 생성하기 위한 소스 인터페이스를 지정합니다.
tunnel destination	VTI 터널 대상의 IP 주소를 지정합니다.
tunnel protection ipsec	터널 보호에 사용할 IPsec 프로파일을 지정합니다.

tunnel protection ipsec

VTI 터널에 대한 IPsec 프로파일을 지정하려면 인터페이스 구성 모드에서 **tunnel protection ipsec** 명령을 사용합니다. 터널에 대한 IPsec 프로파일을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel protection ipsec *IPsec profile name*

no tunnel protection ipsec *IPsec profile name*

구문 설명

ipsec profile name	사용할 IPsec 프로파일의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
인터페이스 구성	• 예	• 아니요	• 예	• 아니요	—

명령 기록

Release	수정 사항
9.7(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 전역 구성 모드에서 **interface tunnel** 명령을 사용한 후에 인터페이스 구성 모드에서 사용할 수 있습니다. 이 명령을 사용하는 경우 IKEv1 정책이 IPsec 프로파일에 연결됩니다.

예

다음 예에서 profile12는 IPsec 프로파일입니다.

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel protection ipsec profile12
```

관련 명령

Command(명령)	설명
interface tunnel	새 VTI 터널 인터페이스를 생성합니다.
tunnel source interface	VTI 터널을 생성하기 위한 소스 인터페이스를 지정합니다.
tunnel destination	VTI 터널 대상의 IP 주소를 지정합니다.
tunnel mode	IPsec이 터널 보호에 사용되도록 지정합니다.

tunnel source interface

VTI 터널에 대한 소스 인터페이스를 지정하려면 인터페이스 구성 모드에서 **tunnel source interface** 명령을 사용합니다. VTI 터널의 소스 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel source interface *interface name*

no tunnel source interface *interface name*

구문 설명

interface name	VTI 터널을 생성하는 데 사용할 소스 인터페이스를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
인터페이스 구성	• 예	• 아니요	• 예	• 아니요	—

명령 기록

Release	수정 사항
9.7(1)	이 명령이 도입되었습니다.

사용 지침

이 명령은 전역 구성 모드에서 **interface tunnel** 명령을 사용한 후에 인터페이스 구성 모드에서 사용할 수 있습니다. IP 주소는 선택한 인터페이스에서 가져옵니다.

예

다음 예에서는 VTI 터널의 소스 인터페이스를 지정합니다.

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel source interface outside
```

관련 명령

Command(명령)	설명
interface tunnel	새 VTI 터널 인터페이스를 생성합니다.
tunnel destination	VTI 터널 대상의 IP 주소를 지정합니다.
tunnel mode	IPsec이 터널 보호에 사용되도록 지정합니다.
tunnel protection ipsec	터널 보호에 사용할 IPsec 프로파일을 지정합니다.

tunnel-group

IPsec 및 WebVPN 터널에 대한 연결별 레코드 데이터베이스를 생성하고 관리하려면 전역 구성 모드에서 **tunnel-group** 명령을 사용합니다. 터널 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-group *name* **type** *type*

no tunnel-group *name*

구문 설명

name	터널 그룹의 이름을 지정합니다. 원하는 문자열을 선택할 수 있습니다. 이름이 IP 주소인 경우 일반적으로 피어의 IP 주소입니다.
type	터널 그룹의 유형을 지정합니다. • remote-access - 사용자가 IPsec 원격 액세스 또는 WebVPN(포털 또는 터널 클라이언트)을 사용하여 연결할 수 있습니다. • ipsec-l2l - 두 개의 사이트 또는 LAN이 인터넷과 같은 공용 네트워크를 통해 안전하게 연결할 수 있는 IPsec LAN-to-LAN을 지정합니다. **참고** 다음 터널 그룹 유형은 릴리스 8.0(2)에서 사용이 중단되었습니다. ipsec-ra - IPsec 원격 액세스 webvpn - WebVPN ASA는 이러한 유형을 remote-access 유형으로 변환합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	참고를 참고하십시오.	• 예	• 예	—

참고 투명 방화벽 모드에서 사용할 수 있는 tunnel-group 명령은 LAN-to-LAN 터널 그룹을 허용하지만 remote-access 그룹 또는 WebVPN 그룹은 허용하지 않습니다. LAN-to-LAN에 사용할 수 있는 모든 **tunnel-group** 명령은 투명 방화벽 모드에서도 사용할 수 있습니다.

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
7.1(1)	webvpn 유형이 추가되었습니다.

Release	수정 사항
8.0(2)	remote-access 유형이 추가되었으며 ipsec-ra 및 webvpn 유형의 사용이 중단되었습니다.
8.3(1)	*name* 인수가 IPv6 주소를 허용하도록 수정되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

SSL VPN 사용자(AnyConnect 및 클라이언트리스)는 다음과 같은 방법을 사용하여 액세스할 터널 그룹을 선택할 수 있습니다.

- group-url
- group-alias
- 인증서 맵(인증서를 사용하는 경우)

이 명령 및 하위 명령은 사용자가 webvpn 서비스에 로그인할 때 드롭다운 메뉴를 통해 그룹을 선택할 수 있게 허용하도록 ASA를 구성합니다. 메뉴에 표시되는 그룹은 ASA에 구성된 실제 연결 프로파일(터널 그룹)의 별칭 또는 URL입니다.

ASA에는 다음과 같은 기본 터널 그룹이 있습니다.

- DefaultRAGroup, 기본 IPsec 원격 액세스 터널 그룹
- DefaultL2LGroup, 기본 IPsec LAN-to-LAN 터널 그룹
- DefaultWEBVPNGroup, 기본 WebVPN 터널 그룹

이 그룹을 변경할 수는 있지만 삭제할 수는 없습니다. ASA는 이 그룹을 사용하여 터널 협상 동안 식별한 특정 터널 그룹이 없는 경우 원격 액세스 및 LAN-to-LAN 터널 그룹을 위한 기본 터널 매개변수를 구성합니다.

tunnel-group 명령을 입력한 후 다음 명령을 입력하여 특정 터널 그룹에 대한 특정 특성을 구성합니다. 이러한 명령은 각각 터널 그룹 특성을 구성하는 구성 모드를 시작합니다.

- **tunnel-group general-attributes**
- **tunnel-group ipsec-attributes**
- **tunnel-group webvpn-attributes**
- **tunnel-group ppp-attributes**

LAN-to-LAN 연결의 경우 ASA는 crypto map에 지정된 피어 주소를 동일한 이름의 터널 그룹과 일치시켜 연결 터널 그룹을 선택합니다. 따라서 IPv6 피어의 경우 터널 그룹 이름을 피어의 IPv6 주소로 구성해야 합니다. 짧거나 긴 표기법으로 터널 그룹 이름을 지정할 수 있습니다. CLI는 이름을 가장 짧은 표기법으로 축약합니다. For example, if you enter this tunnel group command:

```
ciscoasa(config)# tunnel-group 2001:0db8:0000:0000:0000:0000:1428:57ab type ipsec-l2l
```

구성에 다음과 같이 표시됩니다.

```
tunnel-group 2001:0db8::1428:57ab type ipsec-l2l
```

예

다음 예는 전역 구성 모드에서 입력되었습니다. 첫 번째 예에서는 원격 액세스 터널 그룹을 구성합니다. 그룹 이름은 group1입니다.

```
ciscoasa(config)# tunnel-group group1 type remote-access
ciscoasa(config)#
```

다음 예에서는 "group1" 이라는 webvpn 터널 그룹을 구성하는 tunnel-group 명령을 보여 줍니다. 이 명령을 전역 구성 모드에서 입력합니다.

```
ciscoasa(config)# tunnel-group group1 type webvpn
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
clear configure tunnel-group	구성된 모든 터널 그룹을 지웁니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 구성을 표시합니다.
tunnel-group general-attributes	일반적인 터널 그룹 특성을 구성하는 config-general 모드를 시작합니다.
tunnel-group ipsec-attributes	IPsec 터널 그룹 특성을 구성하는 config-ipsec 모드를 시작합니다.
tunnel-group ppp-attributes	L2TP 연결을 위한 PPP 설정을 구성하는 config-ppp 모드를 시작합니다.
tunnel-group webvpn-attributes	WebVPN 터널 그룹 속성을 구성하는 config-webvpn 모드를 시작합니다.

tunnel-group general-attributes

general-attribute 구성 모드를 시작하려면 전역 구성 모드에서 **tunnel-group general-attributes** 명령을 사용합니다. 이 모드는 지원되는 모든 터널링 프로토콜에 일반적인 설정을 구성하는 데 사용됩니다.

모든 일반 속성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-group *name* **general-attributes**

no tunnel-group *name* **general-attributes**

구문 설명

general-attributes	이 터널 그룹에 대한 속성을 지정합니다.
name	터널 그룹의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
tunnel-group general-attributes 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
7.1(1)	다른 터널 그룹 유형의 여러 속성이 일반 터널 그룹 속성 목록으로 마이그레이션되었으며, tunnel-group general-attributes 모드에 대한 프롬프트가 변경되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

예

전역 구성 모드에서 입력된 다음 예에서는 LAN-to-LAN 피어의 IP 주소를 사용하여 원격 액세스 연결을 위한 원격 액세스 터널 그룹을 생성한 다음, 터널 그룹 일반 속성을 구성할 수 있는 general-attributes 구성 모드를 시작합니다. 터널 그룹의 이름은 209.165.200.225입니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type remote-access
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
ciscoasa(config-tunnel-general)#
```

전역 구성 모드에서 입력된 다음 예에서는 IPsec 원격 액세스 연결을 위한 "remotegrp"라는 터널 그룹을 생성한 다음 "remotegrp" 터널 그룹에 대한 일반 속성을 구성할 수 있는 일반 구성 모드를 시작합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
```

```
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)
```

관련 명령

Command(명령)	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 지정된 터널 그룹을 지웁니다.
show running-config tunnel-group	지정된 터널 그룹 또는 모든 터널 그룹에 대한 현재 실행 중인 터널 그룹 구성을 표시합니다.
tunnel-group	IPsec 및 WebVPN 터널에 대한 연결별 레코드 데이터베이스를 생성하고 관리합니다.

tunnel-group ipsec-attributes

ipsec-attribute 구성 모드를 시작하려면 전역 구성 모드에서 **tunnel-group ipsec-attributes** 명령을 사용합니다. 이 모드는 IPsec 터널링 프로토콜에 특정한 설정을 구성하는 데 사용됩니다.

모든 IPsec 속성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-group *name* **ipsec-attributes**

no tunnel-group *name* **ipsec-attributes**

구문 설명

ipsec-attributes	이 터널 그룹에 대한 속성을 지정합니다.
name	터널 그룹의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
7.1(1)	여러 IPsec 터널 그룹 속성이 일반 터널 그룹 속성 목록으로 마이그레이션되었으며, tunnel-group ipsec-attributes 모드에 대한 프롬프트가 변경되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

예

전역 구성 모드에서 입력된 다음 예에서는 IPsec 원격 액세스 연결을 위한 remotegrp라는 터널 그룹을 생성한 다음 IPsec 그룹 속성을 지정합니다.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)
```

관련 명령

Command(명령)	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 지정된 터널 그룹을 지웁니다.

Command(명령)	설명
show running-config tunnel-group	지정된 터널 그룹 또는 모든 터널 그룹에 대한 현재 실행 중인 터널 그룹 구성을 표시합니다.
tunnel-group	IPsec 및 WebVPN 터널에 대한 연결별 레코드 데이터베이스를 생성하고 관리합니다.

tunnel-group-list enable

tunnel-group group-alias에 정의된 터널 그룹을 활성화하려면 **tunnel-group-list enable** 명령을 사용합니다.

tunnel-group-list enable

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
webvpn 구성	• 예	—	• 예	• 예	—

사용 지침

이 명령은 클라이언트리스 및 AnyConnect VPN 클라이언트 세션에서 tunnel-group group-alias 및 group-url 명령과 함께 사용됩니다. 터널 그룹 드롭다운이 로그인 페이지에 표시되도록 기능을 활성화합니다. group-alias는 ASA 관리자가 엔드 유저에게 표시하기 위해 정의한 employees, engineering, consultants 등의 텍스트 문자열입니다.

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

예

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)# group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)# exit
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
```

관련 명령

Command(명령)	설명
tunnel-group	VPN 연결 프로파일을 만들거나 VPN 연결 프로파일의 데이터베이스에 액세스합니다.
group-alias	연결 프로파일(터널 그룹)의 별칭을 구성합니다.

Command(명령)	설명
group-url	VPN 엔드포인트에서 지정한 URL 또는 IP 주소를 연결 프로파일과 일치시킵니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 구성을 표시합니다.

tunnel-group-map

Adaptive Security Appliance에서는 클라이언트 인증서 인증이 포함된 IPsec 연결 요청을 받은 경우 구성된 정책에 따라 해당 연결에 연결 프로파일을 할당합니다.

이 정책에서는 구성된 규칙, 인증서 OU 필드, IKE ID(예: 호스트 이름, IP 주소, 키 ID), 클라이언트 IP 주소 또는 연결 프로파일에 할당할 기본 연결 프로파일을 사용할 수 있습니다. SSL 연결의 경우 Adaptive Security Appliance는 연결 프로파일을 할당하기 위해 구성한 규칙만 사용합니다.

tunnel-group-map 명령은 기존 맵 이름을 연결 프로파일과 연결하여 구성한 규칙을 기반으로 연결 프로파일을 연결에 할당합니다.

연결 프로파일과 맵 이름의 연결을 해제하려면 이 명령의 **no** 형식을 사용합니다. 이 명령의 no 형식은 맵 이름을 삭제하지 않고 연결 프로파일과의 연결만 삭제합니다.

명령 구문은 다음과 같습니다.

tunnel-group-map [mapname] [rule-index] [connection-profile]

no tunnel-group-map [mapname] [rule-index]

참고

- 다음 명령을 사용하여 인증서 맵 이름을 생성합니다.
  crypto ca certificate map [mapname] [rule-index]
- "터널 그룹"은 "연결 프로파일"의 이전 용어입니다. tunnel-group-map 명령은 연결 프로 파일 맵을 생성하는 것으로 생각하면 됩니다.

구문 설명

mapname	필수. **기존** 인증서 맵의 이름을 식별합니다.
rule-index	필수. 맵 이름과 연결된 규칙 인덱스를 식별합니다. rule-index 파라미터는 **crypto ca certificate map** 명령을 사용하여 정의됩니다. 값은 1 - 65535입니다.
connection-profile	이 인증서 맵 목록의 연결 프로파일 이름을 지정합니다.

기본값

tunnel-group-map을 정의하지 않은 경우 ASA는 클라이언트 인증서 인증이 포함된 IPsec 연결 요청을 받으면 인증서 인증 요청을 다음 정책 중 하나와 순서대로 일치시켜 연결 프로파일을 할당합니다.

Certificate ou field - 주체 DN(고유 이름)의 OU(조직 구성 단위) 필드 값을 기반으로 연결 프로파일을 결정합니다.

IKE identity - Phase1 IKE ID 내용을 기반으로 연결 프로파일을 결정합니다.

peer-ip - 설정된 클라이언트 IP 주소를 기반으로 연결 프로파일을 결정합니다.

Default Connection Profile - 위 세 정책이 일치하지 않는 경우 ASA는 기본 연결 프로파일을 할당합니다. 기본 프로파일은 DefaultRAGroup입니다. tunnel-group-map default-group 명령을 사용하여 기본 연결 프로파일을 구성할 수도 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

맵 이름을 연결 프로파일과 연계하려면 먼저 지정한 맵 이름이 이미 존재해야 합니다. **crypto ca certificate map** 명령을 사용하여 맵 이름을 생성할 수 있습니다. 자세한 내용은 **crypto ca certificate map** 명령에 대한 설명서를 참고하십시오.

맵 이름을 연결 프로파일과 연계한 후에는 이전에 설명한 기본 정책 대신 구성한 규칙을 사용하기 위해 tunnel-group-map을 활성화해야 합니다. 이 작업을 수행하려면 전역 구성 모드에서 **tunnel-group-map enable rules** 명령을 실행합니다.

예

다음 예에서는 맵 이름 **SalesGroup**(규칙 인덱스 **10**)을 **SalesConnectionProfile** 연결 프로파일과 연결합니다.

```
ciscoasa(config)# tunnel-group-map SalesGroup 10 SalesConnectionProfile
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
crypto ca certificate map [map name]	ca certificate map 구성 모드를 시작합니다. 이를 사용하여 인증서 맵 이름을 생성할 수 있습니다.
tunnel-group-map enable	설정된 규칙에 따라 인증서 기반 IKE 세션을 활성화합니다.
tunnel-group-map default-group	기존 터널 그룹 이름을 기본 터널 그룹으로 지정합니다.

tunnel-group-map default-group

tunnel-group-map default-group 명령은 구성된 다른 방법을 사용하여 이름을 확인할 수 없는 경우에 사용할 기본 터널 그룹을 지정합니다.

tunnel-group-map을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no tunnel-group-map

구문 설명

default-group *tunnel-group-name*	구성된 다른 방법으로 이름을 확인할 수 없는 경우 기본 터널 그룹을 지정합니다. *tunnel-group name*이 이미 있어야 합니다.
rule index	선택 사항. **crypto ca certificate map** 명령으로 지정된 파라미터를 참조합니다. 값은 1 - 65535입니다.

기본값

tunnel-group-map default-group의 기본값은 DefaultRAGroup입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

tunnel-group-map 명령은 인증서 기반 IKE 세션이 터널 그룹에 매핑되는 정책 및 규칙을 구성합니다. **crypto ca certificate map** 명령을 사용하여 만든 인증서 맵 항목을 터널 그룹과 연결하려면 전역 구성 모드에서 **tunnel-group-map** 명령을 사용합니다. 각 호출이 고유하고 및 맵 색인을 두 번 이상 참조하지 않는 경우에만 해당 명령을 여러 번 호출할 수 있습니다.

crypto ca certificate map 명령은 우선순위가 지정된 인증서 매핑 규칙 목록을 유지 관리합니다. 하나의 맵만 있을 수 있습니다. 그러나 이 맵에 최대 65535개의 규칙이 있을 수 있습니다. 자세한 내용은 **crypto ca certificate map** 명령에 대한 설명서를 참고하십시오.

인증서에서 터널 그룹 이름을 가져오는 프로세스에서는 터널 그룹과 연결되지 않은 인증서 맵의 항목(이 명령으로 식별되지 않은 모든 맵 규칙)을 무시합니다.

예

전역 구성 모드에서 입력된 다음 예에서는 구성된 다른 방법으로 이름을 확인할 수 없는 경우 기본 터널 그룹을 지정합니다. 사용할 터널 그룹의 이름은 group1입니다.

```
ciscoasa(config)# tunnel-group-map default-group group1
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
crypto ca certificate map	crypto ca certificate map 구성 모드를 시작합니다.
subject-name (crypto ca certificate map)	CA 인증서에서 규칙 항목 문자열과 비교할 DN을 식별합니다.
tunnel-group-map enable	인증서 기반 IKE 세션이 터널 그룹에 매핑되는 정책 및 규칙을 구성합니다.

tunnel-group-map enable

tunnel-group-map enable 명령은 인증서 기반 IKE 세션이 터널 그룹에 매핑되는 정책 및 규칙을 구성합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-group-map [*rule-index*] **enable** *policy*

no tunnel-group-map enable [*rule-index*]

구문 설명

policy	인증서에서 터널 그룹 이름 파생에 대한 정책을 지정합니다. *Policy*는 다음 중 하나가 될 수 있습니다. **ike-id** - 터널 그룹이 규칙 조회를 기반으로 결정되거나 ou에서 가져온 것이 아니라 인증서 기반 IKE 세션이 1단계 IKE ID의 콘텐츠에 따라 터널 그룹에 매핑되는 것을 나타냅니다. **ou** - 터널 그룹이 규칙 조회를 기반으로 결정되지 않고 주체 DN(고유 이름)에서 OU(조직 단위)의 값을 사용하는 것을 나타냅니다. **peer-ip** - 터널 그룹이 규칙 조회를 기반으로 결정되거나 ou 또는 ike-id 방식에서 가져온 것이 아니라 설정된 피어 IP 주소를 사용하는 것을 나타냅니다. **rules** - 인증서 기반 IKE 세션이 이 명령에 의해 구성된 인증서 맵 연계를 기반으로 터널 그룹에 매핑되는 것을 나타냅니다.
rule index	(선택 사항) **crypto ca certificate map** 명령을 통해 지정된 매개변수를 참조하십시오. 값은 1 - 65535입니다.

기본값

tunnel-group-map 명령의 기본값은 **enable ou**이고 **default-group**은 DefaultRAGroup으로 설정됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

crypto ca certificate map 명령은 우선순위가 지정된 인증서 매핑 규칙 목록을 유지 관리합니다. 하나의 맵만 있을 수 있습니다. 그러나 이 맵에 최대 65535개의 규칙이 있을 수 있습니다. 자세한 내용은 **crypto ca certificate map** 명령에 대한 설명서를 참고하십시오.

예

다음 예에서는 인증서 기반 IKE 세션을 Phase1 IKE ID의 내용을 기반으로 터널 그룹에 매핑합니다.

```
ciscoasa(config)# tunnel-group-map enable ike-id
ciscoasa(config)#
```

다음 예에서는 인증서 기반 IKE 세션을 설정된 피어 IP 주소를 기반으로 터널 그룹에 매핑합니다.

```
ciscoasa(config)# tunnel-group-map enable peer-ip
ciscoasa(config)#
```

다음 예에서는 주체 DN(고유 이름)의 OU(조직 구성 단위)를 기반으로 인증서 기반 IKE 세션을 매핑합니다.

```
ciscoasa(config)# tunnel-group-map enable ou
ciscoasa(config)#
```

다음 예에서는 설정된 규칙을 기반으로 인증서 기반 IKE 세션을 매핑합니다.

```
ciscoasa(config)# tunnel-group-map enable rules
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
crypto ca certificate map	CA 인증서 맵 모드를 시작합니다.
subject-name (crypto ca certificate map)	CA 인증서에서 규칙 항목 문자열과 비교할 DN을 식별합니다.
tunnel-group-map default-group	기존 터널 그룹 이름을 기본 터널 그룹으로 지정합니다.

tunnel-group ppp-attributes

ppp-attributes 구성 모드를 시작하고 L2TP over IPsec 연결에서 사용하는 PPP 설정을 구성하려면 전역 구성 모드에서 **tunnel-group ppp-attributes** 명령을 사용합니다.

모든 PPP 속성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-group *name* **ppp-attributes**

no tunnel-group *name* **ppp-attributes**

구문 설명

name	터널 그룹의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

PPP 설정은 원격 클라이언트가 전화 접속 전화 서비스 공용 IP 네트워크를 사용하여 사설 회사 네트워크 서버와 안전하게 통신할 수 있도록 해주는 VPN 터널링 프로토콜인 L2TP(계층 2 터널링 프로토콜)에서 사용됩니다. L2TP는 클라이언트/서버 모델을 기반으로 하며 PPP over UDP(포트 1701)를 사용하여 데이터를 터널링합니다. 모든 터널 그룹 ppp 명령은 PPPoE 터널 그룹 유형에 사용할 수 있습니다.

예

다음 예에서는 터널 그룹 *telecommuters*를 만들고 ppp-attributes 구성 모드를 시작합니다.

```
ciscoasa(config)# tunnel-group telecommuters type pppoe
ciscoasa(config)# tunnel-group telecommuters ppp-attributes
ciscoasa(tunnel-group-ppp)#
```

관련 명령

Command(명령)	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 지정된 터널 그룹을 지웁니다.
show running-config tunnel-group	지정된 터널 그룹 또는 모든 터널 그룹에 대한 현재 실행 중인 터널 그룹 구성을 표시합니다.
tunnel-group	IPsec 및 WebVPN 터널에 대한 연결별 레코드 데이터베이스를 생성하고 관리합니다.

tunnel-group-preference

엔드포인트에서 지정한 것과 일치하는 그룹 URL이 있는 연결 프로파일로 VPN 환경 설정을 변경하려면 webvpn 구성 모드에서 **tunnel-group-preference** 명령을 사용합니다. 이 명령을 구성에서 제거하려면 **no** 형식을 사용합니다.

tunnel-group-preference group-url

no tunnel-group-preference group-url

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본적으로 ASA는 연결 프로파일의 인증서 필드 값을 엔드포인트에서 사용하는 인증서의 필드 값과 일치시킨 경우 해당 프로파일을 VPN 연결에 할당합니다. 이 명령은 기본 동작을 재정의합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
Config-webvpn	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.2(5)/8.4(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 연결 프로파일 선택 프로세스 중에 연결 프로파일의 환경 설정을 변경합니다. 많은 이전 ASA 소프트웨어 릴리스에서 사용한 그룹 URL 환경 설정을 따를 수 있습니다. 엔드포인트에서 연결 프로파일에 없는 그룹 URL을 지정했지만 연결 프로파일과 일치하는 인증서 값을 지정한 경우 ASA는 해당 연결 프로파일을 VPN 세션에 할당합니다.

이 명령은 webvpn 구성 모드에서 입력하지만 ASA에서 협상된 모든 클라이언트리스 및 AnyConnect VPN 연결에 대한 연결 프로파일 선택 환경 설정을 변경합니다.

예

다음 예에서는 연결 프로파일 선택 프로세스 중에 연결 프로파일의 환경 설정을 변경합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-preference group-url
ciscoasa(config-webvpn)#
```

관련 명령

Command(명령)	설명
tunnel-group	VPN 연결 프로파일을 만들거나 VPN 연결 프로파일의 데이터베이스에 액세스합니다.
group-url	VPN 엔드포인트에서 지정한 URL 또는 IP 주소를 연결 프로파일과 일치시킵니다.
show running-config tunnel-group	모든 터널 그룹 또는 특정 터널 그룹에 대한 터널 그룹 구성을 표시합니다.

tunnel-group webvpn-attributes

webvpn-attribute 구성 모드를 시작하려면 전역 구성 모드에서 **tunnel-group webvpn-attributes** 명령을 사용합니다. 이 모드는 WebVPN 터널링에 일반적인 설정을 구성합니다.

모든 WebVPN 속성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-group *name* **webvpn-attributes**

no tunnel-group *name* **webvpn-attributes**

구문 설명

name	터널 그룹의 이름을 지정합니다.
webvpn-attributes	이 터널 그룹에 대한 WebVPN 속성을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.
9.8(1)	pre-fill-username 및 secondary-pre-fill-username 값이 clientless에서 client로 변경되었습니다.

사용 지침

webvpn-attribute 모드에서는 일반 속성 외에 WebVPN 연결에 특정한 다음 속성도 구성할 수 있습니다.

- 인증
- customization
- dns-group
- group-alias
- group-url
- without-csd

pre-fill-username 및 secondary-pre-fill-username 속성은 인증 및 권한 부여에 사용하기 위해 인증서에서 사용자 이름을 추출하는 데 사용됩니다. 값은 client 또는 clientless입니다.

예

전역 구성 모드에서 입력된 다음 예에서는 LAN-to-LAN 피어의 IP 주소를 사용하여 WebVPN 연결을 위한 터널 그룹을 생성하고, WebVPN 속성을 구성할 수 있는 webvpn 구성 모드를 시작합니다. 터널 그룹의 이름은 209.165.200.225입니다.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type webvpn
ciscoasa(config)# tunnel-group 209.165.200.225 webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

전역 구성 모드에서 입력된 다음 예에서는 WebVPN 원격 액세스 연결을 위한 "remotegrp"라는 터널 그룹을 생성한 다음 "remotegrp" 터널 그룹에 대한 WebVPN 속성을 구성할 수 있는 webvpn 구성 모드를 시작합니다.

```
ciscoasa(config)# tunnel-group remotegrp type webvpn
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

Command(명령)	설명
clear configure tunnel-group	전체 터널 그룹 데이터베이스 또는 지정된 터널 그룹을 지웁니다.
show running-config tunnel-group	지정된 터널 그룹 또는 모든 터널 그룹에 대한 현재 실행 중인 터널 그룹 구성을 표시합니다.
tunnel-group	IPsec 및 WebVPN 터널에 대한 연결별 레코드 데이터베이스를 생성하고 관리합니다.

tunnel-limit

허용되는 활성 GTP 터널의 최대 수를 지정하려면 정책 맵 파라미터 구성 모드에서 **tunnel limit** 명령을 사용합니다. 터널 제한을 기본값으로 다시 설정하려면 이 명령의 **no** 형식을 사용합니다.

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

구문 설명

max_tunnels	허용되는 최대 터널 수입니다. 이는 PDP 컨텍스트 또는 엔드포인트의 수와 같습니다.

기본값

기본 터널 제한은 500입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령으로 지정된 터널 수에 도달하면 새 요청이 삭제됩니다.

예

다음 예에서는 GTP 트래픽의 최대 터널 수를 10,000개로 지정합니다.

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tunnel-limit 10000
```

관련 명령

명령	설명
clear service-policy inspect gtp	전역 GTP 통계를 지웁니다.
inspect gtp	애플리케이션 검사에 사용할 특정 GTP 맵을 적용합니다.
show service-policy inspect gtp	GTP 구성을 표시합니다.

tx-ring-limit

우선순위 대기열의 깊이를 지정하려면 priority-queue 모드에서 **tx-ring-limit** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

참고 이 명령은 ASA 5580 10GB 이더넷 인터페이스, ASA 5512-X~ASA 5555-X 관리 인터페이스 또는 ASA Services Module에서 지원되지 않습니다. 10GB 이더넷 인터페이스는 ASA 5585-X의 우선순위 대기열에 지원됩니다.

tx-ring-limit *number-of-packets*

no tx-ring-limit *number-of-packets*

구문 설명

number-of-packets	혼잡이 해소되기까지 패킷을 버퍼링할 수 있도록 드라이버가 인터페이스의 큐로 다시 보내기 전에 이더넷 전송 드라이버에 대해 허용되는 짧은 레이턴시 또는 일반 우선순위 패킷의 최대 수를 지정합니다. 3~511 범위입니다.

기본값

기본값은 511입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
Priority-queue	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

ASA에서는 두 개의 트래픽 클래스를 허용합니다. 우선순위가 더 높고 레이턴시에 민감한 트래픽(예: 음성과 비디오)에는 LLQ(Low-Latency Queuing), 나머지 모든 트래픽에는 기본값인 BE(Best Effort)를 허용합니다. ASA는 우선순위 트래픽을 인식하여 적절한 QoS(Quality of Service) 정책을 적용합니다. 우선순위 대기열의 크기와 깊이를 구성하여 트래픽 흐름을 미세 조정할 수 있습니다.

우선순위 대기열을 적용하려면 먼저 **priority-queue** 명령을 사용하여 인터페이스에 대한 우선순위 대기열을 만들어야 합니다. **nameif** 명령으로 정의할 수 있는 모든 인터페이스에 하나의 **priority-queue** 명령을 적용할 수 있습니다.

priority-queue 명령은 프롬프트에 표시된 대로 priority-queue 모드를 시작합니다. priority-queue 모드에서는 지정된 시점에 전송 대기열에서 허용되는 최대 패킷 수(**tx-ring-limit** 명령) 및 패킷을 삭제하기 전에 버퍼할 수 있는 유형(우선순위 또는 최상의 결과)의 패킷 수(**queue-limit** 명령)를 구성할 수 있습니다.

지정한 tx-ring-limit 및 queue-limit은 높은 우선순위 저지연 대기열과 최상의 결과 대기열 모두에 영향을 줍니다. tx-ring-limit은 혼잡이 해결될 때까지 패킷을 버퍼할 수 있도록 드라이버가 인터페이스의 대기열에 다시 추가하기 전에 드라이버에서 유형의 패킷 수입니다. 일반적으로 이 두 파라미터를 조정하여 저지연 트래픽의 흐름을 최적화할 수 있습니다.

큐는 무한한 크기가 아니기 때문에 가득 차고 오버플로될 수 있습니다. 큐가 가득 차면 추가 패킷이 큐에 추가되기 않고 삭제됩니다. 이를 *tail drop*이라고 합니다. 대기열이 가득 차는 것을 방지하기 위해 **queue-limit** 명령을 사용하여 대기열 버퍼 크기를 늘릴 수 있습니다.

참고 **queue-limit** 및 **tx-ring-limit** 명령에 대한 값 범위의 상한은 런타임에 동적으로 결정됩니다. 이 제한을 보려면 명령줄에서 **help** 또는 **?**를 입력합니다. 주요 요소는 대기열을 지원하는 데 필요한 메모리와 장치에서 사용할 수 있는 메모리입니다.

ASA 모델 5505에서는(이 모델에 한정) 하나의 인터페이스에서 구성한 priority-queue가 다른 모든 인터페이스의 동일한 구성을 덮어씁니다. 즉, 마지막으로 적용된 구성만 모든 인터페이스에 존재합니다. 또한 하나의 인터페이스에서 priority-queue를 제거하면 모든 인터페이스에서 제거됩니다.

이 문제를 해결하려면 하나의 인터페이스에서만 **priority-queue** 명령을 구성합니다. 다른 인터페이스에 **queue-limit** 및/또는 **tx-ring-limit** 명령에 대한 다른 설정이 필요한 경우 그 중 하나의 인터페이스에서 모든 queue-limit의 최대값과 모든 tx-ring-limit의 최소값을 사용합니다.

예

다음 예에서는 대기열 제한을 2048개의 패킷으로 지정하고, 전송 대기열 제한을 256개의 패킷으로 지정하여 test라는 인터페이스에 대한 우선순위 대기열을 구성합니다.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 2048
ciscoasa(priority-queue)# tx-ring-limit 256
```

관련 명령

Command(명령)	설명
clear configure priority-queue	명명된 인터페이스의 현재 우선순위 대기열 구성을 제거합니다.
priority-queue	인터페이스에서 우선순위 대기열을 구성합니다.
queue-limit	데이터를 삭제하기 전에 우선순위 대기열에 넣을 수 있는 최대 패킷 수를 지정합니다.
show priority-queue statistics	명명된 인터페이스에 대한 우선순위 대기열 통계를 표시합니다.
show running-config priority-queue	현재 우선순위 대기열 구성을 표시합니다. **all** 키워드를 지정한 경우 이 명령은 모든 현재 **priority-queue**, **queue-limit** 및 **tx-ring-limit** 명령 구성 값을 표시합니다.

type echo

SLA 작업을 에코 응답 시간 프로브 작업으로 구성하려면 SLA 모니터 구성 모드에서 **type echo** 명령을 사용합니다. SLA 구성에서 유형을 제거하려면 이 명령의 **no** 형식을 사용합니다.

type echo protocol ipIcmpEcho *target* **interface** *if-name*

no type echoprotocol ipIcmpEcho *target* **interface** *if-name*

구문 설명

interface *if-name*	**nameif** 명령에 지정된 대로 에코 요청 패킷을 보내는 데 사용되는 인터페이스의 이름을 지정합니다. 인터페이스 소스 주소는 에코 요청 패킷의 소스 주소로 사용됩니다.
protocol	protocol 키워드입니다. 지원되는 값은 에코 작업에 IP/ICMP 에코 요청을 사용하도록 지정하는 **ipIcmpEcho**뿐입니다.
target	모니터링할 개체의 IP 주소 또는 호스트 이름입니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
SLA 모니터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ICMP 패킷의 페이로드 기본 크기는 28바이트이며, 이는 전체 ICMP 패킷 크기를 64바이트로 만듭니다. **request-data-size** 명령을 사용하여 페이로드 크기를 변경할 수 있습니다.

예

다음 예에서는 ICMP 에코 요청/응답 시간 프로브 작업을 사용하는 ID가 123인 SLA 작업을 구성합니다. SLA 연결성을 추적할 ID가 1인 추적 항목을 만듭니다. SLA 작업의 빈도는 10초, 임계값은 2500밀리초, 시간 초과 값은 4000밀리초로 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)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

관련 명령

Command(명령)	설명
num-packets	SLA 작업 중에 전송할 요청 패킷 수를 지정합니다.
request-data-size	SLA 작업 요청 패킷에 대한 페이로드 크기를 지정합니다.
sla monitor	SLA 모니터링 작업을 정의합니다.

uc-ime through username-prompt 명령

uc-ime(사용되지 않음)

Cisco Intercompany Media Engine 프록시 인스턴스를 생성하려면 전역 구성 모드에서 **uc-ime** 명령을 사용합니다. 프록시 인스턴스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

uc-ime *uc-ime_name*

no uc-ime *uc-ime_name*

구문 설명

uc-ime_name	ASA에 구성된 Cisco Intercompany Media Engine 프록시의 인스턴스 이름을 지정합니다. *name*은 64자로 제한됩니다. 하나의 Cisco Intercompany Media Engine 프록시만 ASA에서 구성할 수 있습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• **예**	—	• 예	—	—

명령 기록

Release	수정 사항
8.3(1)	이 명령이 추가되었습니다.
9.4(1)	이 명령의 사용이 중단되었습니다.

사용 지침

Cisco Intercompany Media Engine 프록시를 구성합니다. Cisco Intercompany Media Engine은 VoIP 기술을 통해 사용할 수 있는 고급 기능으로 인터넷을 통한 기업의 온디맨드 상호 연결을 지원합니다. Cisco Intercompany Media Engine은 P2P(peer-to-peer), 보안 및 SIP 프로토콜을 활용해 기업 간의 동적 SIP 트렁크를 만들어 여러 엔터프라이즈의 Cisco Unified Communications Manager 클러스터 간에 B2B(Business-to-Business) 페더레이션을 허용합니다. 엔터프라이즈 컬렉션은 클러스터 내 트렁크로 함께 작동하여 하나의 대규모 기업처럼 보이게 됩니다.

미디어 종단 인스턴스를 Cisco Intercompany Media Engine 프록시에서 지정하려면 먼저 해당 인스턴스를 만들어야 합니다.

하나의 Cisco Intercompany Media Engine 프록시만 ASA에서 구성할 수 있습니다.

예

다음 예에서는 **uc-ime** 명령을 사용하여 Cisco Intercompany Media Engine 프록시를 구성하는 방법을 보여 줍니다.

```
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
```

관련 명령

Command(명령)	설명
fallback	연결 무결성이 저하된 경우 Cisco Intercompany Media Engine이 VoIP에서 PSTN으로 대체하는 데 사용하는 대체 타이머를 구성합니다.
show uc-ime	fallback-notifications, mapping-service-sessions 및 signaling-sessions에 대한 통계 또는 세부 정보를 표시합니다.
ticket	Cisco Intercompany Media Engine 프록시에 대한 티켓 에포크 및 비밀번호를 구성합니다.
ucm	Cisco Intercompany Media Engine 프록시에서 연결하는 Cisco UCM을 구성합니다.

ucm(사용되지 않음)

Cisco Intercompany Media Engine 프록시에서 연결하는 Cisco UCM(Unified Communication Manager)을 구성하려면 전역 구성 모드에서 **ucm** 명령을 사용합니다. Cisco Intercompanuy Media Engine 프록시에 연결된 Cisco UCM을 제거하려면 이 명령의 **no** 형식을 사용합니다.

ucm address *ip_address* **trunk-security-mode** {**nonsecure** | **secure**}

no ucm address *ip_address* **trunk-security-mode** {**nonsecure** | **secure**}

구문 설명

주소	Cisco UCM(Unified Communications Manager)의 IP 주소를 구성할 키워드입니다.
ip_address	Cisco UCM의 IP 주소를 지정합니다. IPv4 형식으로 IP 주소를 입력합니다.
Non-secure	Cisco UCM 또는 Cisco UCM 클러스터가 비보안 모드로 작동하도록 지정합니다.
secure	Specifies that the Cisco UCM or Cisco UCM cluster is operating in secure mode.
trunk-security-mode	Cisco UCM 또는 Cisco UCM 클러스터의 보안 모드를 구성할 키워드입니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
UC-IME 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.3(1)	이 명령이 추가되었습니다.
9.4(1)	이 명령은 모든 **uc-ime** 모드 명령과 함께 사용이 중단되었습니다.

사용 지침

엔터프라이즈에서 Cisco UCM 서버를 지정합니다.

Cisco Intercompany Media Engine 프록시에 대해 여러 **ucm** 명령을 입력할 수 있습니다.

참고 SIP 트렁크가 활성화된 Cisco Intercompany Media Engine이 있는 클러스터에 각 Cisco UCM에 대한 항목을 포함해야 합니다.

Cisco UCM 또는 Cisco UCM 클러스터에 대해 **secure**를 지정한 경우 이는 Cisco UCM 또는 Cisco UCM 클러스터가 TLS를 시작함을 나타내므로 구성요소에 대한 TLS 구성을 설정해야 합니다.

이 작업에서 **secure** 옵션을 지정하거나, 나중에 엔터프라이즈에 대한 TLS를 구성하는 동안 업데이트할 수 있습니다.

엔터프라이즈 내 TLS는 ASA에 표시된 대로 Cisco Intercompany Media Engine 트렁크의 보안 상태를 나타냅니다.

Cisco Intercompany Media Engine 트렁크에 대한 전송 보안이 Cisco UCM에서 변경된 경우 Adaptive Security Appliance에서도 변경되어야 합니다. 불일치할 경우 호출에 실패합니다. Adaptive Security Appliance는 비보안 IME 트렁크를 통한 SRTP를 지원하지 않습니다. Adaptive Security Appliance는 SRTP가 보안 트렁크를 통해 허용되는 것으로 가정합니다. 따라서 TLS를 사용하는 경우 IME 트렁크에 대해 SRTP가 허용되는지 확인해야 합니다. ASA는 보안 IME 트렁크 호출에 대해 RTP로의 SRTP 대체를 지원합니다.

프록시는 엔터프라이즈 경계에 있으며, 엔터프라이즈 간에 생성된 SIP 트렁크 간의 SIP 신호 처리를 검사합니다. 또한 인터넷에서의 TLS 신호 처리를 종료하고 Cisco UCM으로의 TCP 또는 TLS를 시작합니다.

TLS(전송 계층 보안)는 인터넷 등의 네트워크를 통한 통신에 대해 보안을 제공하는 암호화 프로토콜입니다. TLS는 엔드 투 엔드 전송 계층에서 네트워크 연결 세그먼트를 암호화합니다.

TCP가 내부 네트워크 내에서 허용되는 경우에는 이 작업이 필요하지 않습니다.

로컬 엔터프라이즈 내에서 TLS를 구성하는 주요 단계는 다음과 같습니다.

- 로컬 ASA에서 자체 서명된 인증서에 대한 또 다른 RSA 키 및 트러스트 포인트를 만듭니다.
- 로컬 Cisco UCM과 로컬 ASA 간에 인증서를 내보내고 가져옵니다.
- ASA에서 로컬 Cisco UCM에 대한 트러스트 포인트를 만듭니다.

TLS를 통한 인증: ASA가 N개의 엔터프라이즈를 위한 포트 역할을 하려면 Cisco UCM에서 ASA의 인증서 하나를 허용할 수 있어야 합니다. 이렇게 하려면 모든 UC-IME SIP 트렁크를 ASA에서 제공하는 것과 동일한 주체 이름이 포함된 동일한 SIP 보안 프로파일과 연결하면 됩니다. Cisco UCM은 인증서에서 주체 이름을 추출하여 보안 프로파일에 구성된 이름과 비교하기 때문입니다.

예

다음 예에서는 UCM 프록시에 연결하는 방법을 보여 줍니다.

```
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
```

umbrella

DNS 검사 엔진이 Cisco Umbrella DNS 조회 요청을 리디렉션할 수 있도록 하려면 DNS 검사 정책 맵 파라미터 구성 모드에서 **umbrella** 명령을 사용합니다. Cisco Umbrella를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

umbrella [**tag** *umbrella_policy*] [**fail-open**]

no umbrella [**tag** *umbrella_policy*] [**fail-open**]

구문 설명

fail-open	Cisco Umbrella DNS 서버를 사용할 수 없는 경우 이 정책 맵에서 Umbrella를 자체적으로 비활성화하고 DNS 요청이 시스템에 구성된 다른 DNS 서버(있는 경우)로 이동하도록 허용합니다. Umbrella DNS 서버를 다시 사용할 수 있게 되면 정책 맵이 해당 서버를 사용하여 재개됩니다. 이 옵션을 포함하지 않으면 DNS 요청이 계속해서 도달할 수 없는 Umbrella 확인자로 이동하므로 응답을 받지 못합니다.
tag *umbrella_policy*	(선택 사항). Cisco Umbrella에 정의되어 있는 엔터프라이즈 보안 정책의 이름으로, 디바이스에 적용 됩니다. 정책을 지정하지 않거나 입력한 이름이 Cisco Umbrella에 없으면 기본 정책이 할당됩니다.

기본값

태그를 지정하지 않으면 디바이스 등록에서 기본 엔터프라이즈 보안 정책을 할당합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.10(1)	이 명령이 추가되었습니다.
9.12(1)	**fail-open** 키워드가 추가되었습니다.

사용 지침

DNS 검사 정책 맵을 구성할 때 이 명령을 사용합니다.

활성 DNS 검사 정책 맵에 이 명령이 있으면 Cisco Umbrella 등록 서버와의 등록 프로세스가 시작됩니다. HTTPS를 통해 수행되는 연결 및 등록을 설정하려면 등록 서버의 CA 인증서를 설치해야 합니다.

전역 구성 모드에서 **umbrella-global** 명령을 사용하여 전역 파라미터도 구성해야 합니다.

예

다음 예에서는 기본 정책을 사용하여 Umbrella를 활성화하고 전역 DNS 검사에서 사용되는 기본 검사 정책 맵에서 DNScrypt를 활성화합니다.

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

다음 예에서는 기본 정책을 사용하여 Umbrella가 열리지 못하도록 하고 전역 DNS 검사에서 사용되는 기본 검사 정책 맵에서 DNScrypt를 활성화합니다. 이미 태그로 등록한 경우 **fail-open** 옵션만 추가하려면 명령에 동일한 태그를 포함해야 합니다. 그렇지 않으면 태그 없이 디바이스를 다시 등록합니다.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

관련 명령

명령	설명
dnscrypt	디바이스와 Cisco Umbrella 간의 연결에 대한 DNScrypt 암호화를 활성화합니다.
inspect dns	DNS 검사를 활성화합니다.
policy-map type inspect dns	DNS 검사 정책 맵을 생성합니다.
public-key	Cisco Umbrella와 함께 사용 되는 공개 키를 구성 합니다.
token	Cisco Umbrella에 등록하는 데 필요한 API 토큰을 식별합니다.
timeout edns	서버에서 응답이 없는 경우 클라이언트에서 Umbrella 서버로의 연결을 제거하기 전의 유휴 시간 제한을 구성합니다.
umbrella-global	Cisco Umbrella 전역 파라미터를 구성합니다.

umbrella-global

디바이스를 Cisco Umbrella 포털에 연결하는 데 필요한 전역 설정을 구성할 수 있도록 Umbrella 구성 모드를 시작하려면 전역 구성 모드에서 **umbrella-global** 명령을 사용합니다. 전역 Umbrella 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

umbrella-global

no umbrella-global

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 전역 Umbrella 구성은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 컨피그레이션	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.10(1)	이 명령이 추가되었습니다.

사용 지침

Cisco Umbrella 서비스에 가입한 경우 Cisco Umbrella에 등록하도록 디바이스를 구성할 수 있습니다.

Umbrella 전역 설정은 기본적으로 디바이스를 Cisco Umbrella에 등록하는 데 필요한 API 토큰을 정의합니다. Cisco Umbrella 대시보드에서 토큰을 가져옵니다.

전역 설정은 Umbrella를 활성화하는 데 충분하지 않습니다. 또한 파라미터 구성 모드에서 umbrella 명령을 사용하여 DNS 검사 정책 맵에서 Umbrella를 활성화해야 합니다.

예

다음 예에서는 전역 Umbrella 설정을 구성하고 기본 DNS 검사 정책 맵에서 Umbrella를 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

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

관련 명령

명령	설명
dnscrypt	디바이스와 Cisco Umbrella 간의 연결에 대한 DNScrypt 암호화를 활성화합니다.
local-domain-bypass	DNS 요청이 Cisco Umbrella를 우회해야 하는 로컬 도메인을 구성합니다.
public-key	Cisco Umbrella와 함께 사용 되는 공개 키를 구성 합니다.
resolver	DNS 요청을 확인하는 Cisco Umbrella DNS 서버의 주소를 구성합니다.
token	Cisco Umbrella에 등록하는 데 필요한 API 토큰을 식별합니다.
timeout edns	서버에서 응답이 없는 경우 클라이언트에서 Umbrella 서버로의 연결을 제거하기 전의 유휴 시간 제한을 구성합니다.
umbrella	DNS 검사 엔진이 DNS 조회 요청을 Cisco Umbrella로 리디렉션할 수 있도록 합니다.

undebug

현재 세션에서 디버깅 정보 표시를 비활성화하려면 특권 EXEC 모드에서 **undebug** 명령을 사용합니다.

undebug {*command* | **all**}

구문 설명

all	모든 디버그 출력을 비활성화합니다.
command	지정된 명령에 대한 디버그를 비활성화합니다. 지원되는 명령에 대한 자세한 내용은 사용 지침을 참고하십시오.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• **예**	• **예**	• 예	• 예	• **예**

명령 기록

Release	수정 사항
7.0(1)	이 명령이 수정되었습니다. 여기에는 추가 **debug** 키워드가 포함됩니다.

사용 지침

다음 명령은 **undebug** 명령과 함께 사용할 수 있습니다. 특정 명령의 디버깅 또는 특정 **debug** 명령의 연계된 인수 및 키워드에 대한 자세한 내용은 **debug** 명령 항목을 참고하십시오.

- aaa - AAA 정보
- acl - ACL 정보
- all - 모든 디버깅
- appfw - 애플리케이션 방화벽 정보
- arp - NP 작업을 포함하는 ARP
- asdm - ASDM 정보
- auto-update - 자동 업데이트 정보
- boot-mem - 부트 메모리 계산 및 설정
- cifs - CIFS 정보
- cmgr - CMGR 정보
- context - 상황 정보
- cplane - CP 정보

- crypto - 암호화 정보
- ctiqbe - CTIQBE 정보
- ctl-provider - CTL 공급자 디버깅 정보
- dap - DAP 정보
- dcerpc - DCERPC 정보
- ddns - 동적 DNS 정보
- dhcpc - DHCP 클라이언트 정보
- dhcpd - DHCP 서버 정보
- dhcprelay - DHCP 릴레이 정보
- disk - 디스크 정보
- dns - DNS 정보
- eap - EAP 정보
- eigrp - EIGRP 프로토콜 정보
- email - 이메일 정보
- entity - 엔터티 MIB 정보
- eou - EAPoUDP 정보
- esmtp - ESMTP 정보
- fips - FIPS 140-2 정보
- fixup - 수정 정보
- fover - 장애 조치 정보
- fsm - FSM 정보
- ftp - FTP 정보
- generic - 기타 정보
- gtp - GTP 정보
- h323 - H323 정보
- http - HTTP 정보
- icmp - ICMP 정보
- igmp - IGMP(Internet Group Management Protocol)
- ils - LDAP 정보
- im - IM 검사 정보
- imagemgr - 이미지 관리자 정보
- inspect - 디버깅 검사 정보
- integrityfw - 무결성 방화벽 정보
- ip - IP 정보
- ipsec-over-tcp - IPsec over TCP 정보
- ipsec-pass-thru - ipsec-pass-thru 검사 정보
- ipv6 - IPv6 정보
- iua-proxy - IUA 프록시 정보

- kerberos - KERBEROS 정보
- l2tp - L2TP 정보
- ldap - LDAP 정보
- mfib - 멀티캐스트 전달 정보 데이터베이스
- mgcp - MGCP 정보
- module-boot - 서비스 모듈 부트 정보
- mrib - 멀티캐스트 라우팅 정보 데이터베이스
- nac-framework - NAC-FRAMEWORK 정보
- netbios-inspect - NETBIOS 검사 정보
- npshim - NPSHIM 정보
- ntdomain - NT 도메인 정보
- ntp - NTP 정보
- ospf - OSPF 정보
- p2p - P2P 검사 정보
- parser - 파서 정보
- pim - 프로토콜 독립 멀티캐스트
- pix - PIX 정보
- ppp - PPP 정보
- pppoe - PPPoE 정보
- pptp - PPTP 정보
- radius - RADIUS 정보
- redundant-interface - 예비 인터페이스 정보
- rip - RIP 정보
- rtp - RTP 정보
- rtsp - RTSP 정보
- sdi - SDI 정보
- sequence - 시퀀스 번호 추가
- session-command - 세션 명령 정보
- sip - SIP 정보
- skinny - Skinny 정보
- sla - IP SLA 모니터 디버그
- smtp-client - 이메일 시스템 로그 메시지
- splitdns - 스플릿 DNS 정보
- sqlnet - SQLNET 정보
- ssh - SSH 정보
- sunrpc - SUNRPC 정보
- tacacs - TACACS 정보
- tcp - WebVPN용 TCP

- tcp-map - TCP 맵 정보
- timestamps - 타임스탬프 추가
- track - 고정 경로 추적
- vlan-mapping - VLAN 매핑 정보
- vpn-sessiondb - VPN 세션 데이터베이스 정보
- vpnlb - VPN 부하 균형 정보
- wccp - WCCP 정보
- webvpn - WebVPN 정보
- xdmcp - XDMCP 정보
- xml - XML 파서 정보

디버깅 출력은 CPU 프로세스에서 높은 우선순위가 할당되기 때문에 시스템을 사용할 수 없게 만들 수 있습니다. 따라서 **debug** 명령은 특정 문제를 트러블슈팅하거나 Cisco TAC를 통해 세션 문제를 트러블슈팅하는 동안에만 사용해야 합니다. 또한, 네트워크 트래픽과 사용자 수가 적은 기간에 **debug** 명령을 사용하는 것이 가장 좋습니다. 그러한 기간에 디버깅하면 **debug** 명령의 처리 오버헤드 증가로 인해 시스템 사용에 지장이 생길 가능성이 줄어듭니다.

예

다음 예에서는 모든 디버깅 출력을 비활성화합니다.

```
ciscoasa(config)# undebug all
```

관련 명령

Command(명령)	설명
debug	선택한 명령에 대한 디버그 정보를 표시합니다.

unit parallel-join

트래픽이 모듈 간에 고르게 분산되도록 Firepower 9300 섀시의 보안 모듈이 클러스터에 동시에 조인하는지 확인하려면 클러스터 그룹 구성 모드에서 **unit parallel-join** 명령을 사용합니다. 병렬 조인을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*

no unit parallel-join [*num_of_units* **max-bundle-delay** *max_delay_time*]

구문 설명

num_of_units	모듈이 클러스터에 참가하기 전에 준비해야 하는 동일한 섀시의 최소 모듈 수를 1~3 범위에서 지정합니다. 기본값은 1인데, 이는 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하지 않는다는 것을 의미합니다. 예를 들어, 값을 3으로 설정하는 경우, 각 모듈이 클러스터에 참가하기 전에 *max_delay_time*동안 대기하거나 3개의 모듈이 모두 준비 상태가 될 때까지 대기합니다. 3개 모듈 모두 클러스터에 거의 동시에 참가하도록 요청하며 비슷한 시간에 트래픽을 수신하기 시작합니다.
max-bundle-delay ***max_delay_time***	모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하는 것을 중지하기 전의 최대 지연 시간(분)을 0~30분 범위에서 지정합니다. 기본값은 0인데, 이는 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하지 않는다는 것을 의미합니다. *num_of_units*을 1로 설정하는 경우 이 값은 0이어야 합니다. *num_of_units*을 2 또는 3으로 설정하는 경우 이 값은 1 이상이어야 합니다. 이 타이머는 모듈별로 할당되지만 첫 번째 모듈이 클러스터에 참가하면 다른 모든 모듈 타이머가 종료되고 나머지 모듈은 클러스터에 참가합니다. 예를 들어, *num_of_units*을 3으로 설정하고 *max_delay_time*을 5분으로 설정합니다. 모듈 1이 나타나면 5분 타이머가 시작됩니다. 2분 후에 모듈 2가 나타나고 5분 타이머가 시작됩니다. 1분 후에 모듈 3이 나타나므로 4분으로 표시될 때는 이제 모든 모듈이 클러스터에 참가하게 되며, 모든 모듈은 타이머가 완료될 때까지 대기하지 않습니다. 모듈 3이 나타나지 않으면 모듈 1이 5분 타이머 종료 시 클러스터에 참가하게 되고, 모듈 2 또한 참가하게 되는데(타이머에 아직 2분이 남아 있는 경우에도) 이는 타이머가 완료할 때까지 대기하지 않습니다.

명령 기본값

이 기능은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
cluster group 구성	• 예	• 예	• 예	—	• 예

명령 기록

Release	수정 사항
9.10(1)	명령이 추가되었습니다.

사용 지침

모듈이 다른 모듈보다 훨씬 먼저 참가하는 경우, 다른 모듈이 로드를 아직 공유할 수 없기 때문에 이 모듈은 원하는 트래픽보다 더 많은 트래픽을 받을 수 있습니다.

예

다음 예에서는 모듈 수를 2로 설정하고 최대 지연 시간을 6분으로 설정합니다.

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# unit parallel-join 2 max-bundle-delay 6
```

관련 명령

Command(명령)	설명
cluster group	cluster group 구성 모드를 시작합니다.

unix-auth-gid

UNIX 그룹 ID를 설정하려면 group-policy webvpn 구성 모드에서 **unix-auth-gid** 명령을 사용합니다. 이 명령을 구성에서 제거하려면 이 명령의 **no** 버전을 사용합니다.

unix-auth-gid *identifier*

no storage-objects

구문 설명

identifier	0~4294967294 범위의 정수를 지정합니다.

기본값

기본값은 65534입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
group-policy webvpn 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

문자열은 NetFS(네트워크 파일 시스템) 위치를 지정합니다. SMB 및 FTP 프로토콜만 지원됩니다(예: smb:///(NetFS location) 또는 ftp:///(NetFS location)). 이 위치의 이름은 **storage-objects** 명령에서 사용합니다.

예

다음 예에서는 UNIX 그룹 ID를 4567로 설정합니다.

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 4567
```

관련 명령

Command(명령)	설명
unix-auth-uid	UNIX 사용자 ID를 설정합니다.

unix-auth-uid

UNIX 사용자 ID를 설정하려면 group-policy webvpn 구성 모드에서 **unix-auth-uid** 명령을 사용합니다. 이 명령을 컨피그레이션에서 제거하려면 이 명령의 **no** 버전을 사용합니다.

unix-auth-gid *identifier*

no storage-objects

구문 설명

identifier	0~4294967294 범위의 정수를 지정합니다.

기본값

기본값은 65534입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

문자열은 NetFS(네트워크 파일 시스템) 위치를 지정합니다. SMB 및 FTP 프로토콜만 지원됩니다(예: smb://(NetFS location) 또는 ftp://(NetFS location)). 이 위치의 이름은 **storage-objects** 명령에서 사용합니다.

예

다음 예에서는 UNIX 사용자 ID를 333으로 설정합니다.

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# unix-auth-gid 333
```

관련 명령

Command(명령)	설명
unix-auth-gid	UNIX 그룹 ID를 설정합니다.

지원되지 않음

소프트웨어에서 직접 지원하지 않는 Diameter 요소를 기록하려면 정책 맵 파라미터 구성 모드에서 **unsupported** 명령을 사용합니다. 설정을 제거하려면 이 명령의 **no** 형식을 사용합니다.

unsupported {**application-id** | **avp** | **command-code**} **action log**

no unsupported {**application-id** | **avp** | **command-code**} **action log**

구문 설명

application-id	애플리케이션 ID가 직접 지원되지 않는 Diameter 메시지를 기록합니다.
avp	직접 지원되지 않는 AVP(속성-값 쌍)가 포함된 Diameter 메시지를 기록합니다.
command-code	직접 지원되지 않는 명령 코드가 포함된 Diameter 메시지를 로그에 기록합니다.

기본값

기본값은 요소를 기록하지 않고 허용하는 것입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.5(2)	이 명령이 추가되었습니다.

사용 지침

Diameter 검사 정책 맵을 구성할 때 이 명령을 사용합니다.

이러한 옵션은 소프트웨어에서 직접 지원하지 않는 애플리케이션 ID, 명령 코드 및 AVP를 지정합니다. 기본값은 요소를 기록하지 않고 허용하는 것입니다. 명령을 세 번 입력하여 모든 요소에 대한 기록을 활성화할 수 있습니다.

예

다음 예에서는 지원되지 않는 모든 애플리케이션 ID, 명령 코드 및 AVP를 기록합니다.

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# unsupported application-id action log
ciscoasa(config-pmap-p)# unsupported command-code action log
ciscoasa(config-pmap-p)# unsupported avp action log
```

관련 명령

명령	설명
inspect diameter	Diameter 검사를 활성화합니다.
policy-map type inspect diameter	Diameter 검사 정책 맵을 생성합니다.

upgrade rommon

ASA 5506-X 및 ASA 5508-X 시리즈 보안 어플라이언스를 업그레이드하려면 특권 EXEC 모드에서 **upgrade rommon** 명령을 사용합니다.

upgrade rommon [disk0 | disk1 | flash]:/[*path*] *filename*

구문 설명

disk0:/[*path/*]*filename*	이 옵션은 내부 플래시 메모리을 나타냅니다. 또한 **disk0** 대신 별칭이 지정된 **flash**를 사용할 수도 있습니다.
disk1:/[*path/*]*filename*	이 옵션은 외부 플래시 메모리 카드을 나타냅니다.
flash:/[*path/*]*filename*	이 옵션은 내부 플래시 카드를 나타냅니다. **flash**는 **disk0의 별칭입니다.**

기본값

기본 동작 또는 기본값은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.3(2)	이 명령이 추가되었습니다.

사용 지침

명령에 파일 이름을 제공하면 명령에서 파일을 확인하고 업그레이드를 확인하라는 메시지를 표시합니다. 저장되지 않은 구성 정보가 있는 경우 다시 로드를 시작하기 전에 정보를 저장하라는 프롬프트가 표시됩니다. 확인하면 ASA가 ROMMON으로 전환되고 업그레이드 절차가 시작됩니다.

예

다음 예에서는 ASA 5506-X 및 ASA 5508-X 시리즈 보안 어플라이언스를 업그레이드하는 방법을 보여 줍니다.

```
ciscoasa# upgrade rommon disk0:/kenton_rommon_1-0-19_release.SPA
Verifying file integrity of disk0:/kenton_rommon_1-0-19_release.SPA

Computed Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4

Embedded Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4
```

```
Digital signature successfully validated
File Name                     : disk0:/kenton_rommon_1-0-19_release.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 54232BC5
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

upload-max-size

참고 **upload-max size** 명령은 작동하지 않습니다. 사용하지 마십시오. 그러나 실행 중인 구성에서 이를 확인할 수 있으며 CLI에서 사용할 수 있습니다.

업로드할 개체에 허용되는 최대 크기를 지정하려면 group-policy webvpn 구성 모드에서 **upload-max-size** 명령을 사용합니다. 구성에서 이 개체를 제거하려면 이 명령의 **no** 버전을 사용합니다.

upload-max-size *size*

no upload-max-size

구문 설명

size	업로드한 개체에 허용되는 최대 크기를 지정합니다. 범위는 0부터 2147483647까지입니다.

기본값

기본 크기는 2147483647입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

관련 명령

Command(명령)	설명
post-max-size	게시할 개체의 최대 크기를 지정합니다.
webvpn	group-policy 구성 모드 또는 username 구성 모드에서 사용합니다. webvpn 모드를 시작하여 그룹 정책 또는 사용자 이름을 적용되는 파라미터를 구성할 수 있습니다.
webvpn	전역 구성 모드에서 사용합니다. WebVPN에 대한 전역 설정을 구성할 수 있습니다.

srv-id

reference-identity 개체에서 uri-id를 구성하려면 *ca-reference-identity* 모드에서 **uri-id** 명령을 사용합니다. uri-id를 삭제하려면 이 명령의 **no** 형식을 사용합니다. 먼저 **crypto ca reference-identity**를 입력해 *ca-reference-identity* 모드에 액세스하여 reference-identity 개체를 구성할 수 있습니다.

srv-id *value*

no srv-id *value*

구문 설명

value	각 reference-id의 값입니다.
srv-id	RFC 4985에 정의된 대로 이름 양식이 SRVName인 otherName 유형의 subjectAltName 항목입니다. 도메인 이름 및 애플리케이션 서비스 유형 둘 다 SRV-ID 식별자를 포함할 수 있습니다. 예를 들어, ″_imaps.example.net″ 의 SRV-ID는 "example.net"이라는 DNS 도메인 이름 부분과 ″imaps.″ 라는 애플리케이션 서비스 유형 부분으로 분할됩니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
ca-reference-identity	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.6(2)	이 명령이 도입되었습니다.

사용 지침

참조 ID가 생성되면 4개의 식별자 유형 및 연관된 값이 추가되거나 참조 ID에서 삭제될 수 있습니다.

참조 식별자는 애플리케이션 서비스를 식별하는 정보를 포함할 수 있으며 DNS 도메인 이름을 식별하는 정보를 포함해야 합니다.

예

다음 예에서는 syslog 서버에 대한 reference-identity를 생성합니다.

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

관련 명령

Command(명령)	설명
crypto ca reference-identity	reference-identity 개체를 구성합니다.
cn-id	reference-identity 개체에서 공통 이름 식별자를 구성합니다.
dns-id	reference-identity 개체에서 DNS 도메인 이름 식별자를 구성합니다.
uri id	reference-identity 개체에서 URI 식별자를 구성합니다.
logging host	보안 연결에 reference-identity 개체를 사용할 수 있는 기록 서버를 구성합니다.
call-home profile destination address http	보안 연결에 reference-identity 개체를 사용할 수 있는 Smart Call Home 서버를 구성합니다.

uri-non-sip

Alert-Info 및 Call-Info 헤더 필드에 있는 비 SIP URI를 식별하려면 파라미터 구성 모드에서 **uri-non-sip** 명령을 사용합니다. 파라미터 구성 모드는 정책 맵 구성 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

uri-non-sip action {**mask** | **log**} [**log**}

no uri-non-sip action {**mask** | **log**} [**log**}

구문 설명

log	위반 시 독립형 또는 추가 로그를 지정합니다.
mask	비 SIP URI를 마스킹합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

예

다음 예에서는 SIP 검사 정책 맵에서 Alert-Info 및 Call-Info 헤더 필드에 있는 비 SIP URI를 식별하는 방법을 보여 줍니다.

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# uri-non-sip action log
```

관련 명령

Command(명령)	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	Layer 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

url (crl configure)

CRL을 검색할 정적 URL 목록을 유지하려면 crl configure 구성 모드에서 **url** 명령을 사용합니다. crl configure 구성 모드는 **crypto ca trustpoint** 구성 모드에서 액세스할 수 있습니다. 기존 URL을 삭제하려면 이 명령의 **no** 형식을 사용합니다.

url *index url*

no url *index url*

구문 설명

index	목록에서 각 URL의 순위를 결정하는 값(1~5)을 지정합니다. ASA는 인덱스 1의 URL을 가장 먼저 시도합니다.
url	CRL을 검색할 URL을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
crl configure 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

기존 URL을 덮어쓸 수 없습니다. 기존 URL을 바꾸려면 먼저 이 명령의 **no** 형식을 사용하여 삭제합니다.

예

다음 예에서는 crl 구성 모드를 시작하고 CRL 검색을 위한 URL 목록을 만들고 유지할 인덱스 3을 설정한 다음 CRL을 검색할 URL https://example.com을 구성합니다.

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# url 3 https://example.com
ciscoasa(ca-crl)#
```

관련 명령

Command(명령)	설명
crl configure	ca-crl 구성 모드를 시작합니다.

Command(명령)	설명
crypto ca trustpoint	트러스트 포인트 구성 모드를 시작합니다.
policy	CRL을 검색할 소스를 지정합니다.

url (saml idp)

로그인 또는 로그아웃을 위해 SAML IdP URL을 구성하려면 saml idp 구성 모드에서 **url** 명령을 사용합니다. 먼저 **webvpn** 명령을 입력하여 saml idp 구성 모드에 액세스할 수 있습니다. URL을 제거하려면 이 명령의 **no** 형식을 사용합니다.

url {**sign-in** | **sign-out**} **value** *url*

no url *url*

구문 설명

url	CRL을 검색할 URL을 지정합니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
saml idp 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.5(2)	이 명령이 추가되었습니다.

사용 지침

기존 URL을 덮어쓸 수 없습니다. 기존 URL을 바꾸려면 먼저 이 명령의 **no** 형식을 사용하여 삭제합니다.

url-block

필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답에 사용되는 URL 버퍼를 관리하려면 **url-block** 명령을 사용합니다. 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

구문 설명

block *block_buffer*	필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답을 저장할 HTTP 응답 버퍼를 만듭니다. 허용되는 값은 1550바이트 블록 수를 지정하는 1~128입니다.
mempool-size *memory_pool_size*	URL 버퍼 메모리 풀의 최대 크기(KB)를 구성합니다. 허용되는 값은 2KB에서 10240KB 사이의 URL 버퍼 메모리 풀을 지정하는 2~10240입니다.
url-size *long_url_size*	버퍼링할 각 긴 URL에 허용되는 최대 URL 크기(KB)를 구성합니다. 최대 URL 크기를 지정하는 허용되는 값은 Websense의 경우 2, 3 또는 4(2KB, 3KB 또는 4KB를 나타냄)이고, Secure Computing의 경우 2 또는 3(2KB 또는 3KB를 나타냄)입니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

Websense 필터링 서버의 경우 **url-block url-size** 명령은 최대 4KB의 긴 URL을 허용합니다. Secure Computing의 경우 **url-block url-size** 명령은 최대 3KB의 긴 URL을 허용합니다. Websense 및 N2H2 필터링 서비스 모두에 대해 **url-block block** 명령은 ASA가 URL 필터링 서버의 응답을 기다리는 동안 웹 클라이언트 요청에 대한 응답으로 웹 서버에서 받은 패킷을 버퍼하도록 합니다. 이는 기본 ASA 동작에 비해 웹 클라이언트의 성능을 향상시킵니다. 즉, 패킷을 삭제하고 연결이 허용된 경우 웹 서버에서 패킷을 재전송하도록 합니다.

url-block block 명령을 사용하는 경우 필터링 서버에서 연결을 허용하면 ASA는 HTTP 응답 버퍼에서 웹 클라이언트로 블록을 전송하고 버퍼의 블록을 제거합니다. 필터링 서버에서 연결을 거부하는 경우 ASA는 웹 클라이언트로 거부 메시지를 전송하고 HTTP 응답 버퍼에서 블록을 제거합니다.

url-block block 명령을 사용하여 필터링 서버의 필터링 결정을 기다리는 동안 웹 서버 응답을 버퍼하는 데 사용할 블록 수를 지정할 수 있습니다.

url-block url-size 명령을 **url-block mempool-size** 명령과 함께 사용하여 필터링할 URL의 최대 길이 및 URL 버퍼에 할당한 최대 메모리를 지정할 수 있습니다. 이러한 명령을 사용하여 1159바이트보다 긴(최대 4096바이트) URL을 Websense 또는 Secure-Computing 서버로 전달할 수 있습니다. **url-block url-size** 명령은 1159바이트보다 긴 URL을 버퍼에 저장한 다음 Websense 또는 Secure-Computing 서버가 URL을 허용하거나 거부할 수 있도록 TCP 패킷 스트림을 통해 Websense 또는 Secure-Computing 서버로 URL을 전달합니다.

예

다음 예에서는 URL 필터링 서버의 응답을 버퍼하도록 56개의 1550바이트 블록을 할당합니다.

```
ciscoasa#(config)# url-block block 56
```

관련 명령

명령	설명
clear url-block block statistics	블록 버퍼 사용 카운터를 지웁니다.
filter url	URL 필터링 서버로 트래픽을 전송합니다.
show url-block	N2H2 필터 또는 Websense 필터링 서버의 응답을 기다리는 동안 URL을 버퍼하는 데 사용되는 URL 캐시에 대한 정보를 표시합니다.
url-cache	N2H2 또는 Websense 서버에서 응답이 보류 중인 동안 URL 캐싱을 활성화하고 캐시 크기를 설정합니다.
url-server	**filter** 명령에서 사용할 N2H2 또는 Websense 서버를 식별합니다.

url-cache

Websense 서버에서 받은 URL 응답에 대한 URL 캐싱을 활성화하고 캐시 크기를 설정하려면 전역 구성 모드에서 **url-cache** 명령을 사용합니다. 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

no url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

구문 설명

dst	URL 수신 주소를 기반으로 항목을 캐시합니다. 모든 사용자가 Websense 서버에서 동일한 URL 필터링 정책을 공유하는 경우 이 모드를 선택합니다.
size *kbytes*	캐시 크기의 값을 1~128KB 내에서 지정합니다.
src_dst	URL 요청을 시작하는 소스 주소와 URL 수신 주소 둘 다를 기반으로 항목을 캐시합니다. 사용자가 Websense 서버에서 동일한 URL 필터링 정책을 공유하지 않는 경우 이 모드를 선택합니다.
statistics	캐시 조회 및 적중률 수를 포함하여 추가 URL 캐시 통계를 표시하려면 **statistics** 옵션을 사용합니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

url-cache 명령은 URL 서버의 응답을 캐시할 수 있는 구성 옵션을 제공합니다.

url-cache 명령을 사용하여 URL 캐싱을 활성화하고, 캐시 크기를 설정하고, 캐시 통계를 표시할 수 있습니다.

참고 N2H2 서버 애플리케이션은 URL 필터링에 이 명령을 지원하지 않습니다.

캐싱은 ASA의 메모리에 URL 액세스 권한을 저장합니다. 호스트가 연결을 요청하면 ASA는 Websense 서버로 요청을 전달하는 대신 먼저 URL 캐시에서 일치하는 액세스 권한을 조회합니다. **no url-cache** 명령을 사용하여 캐싱을 비활성화할 수 있습니다.

참고 Websense 서버에서 설정을 변경한 경우 **no url-cache** 명령을 사용하여 캐시를 비활성화한 다음 **url-cache** 명령을 사용하여 캐시를 다시 활성화합니다.

URL 캐시를 사용해도 Websense 프로토콜 버전 1에 대한 Websense 어카운트 관리 로그는 업데이트되지 않습니다. Websense 프로토콜 버전 1을 사용하는 경우 Websense 실행 시 로그가 누적되도록 두면 Websense 어카운트 관리 정보를 볼 수 있습니다. 보안 요구 사항에 맞는 사용 프로파일을 받은 후 **url-cache**를 활성화하여 처리량을 늘립니다. 어카운트 관리 로그는 **url-cache** 명령을 사용하는 동안 Websense 프로토콜 버전 4 URL 필터링에 대해 업데이트됩니다.

예

다음 예에서는 소스 및 수신 주소를 기반으로 모든 아웃바운드 HTTP 연결을 캐시합니다.

```
ciscoasa(config)# url-cache src_dst 128
```

관련 명령

명령	설명
clear url-cache statistics	구성에서 **url-cache** 명령문을 제거합니다.
filter url	URL 필터링 서버로 트래픽을 전송합니다.
show url-cache statistics	Websense 필터링 서버에서 받은 URL 응답에 사용되는 URL 캐시에 대한 정보를 표시합니다.
url-server	**filter** 명령에서 사용할 Websense 서버를 식별합니다.

url-entry

포털 페이지에서 HTTP/HTTPS URL을 입력할 수 있는 기능을 활성화하거나 비활성화하려면 dap webvpn 구성 모드에서 **url-entry** 명령을 사용합니다.

url-entry enable | disable

enable | disable	파일 서버 또는 공유를 찾아볼 수 있는 기능을 활성화하거나 비활성화합니다.

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
dap webvpn 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

예

다음 예에서는 Finance라는 DAP 레코드에 대한 URL 항목을 활성화하는 방법을 보여 줍니다.

```
ciscoasa (config) config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# url-entry enable
```

관련 명령

Command(명령)	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
file-entry	액세스할 파일 서버 이름을 입력할 수 있는 기능을 활성화하거나 비활성화합니다.

url-length-limit

RTSP 메시지에서 허용되는 URL의 최대 길이를 구성하려면 파라미터 구성 모드에서 **url-length-limit** 명령을 사용합니다. 파라미터 구성 모드는 정책 맵 구성 모드에서 액세스할 수 있습니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

url-length-limit *length*

no url-length-limit *length*

구문 설명

length	URL 길이 제한(바이트)입니다. 범위는 0~6000입니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

예

다음 예에서는 RTSP 검사 정책 맵에서 URL 길이 제한을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# url-length-limit 50
```

관련 명령

Command(명령)	설명
class	정책 맵에서 클래스 맵 이름을 식별합니다.
class-map type inspect	애플리케이션에 특정한 트래픽과 일치시킬 검사 클래스 맵을 생성합니다.
policy-map	Layer 3/4 정책 맵을 생성합니다.
show running-config policy-map	모든 현재 정책 맵 구성을 표시합니다.

url-list

특정 사용자 또는 그룹 정책에 WebVPN 서버 및 URL 목록을 적용하려면 group-policy webvpn 구성 모드 또는 username webvpn 구성 모드에서 **url-list** 명령을 사용합니다. **url-list none** 명령을 사용하여 만든 null 값을 포함하여 목록을 제거하려면 이 명령의 **no** 형식을 사용합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다. URL 목록을 상속하지 못하도록 하려면 **url-list none** 명령을 사용합니다. 명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

url-list {**value** *name* | **none**} [*index*]

no url-list

구문 설명

index	홈 페이지에서의 표시 우선순위를 나타냅니다.
none	URL 목록에 대해 null 값을 설정합니다. 기본 또는 지정된 그룹 정책에서 목록을 상속받는 것을 방지합니다.
value *name*	이전에 구성된 URL 목록의 이름을 지정합니다. 이러한 목록을 구성하려면 전역 구성 모드에서 **url-list** 명령을 사용합니다.

기본값

기본 URL 목록은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
group-policy webvpn 컨피그레이션	• 예	—	• 예	—	—
username 컨피그레이션	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

명령을 한 번 더 사용하면 이전 설정이 재정의됩니다.

webvpn 모드에서 **url-list** 명령을 사용하여 사용자 또는 그룹 정책에 대해 WebVPN 홈 페이지에 표시할 URL 목록을 식별하려면 먼저 XML 개체를 통해 목록을 만들어야 합니다. 전역 구성 모드에서 **import** 명령을 사용하여 URL 목록을 보안 어플라이언스로 다운로드합니다. 그런 다음 url-list 명령을 사용하여 특정 그룹 정책 또는 사용자에게 목록을 적용합니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 FirstGroupURLs라는 URL 목록을 적용한 후 URL 목록 중 첫 번째 위치에 이 목록을 할당합니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# url-list value FirstGroupURLs 1
```

관련 명령

Command(명령)	설명
clear configure url-list	구성에서 모든 url-list 명령을 제거합니다. 목록 이름이 포함된 경우 ASA는 해당 목록에 대한 명령만 제거합니다.
show running-configuration url-list	현재 구성된 **url-list** 명령 집합을 표시합니다.
webvpn	webvpn 모드를 시작할 수 있도록 합니다. 이는 webvpn 구성 모드, group-policy webvpn 구성 모드(특정 그룹 정책에 대한 webvpn 설정 구성) 또는 username webvpn 구성 모드(특정 사용자에 대한 webvpn 설정 구성)일 수 있습니다.

url-server

filter 명령에 사용할 N2H2 또는 Websense 서버를 식별하려면 전역 구성 모드에서 **url-server** 명령을 사용합니다. 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

N2H2

url-server [(*if_name*)] **vendor** {**smartfilter** | **n2h2**} **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** [connections *number*]} | **UDP**]

no url-server [(*if_name*)] **vendor** {**smartfilter** | **n2h2**} **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** [**connections** *number*]} | **UDP**]

Websense

url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

구문 설명

N2H2

connections	허용되는 최대 TCP 연결 수를 제한합니다.
num_conns	보안 어플라이언스에서 만든 최대 TCP 연결 수를 URL 서버에 지정합니다. 이 수치는 서버당 지정되므로 서버마다 연결 값이 다를 수 있습니다.
host *local_ip*	URL 필터링 애플리케이션을 실행하는 서버입니다.
if_name	(선택 사항) 인증 서버가 상주하는 네트워크 인터페이스입니다. 지정하지 않은 경우 기본값은 inside입니다.
port *number*	N2H2 서버 포트입니다. 또한 ASA는 이 포트에서 UDP 응답을 수신 대기합니다. 기본 포트 번호는 4005입니다.
protocol	프로토콜은 **TCP** 또는 **UDP** 키워드를 사용하여 구성할 수 있습니다. 기본값은 TCP입니다.
timeout *seconds*	ASA가 지정한 다음 서버로 전환하기 전에 허용되는 최대 유휴 시간입니다. 기본값은 30초입니다.
vendor	URL 필터링 서비스('smartfilter' 또는 'n2h2' (이전 버전과의 호환성용)) 를 나타냅니다. 'smartfilter' 는 공급업체 문자열로 저장됩니다.

Websense

connections	허용되는 최대 TCP 연결 수를 제한합니다.
num_conns	보안 어플라이언스에서 만든 최대 TCP 연결 수를 URL 서버에 지정합니다. 이 수치는 서버당 지정되므로 서버마다 연결 값이 다를 수 있습니다.
host *local_ip*	URL 필터링 애플리케이션을 실행하는 서버입니다.
if_name	인증 서버가 상주하는 네트워크 인터페이스입니다. 지정하지 않은 경우 기본값은 inside입니다.

timeout *seconds*	ASA가 지정한 다음 서버로 전환하기 전에 허용되는 최대 유휴 시간입니다. 기본값은 30초입니다.
protocol	프로토콜은 **TCP** 또는 **UDP** 키워드를 사용하여 구성할 수 있습니다. 기본값은 TCP 프로토콜 버전 1입니다.
vendor websense	URL 필터링 서비스 공급업체가 Websense임을 나타냅니다.
version	프로토콜 버전 **1** 또는 **4**를 지정합니다. 기본값은 TCP 프로토콜 버전 1입니다. TCP는 버전 1 또는 버전 4를 사용하여 구성할 수 있습니다. UDP는 버전 4만 사용하여 구성할 수 있습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

url-server 명령은 N2H2 또는 Websense URL 필터링 애플리케이션을 실행하는 서버를 지정합니다. 단일 컨텍스트 모드의 경우 16개의 URL 서버로 제한되고, 다중 모드의 경우 4개의 URL 서버로 제한됩니다. 그러나 한 번에 하나의 애플리케이션(N2H2 또는 Websense)만 사용할 수 있습니다. 또한 ASA에서 구성을 변경해도 애플리케이션 서버의 구성은 업데이트되지 않습니다. 공급업체 지침에 따라 개별적으로 업데이트해야 합니다.

HTTPS 및 FTP에 대해 **filter** 명령을 실행하기 전에 **url-server** 명령을 구성해야 합니다. 모든 URL 서버가 서버 목록에서 제거되면 URL 필터링과 관련된 모든 **filter** 명령도 제거됩니다.

서버를 지정한 후에는 **filter url** 명령을 사용하여 URL 필터링 서비스를 활성화합니다.

show url-server statistics 명령을 사용하여 연결할 수 없는 서버를 비롯한 서버 통계 정보를 볼 수 있습니다.

다음 단계에 따라 URL을 필터링합니다.

단계 1 적절한 형식의 공급업체 관련 **url-server** 명령으로 URL 필터링 애플리케이션 서버를 지정합니다.

단계 2 **filter** 명령으로 URL 필터링을 활성화합니다.

단계 3 (선택 사항) **url-cache** 명령으로 URL 캐싱을 활성화하여 인지된 응답 시간을 향상시킵니다.

단계 4 (선택 사항) **url-block** 명령을 사용하여 긴 URL 및 HTTP 버퍼링 지원을 활성화합니다.

단계 5 **show url-block block statistics**, **show url-cache statistics** 또는 **show url-server statistics** 명령을 사용하여 실행 정보를 볼 수 있습니다.

N2H2 기준 필터링에 대한 자세한 내용은 다음 N2H2 웹사이트를 참고하십시오.

http://www.n2h2.com

Websense 필터링 서비스에 대한 자세한 내용은 다음 웹사이트를 참고하십시오.

http://www.websense.com/

예

다음 예에서는 N2H2를 사용하여 10.0.2.54 호스트의 연결을 제외한 모든 아웃바운드 HTTP 연결을 필터링합니다.

```
ciscoasa(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

다음 예에서는 Websense를 사용하여 10.0.2.54 호스트의 연결을 제외한 모든 아웃바운드 HTTP 연결을 필터링합니다.

```
ciscoasa(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

관련 명령

명령	설명
clear url-server	URL 필터링 서버 통계를 지웁니다.
filter url	URL 필터링 서버로 트래픽을 전송합니다.
show url-block	N2H2 또는 Websense 필터링 서버에서 받은 URL 응답에 사용되는 URL 캐시에 대한 정보를 표시합니다.
url-cache	N2H2 또는 Websense 서버에서 응답이 보류 중인 동안 URL 캐싱을 활성화하고 캐시 크기를 설정합니다.

urgent-flag

TCP 노멀라이저를 통한 URG 포인터를 허용하거나 제거하려면 tcp-map 구성 모드에서 **urgent-flag** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

구문 설명

allow	TCP 노멀라이저를 통한 URG 포인터를 허용합니다.
clear	TCP 노멀라이저를 통한 URG 포인터를 지웁니다.

기본값

긴급 플래그 및 긴급 오프셋은 기본적으로 지워집니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
tcp-map 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용됩니다. **class-map** 명령을 사용하여 트래픽의 클래스를 정의하고, **tcp-map** 명령을 사용하여 TCP 검사를 맞춤 설정합니다. **policy-map** 명령을 사용하여 새 TCP 맵을 적용합니다. **service-policy** 명령을 사용하여 TCP 검사를 활성화합니다.

tcp-map 명령을 사용하여 tcp-map 구성 모드를 시작할 수 있습니다. tcp-map 구성 모드에서 **urgent-flag** 명령을 사용하여 긴급 플래그를 허용할 수 있습니다.

URG 플래그는 스트림 내의 다른 데이터보다 우선순위가 높은 정보가 패킷에 포함되어 있음을 나타내는 데 사용됩니다. TCP RFC는 URG 플래그의 정확한 해석이 모호하므로 종단 시스템에서는 다른 방식으로 긴급 오프셋을 처리하며, 이로 인해 공격에 취약해질 수 있습니다. 기본 동작은 URG 플래그 및 오프셋을 지우는 것입니다.

예

다음 예에서는 긴급 플래그를 허용하는 방법을 보여 줍니다.

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 513
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

Command(명령)	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 구성 모드에 대한 액세스를 허용합니다.

user

ID 방화벽 기능을 지원하는 사용자 그룹 개체에서 사용자를 만들려면 user-group object 구성 모드에서 **user** 명령을 사용합니다. 개체에서 사용자를 제거하려면 이 명령의 **no** 형식을 사용합니다.

user [***domain_nickname***\]***user_name***

[no] user [***domain_nickname***\]***user_name***

구문 설명

domain_nickname	(선택 사항) 사용자를 추가할 도메인을 지정합니다.
user_name	사용자의 이름을 지정합니다. 사용자 이름은 [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.] 버튼을 클릭합니다. 사용자 이름에 공백이 포함된 경우 따옴표로 이름을 묶어야 합니다. **user** 키워드를 사용하여 지정한 *user_name* 인수는 ASCII 사용자 이름을 포함하며, IP 주소를 지정하지 않습니다.

기본값

domain_nickname 인수를 지정하지 않으면 ID 방화벽 기능에 대해 구성된 LOCAL 도메인에 사용자가 생성됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
object-group user 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

ASA는 Active Directory 도메인 컨트롤러에 정의된 사용자 그룹에 대한 LDAP 쿼리를 Active Directory 서버로 전송합니다. ASA는 ID 방화벽 기능을 위해 이러한 그룹을 가져옵니다. 그러나 ASA에 전역으로 정의되지 않고 현지화된 보안 정책이 적용되는 로컬 사용자 그룹이 필요한 현지화된 네트워크 리소스가 있을 수 있습니다. 로컬 사용자 그룹은 Active Directory에서 가져온 중첩된 그룹 및 사용자 그룹을 포함할 수 있습니다. ASA는 로컬 및 Active Directory 그룹을 통합합니다. 사용자는 로컬 사용자 그룹 및 Active Directory에서 가져온 사용자 그룹에 속할 수 있습니다.

ASA는 최대 256개의 사용자 그룹(가져온 사용자 그룹 및 로컬 사용자 그룹 포함)을 지원합니다.

액세스 그룹, 캡처 또는 서비스 정책에 포함하면 사용자 그룹 개체가 활성화됩니다.

사용자 그룹 개체 내에서 다음 개체 유형을 정의할 수 있습니다.

- **User** - object-group user에 단일 사용자를 추가합니다. 이 사용자는 LOCAL 사용자 또는 가져온 사용자일 수 있습니다.

가져온 사용자의 이름은 고유하지 않을 수 있는 CN(공통 이름)이 아니라 고유한 sAMAccountName이어야 합니다. 그러나 일부 Active Directory 서버 관리자는 sAMAccountName과 CN이 동일하도록 요구할 수도 있습니다. 이 경우 ASA가 **show user-identity ad-group-member** 명령의 출력에 표시하는 CN을 사용자 개체에서 정의된 가져온 사용자에 사용할 수 있습니다.

- **User-group** - Microsoft Active Directory 서버와 같은 외부 디렉터리 서버에서 정의된 가져온 사용자 그룹을 group-object user에 추가합니다.

  사용자 그룹의 그룹 이름은 고유하지 않을 수 있는 CN(공통 이름)이 아니라 고유한 sAMAccountName이어야 합니다. 그러나 일부 Active Directory 서버 관리자는 sAMAccountName과 CN이 동일하도록 요구할 수도 있습니다. 이 경우 ASA가 **show user-identity ad-group-member** command 명령의 출력에 표시하는 CN을 **user-group** 키워드로 지정된 *user_group_name* 인수에서 사용할 수 있습니다.

  참고 먼저 개체에서 지정하지 않고 사용자 그룹 개체 내에서 *domain_nickname**user_group_name* 또는 *domain_nickname**user_ name*을 직접 추가할 수 있습니다. *domain_nickname*이 AAA 서버와 연결된 경우 ASA는 사용자 개체 그룹이 활성화되면 Microsoft Active Directory 서버와 같은 외부 디렉터리 서버에 정의된 자세한 중첩된 사용자 그룹 및 사용자를 ASA로 가져옵니다.

- **Group-object** - ASA에서 로컬로 정의된 그룹을 object-group user에 추가합니다.

  참고 object-group user 개체 내에 개체 그룹을 포함하면 ASA는 ACL 최적화를 활성화한 경우에도 액세스 그룹에서 개체 그룹을 확장하지 않습니다. **show object-group** 명령의 출력에 적중 횟수가 표시되지 않습니다. 적중 횟수는 ACL 최적화가 활성화된 경우 일반 네트워크 개체 그룹에만 사용할 수 있습니다.

- **Description** - object-group user에 대한 설명을 추가합니다.

예

다음 예에서는 **user** 명령을 **user-group object** 명령과 함께 사용하여 ID 방화벽 기능에서 사용할 사용자 그룹 개체에서 사용자를 추가하는 방법을 보여 줍니다.

```
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 CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\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 CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

관련 명령

Command(명령)	설명
description	**object-group user** 명령으로 생성한 그룹에 설명을 추가합니다.
group-object	ID 방화벽 기능에서 사용하기 위해 **object-group user** 명령으로 만든 사용자 개체 그룹에 로컬로 정의된 개체 그룹을 추가합니다.
object-group user	ID 방화벽 기능을 위해 사용자 그룹 개체를 생성합니다.

Command(명령)	설명
user-group	Microsoft Active Directory에서 가져온 사용자 그룹 **object-group user** 명령으로 만든 그룹에 추가합니다.
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

user-alert

현재 활성 세션의 모든 클라이언트리스 SSL VPN 사용자에 대해 긴급 메시지 브로드캐스트를 활성화하려면 특권 EXEC 모드에서 **user-alert** 명령을 사용합니다. 메시지를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

user-alert *string cancel*

no user-alert

구문 설명

cancel	팝업 브라우저 창 시작을 취소합니다.
string	영숫자입니다.

기본값

메시지가 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

이 명령을 실행하면 엔드 유저에게 구성된 메시지가 포함된 팝업 브라우저 창이 표시됩니다. 이 명령을 사용해도 ASA 구성 파일은 변경되지 않습니다.

예

다음 예에서는 DAP 추적 디버깅을 활성화하는 방법을 보여 줍니다.

```
ciscoasa # We will reboot the security appliance at 11:00 p.m. EST time. We apologize for
any inconvenience.
ciscoasa #
```

user-authentication

사용자 인증을 활성화하려면 group-policy 구성 모드에서 **user-authentication enable** 명령을 사용합니다. 사용자 인증을 비활성화하려면 **user-authentication disable** 명령을 사용합니다. 실행 중인 구성에서 사용자 인증 속성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션을 사용하면 다른 그룹 정책에서 사용자 인증을 위한 값을 상속받을 수 있습니다.

활성화되어 있는 경우, 사용자 인증을 하려면 하드웨어 클라이언트 뒤에 있는 개별 사용자가 인증하여 터널을 통과하는 네트워크에 대한 액세스 권한을 획득해야 합니다.

user-authentication {**enable | disable**}

no user-authentication

구문 설명

disable	사용자 인증을 비활성화합니다.
enable	사용자 인증을 활성화합니다.

기본값

사용자 인증은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

개별 사용자는 구성된 인증 서버의 순서에 따라 인증됩니다.

1차 ASA에서 사용자 인증이 필요한 경우, 모든 백업 서버에서도 이를 구성했는지 확인하십시오.

예

다음 예는 이름이 "FirstGroup" 인 그룹 정책에 대해 사용자 인증을 활성화하는 방법을 보여줍니다.

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

관련 명령

Command(명령)	설명
ip-phone-bypass	IP 전화기가 사용자 인증 없이 연결되도록 합니다. 보안 디바이스 인증은 그대로 적용됩니다.
leap-bypass	VPN 클라이언트 뒤에 있는 무선 장치의 LEAP 패킷이 사용자 인증(활성화된 경우) 전에 VPN 터널을 통과하도록 합니다. 이를 통해 Cisco 무선 액세스 포인트 디바이스를 사용하는 워크스테이션에서 LEAP 인증을 설정할 수 있습니다. 그런 다음 사용자 인증 시마다 다시 인증합니다.
secure-unit-authentication	VPN 클라이언트가 터널을 시작할 때마다 사용자 이름 및 비밀번호로 인증하도록 함으로써 보안을 강화합니다.
user-authentication-idle-timeout	개별 사용자에 대한 유휴 시간 제한을 설정합니다. 유휴 시간 제한 동안 사용자 연결에서 통신 활동이 없는 경우 ASA는 연결을 종료합니다.

user-authentication-idle-timeout

하드웨어 클라이언트 뒤에 있는 개별 사용자에 대한 유휴 시간 제한을 설정하려면 group-policy 구성 모드에서 **user-authentication-idle-timeout** 명령을 사용합니다. 유휴 시간 제한 값을 삭제하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션을 사용하면 다른 그룹 정책에서 유휴 시간 제한 값을 상속받을 수 있습니다. 유휴 시간 제한 값을 상속하지 못하도록 하려면 **user-authentication-idle-timeout none** 명령을 사용합니다.

유휴 시간 제한 동안 하드웨어 클라이언트 뒤에 있는 개별 사용자의 통신 활동이 없는 경우 ASA는 연결을 종료합니다.

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

구문 설명

minutes	유휴 시간 제한에서 분 수를 지정합니다. 범위는 1~35791394분입니다.
none	무제한 유휴 시간 제한을 허용합니다. 유휴 시간 제한을 null 값으로 설정하여 유휴 시간 제한을 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 사용자 인증 유휴 시간 제한 값을 상속하지 못하도록 합니다.

기본값

30분입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

최소값은 1 분이고, 기본값은 30분이며, 최대값은 10,080분입니다.

이 타이머는 VPN 터널 자체가 아니라 VPN 터널을 통한 클라이언트 액세스만 종료합니다.

show uauth 명령에 대한 응답으로 표시되는 유휴 시간 제한은 항상 Cisco Easy VPN 원격 디바이스의 터널에 인증된 사용자의 유휴 시간 제한 값입니다.

예

다음 예에서는 ″FirstGroup″ 이라는 그룹 정책에 대한 유휴 시간 제한 값을 45분으로 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# user-authentication-idle-timeout 45
```

관련 명령

Command(명령)	설명
user-authentication	하드웨어 클라이언트 뒤에 있는 사용자가 연결하기 전에 ASA에 자신을 식별해야 합니다.

user-group

ID 방화벽 기능에서 사용하기 위해 **object-group user** 명령으로 만든 그룹에 Microsoft Active Directory 가져온 사용자 그룹을 추가하려면 **user-group object** 구성 모드에서 **user-group** 명령을 사용합니다. 개체에서 사용자 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-group [***domain_nickname***\]***user_group_name***

[no] user-group [***domain_nickname***\]***user_group_name***

구문 설명

domain_nickname	(선택 사항) 사용자 그룹을 생성할 도메인을 지정합니다.
user_group_name	사용자 그룹의 이름을 지정합니다. 그룹 이름은 [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.] 버튼을 클릭합니다. 그룹 이름에 공백이 포함된 경우 따옴표로 이름을 묶어야 합니다.

기본값

domain_nickname 인수를 지정하지 않으면 ID 방화벽 기능에 대해 구성된 LOCAL 도메인에 사용자 그룹이 생성됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
object-group user 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

ASA는 Active Directory 도메인 컨트롤러에 정의된 사용자 그룹에 대한 LDAP 쿼리를 Active Directory 서버로 전송합니다. ASA는 ID 방화벽 기능을 위해 이러한 그룹을 가져옵니다. 그러나 ASA에 전역으로 정의되지 않고 현지화된 보안 정책이 적용되는 로컬 사용자 그룹이 필요한 현지화된 네트워크 리소스가 있을 수 있습니다. 로컬 사용자 그룹은 Active Directory에서 가져온 중첩된 그룹 및 사용자 그룹을 포함할 수 있습니다. ASA는 로컬 및 Active Directory 그룹을 통합합니다. 사용자는 로컬 사용자 그룹 및 Active Directory에서 가져온 사용자 그룹에 속할 수 있습니다.

ASA는 최대 256개의 사용자 그룹(가져온 사용자 그룹 및 로컬 사용자 그룹 포함)을 지원합니다.

액세스 그룹, 캡처 또는 서비스 정책에 포함하면 사용자 그룹 개체가 활성화됩니다.

사용자 그룹 개체 내에서 다음 개체 유형을 정의할 수 있습니다.

- **User** - object-group user에 단일 사용자를 추가합니다. 이 사용자는 LOCAL 사용자 또는 가져온 사용자일 수 있습니다.

가져온 사용자의 이름은 고유하지 않을 수 있는 CN(공통 이름)이 아니라 고유한 sAMAccountName이어야 합니다. 그러나 일부 Active Directory 서버 관리자는 sAMAccountName과 CN이 동일하도록 요구할 수도 있습니다. 이 경우 ASA가 **show user-identity ad-group-member** 명령의 출력에 표시하는 CN을 사용자 개체에서 정의된 가져온 사용자에 사용할 수 있습니다.

- **User-group** - Microsoft Active Directory 서버와 같은 외부 디렉터리 서버에서 정의된 가져온 사용자 그룹을 group-object user에 추가합니다.

  사용자 그룹의 그룹 이름은 고유하지 않을 수 있는 CN(공통 이름)이 아니라 고유한 sAMAccountName이어야 합니다. 그러나 일부 Active Directory 서버 관리자는 sAMAccountName과 CN이 동일하도록 요구할 수도 있습니다. 이 경우 ASA가 **show user-identity ad-group-member** command 명령의 출력에 표시하는 CN을 **user-group** 키워드로 지정된 *user_group_name* 인수에서 사용할 수 있습니다.

  참고 먼저 개체에서 지정하지 않고 사용자 그룹 개체 내에서 *domain_nickname**user_group_name* 또는 *domain_nickname**user_ name*을 직접 추가할 수 있습니다. *domain_nickname*이 AAA 서버와 연결된 경우 ASA는 사용자 개체 그룹이 활성화되면 Microsoft Active Directory 서버와 같은 외부 디렉토리 서버에 정의된 자세한 중첩된 사용자 그룹 및 사용자를 ASA로 가져옵니다.

- **Group-object** - ASA에서 로컬로 정의된 그룹을 object-group user에 추가합니다.

  참고 object-group user 개체 내에 개체 그룹을 포함하면 ASA는 ACL 최적화를 활성화한 경우에도 액세스 그룹에서 개체 그룹을 확장하지 않습니다. **show object-group** 명령의 출력에 적중 횟수가 표시되지 않습니다. 적중 횟수는 ACL 최적화가 활성화된 경우 일반 네트워크 개체 그룹에만 사용할 수 있습니다.

- **Description** - object-group user에 대한 설명을 추가합니다.

예

다음 예에서는 **user-group** 명령을 **user-group object** 명령과 함께 사용하여 ID 방화벽 기능에서 사용할 사용자 그룹 개체에서 사용자를 추가하는 방법을 보여 줍니다.

```
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 CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\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 CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

관련 명령

Command(명령)	설명
description	**object-group user** 명령으로 생성한 그룹에 설명을 추가합니다.
group-object	ID 방화벽 기능에서 사용하기 위해 **object-group user** 명령으로 만든 사용자 개체 그룹에 로컬로 정의된 개체 그룹을 추가합니다.
object-group user	ID 방화벽 기능을 위해 사용자 그룹 개체를 만듭니다.

Command(명령)	설명
user	**object-group user** 명령으로 만든 개체 그룹에 사용자를 추가합니다.
user-identity enable	Cisco ID 방화벽 인스턴스를 생성합니다.

user-identity action ad-agent-down

Active Directory 에이전트가 응답하지 않을 때의 Cisco ID 방화벽 인스턴스에 대한 동작을 설정하려면 전역 구성 모드에서 **user-identity action ad-agent-down** 명령을 사용합니다. ID 방화벽 인스턴스에 대한 이 동작을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity action ad-agent-down disable-user-identity-rule

no user-identity action ad-agent-down disable-user-identity-rule

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 이 명령은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

AD 에이전트가 응답하지 않을 때의 동작을 지정합니다.

user-identity action ad-agent-down 명령이 구성된 경우 AD 에이전트의 작동이 중지되면 ASA는 해당 도메인의 사용자와 연결된 사용자 ID 규칙을 비활성화합니다. 또한 해당 도메인의 모든 사용자 IP 주소에 대한 상태가 **show user-identity user** 명령의 출력에 비활성화된 것으로 표시됩니다.

예

다음 예에서는 ID 방화벽에 대한 이 동작을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity action ad-agent-down disable-user-identity-rule
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity action domain-controller-down

Active Directory 도메인 컨트롤러의 작동이 중지되었을 때의 Cisco ID 방화벽 인스턴스에 대한 동작을 설정하려면 전역 구성 모드에서 **user-identity action domain-controller-down** 명령을 사용합니다. 이 동작을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity action domain-controller-down *domain_nickname*
disable-user-identity-rule

no user-identity action domain-controller-down ***domain_nickname***
disable-user-identity-rule

구문 설명

domain_nickname	ID 방화벽에 대한 도메인 이름을 지정합니다.

기본값

기본적으로 이 명령은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

Active Directory 도메인 컨트롤러가 응답하지 않아 도메인의 작동이 중지된 경우의 동작을 지정합니다.

disable-user-identity-rule 키워드가 구성된 경우 도메인의 작동이 중지되면 ASA는 해당 도메인에 대해 사용자 ID-IP 주소 매핑을 비활성화합니다. 또한 해당 도메인의 모든 사용자 IP 주소에 대한 상태가 **show user-identity user** 명령의 출력에 비활성화된 것으로 표시됩니다.

예

다음 예에서는 ID 방화벽에 대한 이 동작을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity action domain-controller-down SAMPLE
disable-user-identity-rule
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity action mac-address-mismatch

사용자의 MAC 주소가 ASA 장치 IP 주소와 일치하지 않을 때의 Cisco ID 방화벽 인스턴스에 대한 동작을 설정하려면 전역 구성 모드에서 **user-identity action mac-address mismatch** 명령을 사용합니다. 이 동작을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity action mac-address mismatch remove-user-ip

no user-identity action mac-address mismatch remove-user-ip

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

이 명령을 지정한 경우 ASA는 기본적으로 **remove-user-ip**를 사용합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

사용자의 MAC 주소가 현재 해당 MAC 주소에 매핑된 ASA 장치 IP 주소와 일치하지 않을 때의 동작을 지정합니다. 이 동작은 사용자 ID 규칙의 효과를 비활성화합니다.

user-identity action mac-address-mismatch 명령을 구성한 경우 ASA는 해당 클라이언트에 대해 사용자 ID-IP 주소 매핑을 제거합니다.

예

다음 예에서는 ID 방화벽을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity action mac-address-mismatch remove-user-ip
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity action netbios-response-fail

클라이언트가 Cisco ID 방화벽 인스턴스에 대한 NetBIOS 프로브에 응답하지 않을 때의 동작을 설정하려면 전역 구성 모드에서 **user-identity action netbios-response-fail** 명령을 사용합니다. 이 동작을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity action netbios-response-fail remove-user-ip

no user-identity action netbios-response-fail remove-user-ip

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 이 명령은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

클라이언트가 NetBIOS 프로브에 응답하지 않을 때의 동작을 지정합니다. 예를 들어 해당 클라이언트에 대한 네트워크 연결이 차단되거나 클라이언트가 활성 상태가 아닐 수 있습니다.

user-identity action remove-user-ip 명령을 구성한 경우 ASA는 해당 클라이언트에 대해 사용자 ID-IP 주소 매핑을 제거합니다.

예

다음 예에서는 ID 방화벽을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity action netbios-response-fail remove-user-ip
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity ad-agent aaa-server

Cisco ID 방화벽 인스턴스에 대한 AD 에이전트의 서버 그룹을 정의하려면 AAA 서버 호스트 구성 모드에서 **user-identity ad-agent aaa-server** 명령을 사용합니다. 이 동작을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*

no user-identity user-identity ad-agent aaa-server ***aaa_server_group_tag***

구문 설명

aaa_server_group_tag	ID 방화벽과 연결된 AAA 서버 그룹을 지정합니다.

기본값

이 명령에는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
aaa-server-host 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

aaa_server_group_tag 변수에 정의된 첫 번째 서버는 기본 AD 에이전트이고, 두 번째 서버는 보조 AD 에이전트입니다.

ID 방화벽은 두 개의 AD 에이전트 호스트만 정의하도록 지원합니다.

보조 에이전트가 지정된 경우 ASA는 기본 AD 에이전트의 작동이 중지된 것을 탐지하면 보조 AD 에이전트로 전환합니다. AD 에이전트의 AAA 서버는 RADIUS를 통신 프로토콜로 사용하며, ASA와 AD 에이전트 간의 공유 암호에 대한 키 특성을 지정해야 합니다.

예

다음 예에서는 ID 방화벽에 대한 AD 에이전트 AAA 서버 호스트를 정의하는 방법을 보여 줍니다.

```
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity ad-agent active-user-database

ASA가 Cisco ID 방화벽 인스턴스의 AD 에이전트에서 사용자 ID-IP 주소 매핑 정보를 검색하는 방법을 정의하려면 전역 구성 모드에서 **user-identity ad-agent active-user-database** 명령을 사용합니다. 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity ad-agent active-user-database {**on-demand** | **full-download**}

no user-identity ad-agent active-user-database {**on-demand** | **full-download**}

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 ASA 5505에서는 on-demand 옵션을 사용합니다. 다른 ASA 플랫폼에서는 full-download 옵션을 사용합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

ASA가 AD 에이전트에서 사용자 ID-IP 주소 매핑 정보를 검색하는 방법을 정의합니다.

- **full-download** - ASA가 시작될 때 ASA에서 AD 에이전트로 전체 IP-사용자 매핑 테이블 다운로드 요청을 보낸 다음 사용자가 로그인 및 로그아웃하면 증분 IP-사용자 매핑을 수신하도록 지정합니다.
- **on-demand** - ASA가 새로운 연결이 필요한 패킷을 수신할 때, 해당 소스 IP 주소의 사용자가 사용자-ID 데이터베이스에 없다면 ASA에서 AD 에이전트로부터 IP 주소의 사용자 매핑 정보를 검색하도록 지정합니다.

기본적으로 ASA 5505에서는 on-demand 옵션을 사용합니다. 다른 ASA 플랫폼에서는 full-download 옵션을 사용합니다.

전체 다운로드는 이벤트 기반이므로 데이터베이스 다운로드에 대한 후속 요청에서는 사용자 ID-IP 주소 매핑 데이터베이스에 만 업데이트만 전송합니다.

ASA가 AD 에이전트에 요청 변경을 등록하면 AD 에이전트에서 ASA로 새 이벤트를 전송합니다.

예

다음 예에서는 ID 방화벽에 대한 이 옵션을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity ad-agent active-user-database full-download
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity ad-agent hello-timer

Cisco ID 방화벽 인스턴스의 AD 에이전트와 ASA 간의 타이머를 정의하려면 전역 구성 모드에서 **user-identity ad-agent hello-timer** 명령을 사용합니다. 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

no user-identity ad-agent hello-timer seconds ***seconds*** **retry-times** ***number***

구문 설명

number	타이머를 재시도할 횟수를 지정합니다.
seconds	타이머의 기간을 지정합니다.

기본값

기본적으로 hello 타이머는 30초 및 5회 재시도로 설정됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

ASA와 AD 에이전트 간의 hello 타이머를 정의합니다.

ASA와 AD 에이전트 간의 hello 타이머는 ASA가 hello 패킷을 교환하는 빈도를 정의합니다. ASA는 hello 패킷을 사용하여 ASA 복제 상태(in-sync 또는 out-of-sync) 및 도메인 상태(up 또는 down)를 가져옵니다. ASA는 AD 에이전트에서 응답을 받지 못한 경우 지정된 간격 후 hello 패킷을 다시 전송합니다.

기본적으로 hello 타이머는 30초 및 5회 재시도로 설정됩니다.

예

다음 예에서는 ID 방화벽에 대한 이 옵션을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity ad-agent hello-timer seconds 20 retry-times 3
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity ad-agent event-timestamp-check

권한 부여 재생 공격의 변경으로부터 ASA를 방지하기 위해 RADIUS 이벤트 타임스탬프 확인을 활성화하려면 전역 구성 모드에서 **user-identity ad-agent event-timestamp-check** 명령을 사용합니다. 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity ad-agent event-timestamp-check

no user-identity ad-agent event-timestamp-check

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 설정은 disabled입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• **예**	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.1(5)	이 명령이 추가되었습니다.

사용 지침

이 명령을 사용하면 ASA가 각 식별자에 대해 마지막으로 받은 이벤트 타임스탬프를 추적하고, 이벤트 타임스탬프가 ASA의 클럭보다 5분 이상 오래되거나 해당 타임스탬프가 마지막 이벤트의 타임스탬프보다 빠른 경우 모든 메시지를 삭제합니다.

마지막 이벤트 타임스탬프를 모르는 새로 부팅된 ASA의 경우 ASA는 이벤트 타임스탬프를 해당 클럭과 비교합니다. 이벤트가 5분 이상 오래된 경우 ASA는 메시지를 허용하지 않습니다.

참고 ASA, Active Directory, Active Directory 에이전트끼리 NTP를 사용하여 시계를 동기화하도록 구성하는 것이 좋습니다.

예

다음 예에서는 ID 방화벽에 대한 이벤트 타임스탬프 확인을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity ad-agent event-timestamp-check
```

관련 명령

Command(명령)	설명
user-identity ad-agent hello-timer	Cisco ID 방화벽 인스턴스의 AD 에이전트와 ASA 간의 타이머를 정의합니다.

user-identity default-domain

Cisco ID 방화벽 인스턴스에 대한 기본 도메인을 지정하려면 전역 구성 모드에서 **user-identity default-domain** 명령을 사용합니다. 기본 도메인을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity default-domain *domain_NetBIOS_name*

no user-identity default-domain *domain_NetBIOS_name*

구문 설명

domain_NetBIOS_name	ID 방화벽에 대한 기본 도메인을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

*domain_NetBIOS_name*에는 [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] 등으로 구성된 최대 32자의 이름을 입력합니다. 단, 첫 자에는 '.' 및 ' '을 사용할 수 없습니다. 도메인 이름에 공백이 포함된 경우 따옴표로 전체 이름을 묶어야 합니다. 도메인 이름은 대/소문자를 구분하지 않습니다.

사용자 또는 그룹에 대해 도메인이 명시적으로 구성되지 않은 경우에는 모든 사용자 및 사용자 그룹에 기본 도메인이 사용됩니다. 기본 도메인을 지정하지 않은 경우 사용자 및 그룹의 기본 도메인은 LOCAL입니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간 내에서뿐만 아니라 각 상황에 대한 기본 도메인 이름을 설정할 수 있습니다.

참고 기본 도메인 이름은 Active Directory 도메인 컨트롤러에 구성된 NetBIOS 도메인 이름과 일치하도록 지정해야 합니다. 도메인 이름이 일치하지 않을 경우, AD 에이전트는 사용자 ID-IP 주소 매핑을 ASA 구성 시 입력한 도메인 이름과 잘못 연결합니다. NetBIOS 도메인 이름을 보려면 아무 텍스트 편집기에서나 Active Directory 사용자 이벤트 보안 로그를 엽니다.

ID 방화벽은 로컬로 정의된 모든 사용자 그룹 또는 로컬로 정의된 모든 사용자에 LOCAL 도메인을 사용합니다. 웹 포털(컷스루 프록시)을 통해 로그인하는 사용자는 인증된 Active Directory 도메인에 속한 것으로 지정됩니다. VPN을 통해 로그인하는 사용자는 해당 VPN이 Active Directory에서 LDAP로 인증되지 않은 한 LOCAL 도메인에 속하는 것으로 지정됩니다. 이는 ID 방화벽이 사용자를 해당 Active Directory 도메인과 연결할 수 있도록 하기 위한 것입니다.

예

다음 예에서는 ID 방화벽에 대한 기본 도메인을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity default-domain SAMPLE
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity domain

Cisco ID 방화벽 인스턴스에 대한 도메인을 연결하려면 전역 구성 모드에서 **user-identity domain** 명령을 사용합니다. 도메인 연결을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

no user-identity *domain_nickname* **aaa-server** ***aaa_server_group_tag***

구문 설명

aaa_server_group_tag	ID 방화벽과 연결된 AAA 서버 그룹을 지정합니다.
domain_nickname	ID 방화벽에 대한 도메인 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• **예**	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

사용자 그룹 쿼리를 가져오기 위해 AAA 서버에 대해 정의된 LDAP 파라미터를 도메인 이름과 연결합니다.

*domain_nickname*에는 [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] 등으로 구성된 최대 32자의 이름을 입력합니다. 단, 첫 자에는 '.' 및 ' '을 사용할 수 없습니다. 도메인 이름에 공백이 포함된 경우 해당 공백 문자를 따옴표로 묶어야 합니다. 도메인 이름은 대/소문자를 구분하지 않습니다.

예

다음 예에서는 ID 방화벽에 대한 도메인을 연결하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity domain SAMPLE aaa-server ds
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity enable

Cisco ID 방화벽 인스턴스를 만들려면 전역 구성 모드에서 **user-identity enable** 명령을 사용합니다. ID 방화벽 인스턴스를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

user-identity enable

no user-identity enable

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 ID 방화벽을 활성화합니다.

예

다음 예에서는 ID 방화벽을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity enable
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity inactive-user-timer

Cisco ID 방화벽 인스턴스에 대해 사용자가 유휴 상태로 간주되기 위해 경과해야 하는 시간을 지정하려면 전역 구성 모드에서 **user-identity inactive-user-timer** 명령을 사용합니다. 타이머를 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity inactive-user-timer minutes *minutes*

no user-identity inactive-user-timer minutes ***minutes***

구문 설명

minutes	사용자가 유휴 상태로 간주되기 위해 경과해야 하는 시간(분), 즉 ASA가 지정된 기간 동안 사용자 IP 주소에서 트래픽을 받지 못한 시간을 지정합니다.

기본값

기본적으로 유휴 시간 제한은 60분으로 설정됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

타이머가 만료되면 사용자의 IP 주소가 비활성으로 표시되고, 로컬로 캐시된 사용자 ID-IP 주소 매핑 데이터베이스에서 제거되며, ASA가 해당 IP 주소 제거에 대해 더 이상 AD 에이전트에 알리지 않습니다. 기존 트래픽은 여전히 통과하도록 허용됩니다. 이 명령을 지정하면 NetBIOS 로그아웃 프로브가 구성된 경우에도 ASA에서 비활성 타이머를 실행합니다.

참고 유휴 시간 제한 옵션은 VPN 또는 컷스루 프록시 사용자에게는 적용되지 않습니다.

예

다음 예에서는 ID 방화벽을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity inactive-user-timer minutes 120
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity logout-probe

Cisco ID 방화벽 인스턴스에 대한 NetBIOS 프로빙을 활성화하려면 전역 구성 모드에서 **user-identity logout-probe** 명령을 사용합니다. 프로빙을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed** | **match-any** | **exact-match**]

no user-identity logout-probe netbios local-system probe-time minutes ***minutes*** **retry-interval seconds** ***seconds*** **retry-count** ***times*** [**user-not-needed** | **match-any** | **exact-match**]

구문 설명

minutes	프로브 간의 간격(분)을 지정합니다.
seconds	재시도 간격을 지정합니다.
times	프로브를 재시도할 횟수를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

NetBIOS 패킷을 최소화하기 위해 ASA는 사용자가 지정된 기간(분)보다 오래 유휴 상태로 유지된 경우에만 클라이언트로 NetBIOS 프로브를 전송합니다.

NetBIOS 프로브 타이머(1~65535분) 및 재시도 간격(1~256)을 설정합니다. 프로브를 재시도할 횟수를 지정합니다.

- **match-any** - 클라이언트의 NetBIOS 응답에 IP 주소에 할당된 사용자의 사용자 이름이 포함되어 있으면 사용자 ID가 유효한 것으로 간주됩니다. 이 옵션을 지정하려면 클라이언트에서 메신저 서비스가 활성화되고 WINS 서버가 구성되어 있어야 합니다.
- **exact-match** - IP 주소에 지정된 사용자의 사용자 이름은 NetBIOS 응답에서 하나뿐이어야 합니다. 그렇지 않으면 해당 IP 주소의 사용자 ID가 유효하지 않은 것으로 간주됩니다. 이 옵션을 지정하려면 클라이언트에서 메신저 서비스가 활성화되고 WINS 서버가 구성되어 있어야 합니다.

- **user-not-needed** - ASA가 클라이언트에서 NetBIOS 응답을 받으면 사용자 ID가 유효한 것으로 간주됩니다.

ID 방화벽은 활성 상태이고 하나 이상의 보안 정책에 있는 사용자 ID에 대해서만 NetBIOS 프로브를 수행합니다. ASA는 사용자가 컷스루 프록시를 통해 또는 VPN을 사용하여 로그인한 경우 클라이언트에 대해 NetBIOS 프로빙을 수행하지 않습니다.

예

다음 예에서는 ID 방화벽을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10
retry-interval seconds 10 retry-count 2 user-not-needed
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity monitor

Cloud Web Security의 경우 AD 에이전트에서 지정된 사용자 또는 그룹 정보를 다운로드하려면 전역 구성 모드에서 user-identity monitor 명령을 사용합니다. 모니터링을 중지하려면 이 명령의 **no** 형식을 사용합니다.

user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*}

no user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*}

구문 설명

object-group-user ***object-group-name***	**object-group user** 이름을 지정합니다. 이 그룹은 여러 그룹을 포함할 수 있습니다.
user-group [*domain-name*\\] *group-name*	인라인 그룹 이름을 지정합니다. 도메인과 그룹 사이에 백슬래시 2개(\\)를 지정한 경우에도 ASA는 Cloud Web Security 표기법 규칙을 준수하기 위해 Cloud Web Security로 전송할 때 백슬래시를 하나만 포함하도록 이름을 수정합니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

ID 방화벽 기능을 사용할 때 ASA는 AD 서버에서 활성 ACL에 포함된 사용자 및 그룹에 대한 사용자 ID 정보만 다운로드합니다. ACL은 액세스 규칙, AAA 규칙, 서비스 정책 규칙 또는 활성 상태로 간주되는 기타 기능에서 사용되어야 합니다. Cloud Web Security는 해당 정책이 사용자 ID를 기반으로 할 수 있기 때문에 모든 사용자에 대해 ID 방화벽을 완전히 적용하려는 경우 활성 ACL의 일부가 아닌 그룹을 다운로드해야 할 수도 있습니다. 예를 들어 사용자 및 그룹이 포함된 ACL을 사용하도록 Cloud Web Security 서비스 정책 규칙을 구성하여 모든 관련 그룹을 활성화할 수 있지만 이는 필수 사항이 아닙니다. IP 주소만을 기반으로 하는 ACL을 사용할 수 있습니다. 사용자 ID 모니터 기능을 사용하면 AD 에이전트에서 직접 그룹 정보를 다운로드할 수 있습니다.

ASA는 사용자 ID 모니터에 대해 구성된 그룹 및 액티브 ACL을 통해 모니터링되는 그룹을 포함하여 최대 512개의 그룹만 모니터링할 수 있습니다.

예

다음 예에서는 CISCO\\Engineering 사용자 그룹을 모니터링합니다.

```
ciscoasa(config)# user-identity monitor user-group CISCO\\Engineering
```

관련 명령

Command(명령)	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](parameters)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스에서 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	화이트리스트를 기준으로 사용자 또는 그룹을 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	Cloud Web Security 프록시 서버를 폴링하여 가용성 여부를 확인하기까지 ASA에서 대기하는 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 컨텍스트 모드에서는 컨텍스트 단위로 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN(Fully Qualified Domain Name) 또는 IP 주소를 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe server	서버의 상태, 즉 현재 활성 서버인지, 백업 서버인지 또는 도달할 수 없는 서버인지 표시합니다.
show scansafe statistics	총 HTTP 연결 수와 현재 HTTP 연결 수를 표시합니다.
whitelist	트래픽의 클래스에 대해 화이트리스트 작업을 수행합니다.

user-identity poll-import-user-group-timer

ASA가 Active Directory 서버에서 Cisco ID 방화벽 인스턴스에 대한 사용자 그룹 정보를 쿼리하기 전에 경과해야 하는 시간을 지정하려면 전역 구성 모드에서 **user-identity poll-import-user-group-timer** 명령을 사용합니다. 타이머를 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity poll-import-user-group-timer hours *hours*

no user-identity poll-import-user-group-timer hours *hours*

구문 설명

hours	폴링 타이머 시간을 설정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다 .

사용 지침

ASA가 Active Directory 서버에서 사용자 그룹 정보를 쿼리하기 전에 경과해야 하는 시간을 지정합니다.

사용자가 Active Directory 그룹에서 추가되거나 삭제된 경우 ASA는 그룹 가져오기 타이머가 실행된 후 업데이트된 사용자 그룹을 받습니다.

기본적으로 폴링 타이머는 8시간입니다.

사용자 그룹 정보를 즉시 업데이트하려면 **user-identity update import-user** 명령을 입력합니다.

예

다음 예에서는 ID 방화벽을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity poll-import-user-group-timer hours 1
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity static user

새 사용자-IP 주소 매핑을 만들거나 Cisco ID 방화벽 기능에 대해 사용자의 IP 주소를 비활성으로 설정하려면 전역 구성 모드에서 **user-identity static user** 명령을 사용합니다. ID 방화벽에 대한 이 구성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity static user [*domain*\] *user_name host_ip*

no user-identity static user [***domain***\] ***user_name host_ip***

구문 설명

domain	새 사용자-IP 주소 매핑을 만들거나 지정된 도메인의 사용자에 대한 IP 주소를 비활성으로 설정합니다.
host_ip	새 사용자-IP 주소 매핑을 만들거나 비활성으로 설정할 사용자의 IP 주소를 지정합니다.
user_name	새 사용자-IP 주소 매핑 또는 사용자를 만들거나 사용자의 IP 주소를 비활성으로 설정할 사용자 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.7(1)	이 명령이 도입되었습니다.

사용 지침

이 명령에 대한 사용 지침은 없습니다.

예

다음 예는 user1에 대한 고정 경로 생성 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity static user SAMPLE\user1 192.168.1.101
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity update active-user-database

Active Directory 에이전트에서 전체 활성 사용자 데이터베이스를 다운로드하려면 전역 구성 모드에서 **user-identity update active-user-database** 명령을 사용합니다.

user-identity update active-user-database [**timeout minutes** *minutes*]

구문 설명

minutes	시간 제한 기간(분)을 지정합니다.

기본값

기본 시간 제한은 5분입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Active Directory 에이전트에서 전체 활성 사용자 데이터베이스를 다운로드합니다.

이 명령은 업데이트 작업을 시작하고, 시작 업데이트 로그를 생성하여 즉시 반환합니다. 업데이트 작업이 완료되거나 타이머 만료 시 중단되면 다른 시스템 로그 메시지가 생성됩니다. 미해결 업데이트 작업은 하나만 허용됩니다. 명령을 다시 실행하면 오류 메시지가 표시됩니다.

명령 실행이 완료되면 ASA에서 명령 프롬프트에 [Done]을 표시한 다음 시스템 로그 메시지를 생성합니다.

예

다음 예에서는 ID 방화벽에 대한 이 동작을 활성화하는 방법을 보여 줍니다.

```
ciscoasa# user-identity update active-user-database
ERROR: one update active-user-database operation is already in progress
[Done] user-identity update active-user-database
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity update import-user

Active Directory 에이전트에서 전체 활성 사용자 데이터베이스를 다운로드하려면 전역 구성 모드에서 **user-identity update active-user-database** 명령을 사용합니다.

user-identity update import-user [[*domain_nickname*\\] *user_group_name* [**timeout seconds** *seconds*]]

구문 설명

domain_nickname	업데이트할 그룹의 도메인을 지정합니다.
seconds	시간 제한 기간(초)을 지정합니다.
user_group_name	*user_group_name*을 지정하면 지정된 가져오기 사용자 그룹만 업데이트됩니다. 활성화된 그룹(예: 액세스 그룹, 액세스 목록, 캡처 또는 서비스 정책의 그룹)만 업데이트할 수 있습니다. 지정된 그룹이 활성화되지 않은 경우 이 명령은 작업을 거부합니다. 지정된 그룹에 여러 수준의 계층이 있으면 재귀적 LDAP 쿼리가 수행됩니다. *user_group_name*을 지정하지 않은 경우 ASA는 LDAP 업데이트 서비스를 즉시 시작하고 활성화된 모든 그룹을 정기적으로 업데이트합니다.

기본값

ASA는 최대 5번 업데이트를 재시도하며, 필요한 경우 경고 메시지를 생성합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• **예**	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

이 명령은 가져오기 사용자 그룹 폴링 타이머의 만료를 기다리지 않고 Active Directory 서버를 즉시 쿼리하여 지정된 가져오기 사용자 그룹 데이터베이스를 명령합니다. 그룹 ID 데이터베이스는 로컬 사용자 그룹에 구성 변경이 있을 때마다 업데이트되므로 로컬 사용자 그룹을 업데이트하는 명령은 없습니다.

이 명령은 LDAP 쿼리 반환을 대기하기 위해 콘솔을 차단하지 않습니다.

이 명령은 업데이트 작업을 시작하고, 시작 업데이트 로그를 생성하여 즉시 반환합니다. 업데이트 작업이 완료되거나 타이머 만료 시 중단되면 다른 시스템 로그 메시지가 생성됩니다. 미해결 업데이트 작업은 하나만 허용됩니다. 명령을 다시 실행하면 오류 메시지가 표시됩니다.

LDAP 쿼리에 성공하면 ASA는 검색된 사용자 데이터를 로컬 데이터베이스에서 저장하고 그에 따라 사용자/그룹 연결을 변경합니다. 업데이트 작업에 성공한 경우 **show user-identity user-of-group** *domain\\group* 명령을 실행하여 저장된 모든 사용자를 이 그룹 아래에 나열할 수 있습니다.

ASA는 각 업데이트 후 가져온 모든 그룹을 확인합니다. 활성화된 Active Directory 그룹이 Active Directory에 없는 경우 ASA는 시스템 로그 메시지를 생성합니다.

*user_group_name*을 지정하지 않은 경우 ASA는 LDAP 업데이트 서비스를 즉시 시작하고 활성화된 모든 그룹을 정기적으로 업데이트합니다. LDAP 업데이트 서비스는 백그라운드에서 실행되며, Active Directory 서버에서 LDAP 쿼리를 통해 가져오기 사용자 그룹을 정기적으로 업데이트합니다.

시스템 부팅 시 액세스 그룹에 정의된 가져오기 사용자 그룹이 있는 경우 ASA는 LDAP 쿼리를 통해 사용자/그룹 데이터를 검색합니다. 업데이트 중 오류가 발생한 경우 ASA는 최대 5번 업데이트를 재시도하고 필요한 경우 경고 메시지를 생성합니다.

명령 실행이 완료되면 ASA에서 명령 프롬프트에 [Done]을 표시한 다음 시스템 로그 메시지를 생성합니다.

예

다음 예에서는 ID 방화벽에 대한 이 동작을 활성화하는 방법을 보여 줍니다.

```
ciscoasa# user-identity update import-user group.sample-group1
ERROR: Update import-user group is already in progress
[Done] user-identity update import-user group.sample-group1
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-identity user-not-found

Cisco ID 방화벽 인스턴스에 대한 user-not-found 추적을 활성화하려면 전역 구성 모드에서 **user-identity user-not-found** 명령을 사용합니다. ID 방화벽 인스턴스에 대한 이 추적을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-identity user-not-found enable

no user-identity user-not-found enable

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 이 명령은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• **예**	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

최근 1024개의 IP 주소만 추적됩니다.

예

다음 예에서는 ID 방화벽에 대한 이 동작을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# user-identity user-not-found enable
```

관련 명령

Command(명령)	설명
clear configure user-identity	ID 방화벽 기능에 대한 컨피그레이션을 지웁니다.

user-message

DAP 레코드를 선택한 경우 표시할 텍스트 메시지를 지정하려면 dynamic-access-policy-record 모드에서 user-message 명령을 사용합니다. 이 메시지를 제거하려면 이 명령의 **no** 버전을 사용합니다. 동일한 DAP 레코드에 명령을 두 번 이상 사용하면 이전 메시지가 새 메시지로 대체됩니다.

user-message *message*

no user-message

구문 설명

message	이 DAP 레코드에 할당된 사용자에 대한 메시지입니다. 최대 128자입니다. 메시지에 공백이 포함된 경우 큰따옴표로 묶습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
dynamic-access-policy-record	• 예	• 예	• 예	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

SSL VPN 연결에 성공한 경우 사용자가 연결과 연계된 메시지를 볼 수 있도록 클릭 가능한 아이콘이 포털 페이지에서 깜박입니다. DAP 정책에서 연결이 종료된 경우(action = terminate) 및 해당 DAP 레코드에 구성된 사용자 메시지가 있는 경우 해당 메시지가 로그인 화면에 표시됩니다.

둘 이상의 DAP 레코드가 연결에 적용된 경우 ASA는 적용 가능한 사용자 메시지를 조합하여 단일 문자열로 표시합니다.

예

다음 예에서는 Finance라는 DAP 레코드에 대해 "Hello Money Managers" 라는 사용자 메시지를 설정하는 방법을 보여 줍니다.

```
ciscoasa (config) config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# user-message "Hello Money Managers"
ciscoasa(config-dynamic-access-policy-record)#
```

관련 명령

Command(명령)	설명
dynamic-access-policy-record	DAP 레코드를 생성합니다.
show running-config dynamic-access-policy-record [*name*]	모든 DAP 레코드 또는 명명된 DAP 레코드에 대한 실행 중인 구성을 표시합니다.

user-parameter

SSO 인증을 위해 사용자 이름을 제출해야 하는 HTTP POST 요청 파라미터의 이름을 지정하려면 aaa-server-host 구성 모드에서 **user-parameter** 명령을 사용합니다.

user-parameter *name*

참고 HTTP 프로토콜로 SSO를 올바르게 설정하려면 인증 및 HTTP 프로토콜 교환에 대해 완벽한 지식을 갖추어야 합니다.

구문 설명

string	HTTP POST 요청에 포함된 사용자 이름 파라미터의 이름입니다. 이름은 최대 128자입니다.

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
aaa-server-host 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.

사용 지침

이는 HTTP 양식을 사용하는 SSO 명령입니다. ASA의 WebVPN 서버는 HTTP POST 요청을 사용하여 SSO(Single Sign On) 서버에 SSO 인증 요청을 제출합니다. The required command **user-parameter** specifies that the HTTP POST request must include a username parameter for SSO authentication.

참고 로그인 시 사용자는 HTTP POST 요청에 입력되어 인증하는 웹 서버로 전달되는 실제 이름 값을 입력합니다.

예

aaa-server-host 구성 모드에서 입력된 다음 예에서는 SSO 인증에 사용되는 HTTP POST 요청에 사용자 이름 파라미터 userid를 포함하도록 지정합니다.

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# user-parameter userid
ciscoasa(config-aaa-server-host)#
```

관련 명령

Command(명령)	설명
action-uri	SSO(Single Sign-On) 인증에 필요한 사용자 이름 및 비밀번호를 받을 웹 서버 URI를 지정합니다.
auth-cookie-name	인증 쿠키 이름을 지정합니다.
hidden-parameter	인증 웹 서버와 교환할 숨겨진 파라미터를 생성합니다.
password-parameter	SSO 인증을 위해 사용자 비밀번호를 제출해야 하는 HTTP POST 요청 파라미터의 이름을 지정합니다.
start-url	사전 로그인 쿠키를 검색할 URL을 지정합니다.

user-statistics

MPF 및 ID 방화벽에 대한 일치 조회 동작의 사용자 통계 수집을 활성화하려면 policy-map 구성 모드에서 **user-statistics** 명령을 사용합니다. 사용자 통계 수집을 제거하려면 이 명령의 **no** 형식을 사용합니다.

user-statistics [**accounting | scanning**]

no user-statistics [**accounting | scanning**]

구문 설명

accounting	(선택 사항) ASA에서 보낸 패킷 수, 보낸 삭제 수 및 받은 패킷 수를 수집하도록 지정합니다.
scanning	(선택 사항) ASA에서 보낸 삭제 수만 수집하도록 지정합니다.

기본값

기본적으로 이 명령은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
policy-map 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
8.4(2)	이 명령이 추가되었습니다.

사용 지침

사용자 통계를 수집하도록 정책 맵을 구성한 경우 ASA는 선택한 사용자에 대한 자세한 통계를 수집합니다. **user-statistics** 명령을 **accounting** 또는 **scanning** 키워드 없이 지정한 경우 ASA는 어카운팅 통계와 검사 통계를 모두 수집합니다.

예

다음 예에서는 ID 방화벽에 대한 사용자 통계를 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# class-map c-identity-example-1
ciscoasa(config-cmap)# match access-list identity-example-1
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map p-identity-example-1
ciscoasa(config-pmap)# class c-identity-example-1
ciscoasa(config-pmap)# user-statistics accounting
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy p-identity-example-1 interface outside
```

관련 명령

Command(명령)	설명
policy-map	MPF(Modular Policy Framework)를 사용할 때 계층 3/4 클래스 맵으로 식별한 동작을 트래픽에 할당합니다.
service-policy(**global**)	정책 맵을 모든 인터페이스에서 전역적으로 활성화하거나 대상 인터페이스에서 활성화합니다.
show service-policy [**user-statistics**]	ID 방화벽에 대한 사용자 통계 스캔 또는 어카운트 관리를 활성화한 경우 구성된 서비스 정책에 대한 사용자 통계를 표시합니다.
show user-identity ip-of-user [**detail**]	ID 방화벽에 대한 사용자 통계 스캔 또는 어카운트 관리를 활성화한 경우 지정된 사용자의 IP 주소에 대한 받은 패킷, 보낸 패킷 및 삭제 통계를 표시합니다.
show user-identity user active [**detail**]	ID 방화벽에 대한 사용자 통계 스캔 또는 어카운트 관리를 활성화한 경우 활성 사용자에 대해 지정된 기간 동안의 받은 패킷, 보낸 패킷 및 삭제 통계를 표시합니다.
show user-identity user-of-ip [**detail**]	ID 방화벽에 대한 사용자 통계 스캔 또는 어카운트 관리를 활성화한 경우 지정된 IP 주소의 사용자에 대한 받은 패킷, 보낸 패킷 및 삭제 통계를 표시합니다.
user-identity enable	ID 방화벽 인스턴스를 생성합니다.

user-storage

클라이언트리스 SSL VPN 세션 간의 개인 설정된 사용자 정보를 저장하려면 group-policy webvpn 구성 모드에서 **user storage** 명령을 사용합니다. 사용자 저장소를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

user-storage *NETFS-location*

no user-storage]

구문 설명

NETFS-location	proto://user:password@host:port/path 형식으로 파일 시스템 대상을 지정합니다. 사용자 이름 및 비밀번호가 NETFS-location에 포함된 경우 비밀번호 입력은 일반 텍스트로 처리됩니다.

기본값

사용자 저장소는 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
group-policy webvpn 모드	• 예	—	• **예**	—	—

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.
8.4(6)	비밀번호가 **show-run** 중에 일반 텍스트로 표시되는 것이 방지되었습니다.

사용 지침

user-storage를 사용하면 ASA 플래시가 아닌 다른 위치에 캐시된 크리덴셜 및 쿠키를 저장할 수 있습니다. 이 명령은 클라이언트리스 SSL VPN 사용자의 개인 책갈피에 대한 SSO(Single Sign On)을 제공합니다. 사용자 크리덴셜은 FTP/CIFS/SMB 서버에 암호 해독이 불가능하지 않은 <user_id>.cps 파일로 암호화된 형식으로 저장됩니다.

사용자 이름, 비밀번호 및 사전 공유 키가 구성에 표시되지만 ASA는 내부 알고리즘을 사용하여 이 정보를 암호화된 형식으로 저장하므로 보안 위험이 없습니다.

데이터가 외부 FTP 또는 SMB 서버에 암호화되어 있는 경우 책갈피 추가를 선택하여 포털 페이지 내에 개인 책갈피(예: user-storage cifs://jdoe:test@10.130.60.49/SharedDocs)를 정의할 수 있습니다. 모든 플러그인 프로토콜에 대해 개인 설정된 URL도 만들 수 있습니다.

참고 모두 동일한 FTP/CIFS/SMB 서버를 참조하고 동일한 "storage-key" 를 사용하는 ASA 클러스터가 있는 경우 클러스터의 ASA 중 하나를 통해 책갈피에 액세스할 수 있습니다.

예

다음 예에서는 newuser라는 사용자에 대해 anyfiler02a/new_share 경로의 anyshare라는 파일 공유에 비밀번호가 12345678인 사용자 저장소를 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# wgroup-policy DFLTGrpPolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
ciscoasa(config-group_webvpn)#
```

관련 명령

Command(명령)	설명
storage-key	세션 간에 저장되는 데이터를 보호할 저장소 키를 지정합니다.
storage-objects	세션 간에 저장된 데이터의 저장소 개체를 구성합니다.

username

ASA 로컬 데이터베이스에 사용자를 추가하려면 전역 구성 모드에서 **username** 명령을 입력합니다. 사용자를 제거하려면 제거할 사용자 이름과 함께 이 명령의 **no** 형식을 사용합니다.

username *name* [**password** *password* [**pbkdf2** | **mschap** | **encrypted** | **nt-encrypted**] | **nopassword**] [**privilege** *priv_level*]

no username *name* [**password** *password* [**pbkdf2** | **mschap** | **encrypted** | **nt-encrypted**] | **nopassword**] [**privilege** *priv_level*]

구문 설명

encrypted	9.6 이하 버전의 경우 32자 이하의 비밀번호가 암호화됨을 나타냅니다(**mschap**를 지정하지 않은 경우). **username** 명령에서 비밀번호를 정의하는 경우 ASA에서는 비밀번호를 구성에 저장할 때 MD5 해시를 생성하여 보안을 강화합니다. **show running-config** 명령을 입력한 경우 **username** 명령은 실제 비밀번호를 표시하지 않습니다. 그 대신 암호화된 비밀번호를 표시하고 그 뒤에 **encrypted** 키워드를 표시합니다. 예를 들어 비밀번호로 "test" 를 입력하면 다음과 유사한 **show running-config** 명령 출력이 표시됩니다. `username pat password rvEdRh0xPC8bel7s encrypted` CLI에서 실제로 **encrypted** 키워드를 입력하는 경우는 구성을 잘라내어 다른 ASA에 붙여넣고 동일한 비밀번호를 사용하려는 경우뿐입니다. 9.7 이상에서는 모든 길이의 비밀번호에 PBKDF2를 사용합니다.
mschap	비밀번호를 입력한 후 해당 비밀번호가 유니코드로 변환되고 MD4를 통해 해시되도록 지정합니다. MSCHAPv1 또는 MSCHAPv2를 사용하여 사용자를 인증하는 경우 이 키워드를 사용합니다.
name	공백 및 물음표를 제외하고 인쇄 가능 ASCII 문자(문자 코드 32~126)를 조합한 3~64자의 문자열로 사용자 이름을 지정합니다.
nopassword	*모든* 비밀번호를 이 사용자에 대해 입력할 수 있음을 나타냅니다. 이는 보안되지 않은 구성이므로 이 키워드를 주의해서 사용하십시오. (9.6(2) 이상) 비밀번호 없이 사용자 이름을 생성하려면 **password** 또는 **nopassword** 키워드를 입력하지 마십시오. 예를 들어 **ssh authentication** 명령을 사용하면 ASA에 공개 키를 설치하고 SSH 클라이언트에서 개인 키를 사용할 수 있으므로 비밀번호를 구성하지 않을 수 있습니다.

nt-encrypted	MSCHAPv1 또는 MSCHAPv2에서 사용하도록 비밀번호가 암호화됨을 나타냅니다. 사용자를 추가 할 때 **mschap** 키워드를 지정한 경우에는 **show running-config** 명령을 사용하여 구성을 볼 때 **encrypted** 키워드 대신 이 키워드가 표시됩니다. **username** 명령에서 비밀번호를 정의할 때 ASA에서는 비밀번호를 컨피그레이션에 저장할 때 암호화하여 보안을 강화합니다. **show running-config** 명령을 입력한 경우 **username** 명령은 실제 비밀번호를 표시하지 않습니다. 그 대신 암호화된 비밀번호를 표시하고 그 뒤에 **nt-encrypted** 키워드를 표시합니다. 예를 들어 비밀번호로 "test" 를 입력하면 다음과 유사한 **show running-config** 화면이 표시됩니다. `username pat password DLaUiAX3178qgoB5c7iVNw== nt-encrypted` CLI에서 실제로 **nt-encrypted** 키워드를 입력하는 경우는 구성을 잘라내어 다른 ASA에 붙여넣고 동일한 비밀번호를 사용하려는 경우뿐입니다.
password *password*	공백 및 물음표를 제외하고 인쇄 가능 ASCII 문자(문자 코드 32~126)를 조합한 3~32자의 문자열로 비밀번호를 지정합입니다(9.5 이하).
pbkdf2	비밀번호가 암호화되어 있음을 나타냅니다. 9.6 이하 버전의 경우 비밀번호가 32자보다 길 때만 PBKDF2(Password-Based Key Derivation Function 2) 해시가 사용됩니다. 9.7 이상에서는 모든 비밀번호에 PBKDF2를 사용합니다. **username** 명령에서 비밀번호를 정의하는 경우 ASA에서는 비밀번호를 구성에 저장할 때 PBKDF2 해시를 생성하여 보안을 강화합니다. **show running-config** 명령을 입력하면 **username** 명령에서는 실제 비밀번호를 표시하지 않습니다. 암호화된 비밀번호 뒤에 **pbkdf2** 키워드가 표시됩니다. 예를 들어 긴 비밀번호를 입력하면 다음과 유사한 **show running-config** 명령 출력이 표시됩니다. `username pat password rvEdRh0xPC8bel7s pbkdf2` CLI에서 실제로 **pbkdf2** 키워드를 입력하는 경우는 구성을 잘라내어 다른 ASA에 붙여넣고 동일한 비밀번호를 사용하려는 경우뿐입니다. 새 비밀번호를 입력하지 않는 한, 기존 비밀번호에서는 MD5 기반 해시를 계속해서 사용합니다.
privilege *priv_level*	이 사용에 대한 권한 수준을 0부터 15까지 오름차순으로 설정합니다. 기본 권한 수준은 2입니다. 이 권한 레벨은 명령 권한 부여와 함께 사용됩니다.

기본값

기본 권한 수준은 2입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0.1	이 명령이 추가되었습니다.
7.2(1)	**mschap** 및 **nt-encrypted** 키워드가 추가되었습니다.
9.6(1)	비밀 번호 길이가 127자로 증가했으며 **pbkdf2** 키워드가 추가되었습니다.
9.6(2)	이제 **password** 또는 **nopassword** 키워드 없이 사용자 이름을 생성할 수 있습니다.
9.7(1)	이제 모든 길이의 비밀번호가 PBKDF2 해시를 사용하여 구성에 저장됩니다.

사용 지침

login 명령은 인증을 위해 이 데이터베이스를 사용합니다.

CLI에 액세스할 수 있으며 특권 모드를 시작하지 않으려는 사용자를 로컬 데이터베이스에 추가하려면 권한 부여 명령을 활성화해야 합니다. (**aaa authorization command** 명령 참고.) 명령 권한 부여가 없으면, 권한 수준이 2 이상(2가 기본값)인 사용자는 CLI에서 각자의 비밀번호를 사용하여 특별 권한 EXEC 모드(및 모든 명령)에 액세스할 수 있습니다. 또는 사용자가 **login** 명령을 사용할 수 없도록 AAA 인증을 사용하거나, **enable** 비밀번호를 사용하여 특권 EXEC 모드에 액세스할 수 있는 사용자를 제어할 수 있도록 모든 로컬 사용자를 수준 1로 설정할 수 있습니다.

기본적으로 이 명령을 사용하여 추가하는 VPN 사용자에게는 특성 또는 그룹 정책 연결이 없습니다. **username attributes** 명령을 사용하여 모든 값을 명시적으로 구성해야 합니다.

비밀번호 인증 정책이 활성화된 경우에는 더 이상 **username** 명령을 사용하여 자신의 비밀번호를 변경하거나 사용자 고유의 계정을 삭제할 수 없습니다. 그러나 **change-password** 명령을 사용하여 비밀번호를 변경할 수 있습니다.

사용자 이름 비밀번호 날짜를 표시하려면 **show running-config all username** 명령을 사용합니다.

예

다음 예에서는 비밀번호가 12345678이고 권한 수준이 12인 "anyuser" 라는 사용자를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# username anyuser password 12345678 privilege 12
```

관련 명령

Command(명령)	설명
aaa authorization command	권한 부여 명령을 구성합니다.
clear config username	특정 사용자 또는 모든 사용자에 대한 구성을 지웁니다.
show running-config username	특정 사용자 또는 모든 사용자에 대한 실행 중인 컨피그레이션을 표시합니다.
username attributes	특정 사용자에 대한 특성을 구성할 수 있는 username attributes 모드를 시작합니다.
webvpn	지정된 그룹에 대한 WebVPN 특성을 구성할 수 있는 config-group-webvpn 모드를 시작합니다.

username attributes

username attributes 모드를 시작하려면 username 구성 모드에서 **username attributes** 명령을 사용합니다. 특정 사용자에 대한 모든 특성을 제거하려면 이 명령의 **no** 형식을 사용하고 사용자 이름을 추가합니다. 모든 사용자에 대한 모든 특성을 제거하려면 사용자 이름을 추가하지 않고 이 명령의 **no** 형식을 사용합니다. 특성 모드를 통해 지정된 사용자에 대한 특성-값 쌍을 구성할 수 있습니다.

username *name* **attributes**

no username *name* **attributes**

구문 설명

name	사용자의 이름을 제공합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
username 컨피그레이션	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
8.0(2)	**service-type** 특성이 추가되었습니다.
9.1(2)	**ssh authentication** {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]} 특성이 추가되었습니다.

사용 지침

내부 사용자 인증 데이터베이스는 **username** 명령을 사용하여 입력된 사용자로 구성됩니다. **login** 명령은 인증을 위해 이 데이터베이스를 사용합니다. **username** 명령 또는 **username attributes** 명령을 사용하여 사용자 이름 특성을 구성할 수 있습니다.

username 구성 모드의 명령 구문에는 일반적으로 다음과 같은 특성이 있습니다.

- **no** 형식은 실행 중인 구성에서 특성을 제거합니다.
- **none** 키워드도 실행 중인 구성에서 특성을 제거합니다. 그러나 이렇게 하려면 상속하지 못하도록 특성을 null 값으로 설정해야 합니다.
- 부울 특성에는 enabled 및 disabled 설정에 대한 명시적 구문이 있습니다.

username attributes 명령은 다음과 같은 특성을 구성할 수 있는 username attributes 모드를 시작합니다.

특성	기능
group-lock	사용자가 연결해야 하는 기존 터널 그룹의 이름을 지정합니다.
password-storage	클라이언트 시스템에서 로그인 비밀번호의 저장을 활성화하거나 비활성화합니다.
service-type [**remote-access** | **admin** | **nas-prompt**]	콘솔 로그인을 제한하고 적절한 수준이 할당된 사용자에 대해 로그인을 활성화합니다. **remote-access** 옵션은 원격 액세스를 위한 기본 AAA 서비스를 지정합니다. **admin** 옵션은 AAA 서비스, 로그인 콘솔 권한, EXEC 모드 권한, 활성화 권한 및 CLI 권한을 지정합니다. **nas-prompt** 옵션은 AAA 서비스, 로그인 콘솔 권한 및 EXEC 모드 권한을 지정하지만 활성화 권한은 지정하지 않습니다.
ssh authentication {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]}	사용자별로 공개 키 인증을 활성화합니다. *key* 인수 값은 다음을 참조할 수 있습니다. • *key* 인수를 제공하고 해시된 태그를 지정하지 않은 경우 키 값은 SSH-RSA 원시 키(즉, 인증서가 없음)를 생성할 수 있는 SSH 키 생성 소프트웨어에서 생성된 Base 64로 인코딩된 공개 키여야 합니다. Base 64로 인코딩된 공개 키를 전송하면 이 키는 SHA-256을 통해 해시되며, 해당 32바이트 해시가 모든 추가 비교에 사용됩니다. • *key* 인수를 제공하고 해시된 태그를 지정한 경우 키 값은 이전에 SHA-256으로 해시되고 길이가 32바이트이며, 각 바이트가 콜론으로 구분(구문 분석을 위해)되어 있습니다. **pkf** 옵션은 4096비트 RSA 키를 SSH PKF(공개 키 파일)로 사용하여 인증할 수 있도록 합니다. 이 옵션은 4096비트 RSA 키에 국한되지 않고 4096비트 RSA 키보다 작거나 같은 모든 크기에 사용할 수 있습니다. **nointeractive** 옵션은 SSH 공개 키 형식의 키를 가져올 때 모든 프롬프트를 표시하지 않도록 설정합니다. 이 비대화형 데이터 입력 모드는 ASDM 전용으로 제공됩니다. *key* 필드와 **hashed** 키워드는 **publickey** 옵션에서만 사용할 수 있으며, **nointeractive** 키워드는 **pkf** 옵션에서만 사용할 수 있습니다. 구성을 저장하면 해시된 키 값이 구성에 저장되며 ASA가 재부팅될 때 사용됩니다. **참고** 장애 조치가 활성화된 경우 PKF 옵션을 사용할 수 있지만 PKF 데이터가 대기 시스템에 자동으로 복제되지는 않습니다. 장애 조치 쌍의 대기 시스템에 PKF 설정을 동기화하려면 **write standby** 명령을 입력해야 합니다.
vpn-access-hours	구성된 시간 범위 정책의 이름을 지정합니다.
vpn-filter	사용자별 ACL의 이름을 지정합니다.
vpn-framed-ip-address	클라이언트에 할당할 IP 주소 및 넷마스크를 지정합니다.

특성	기능
vpn-group-policy	특성을 상속할 그룹 정책의 이름을 지정합니다.
vpn-idle-timeout [**alert-interval**]	유휴 시간 제한(분)을 지정하거나, **none**을 지정하여 유휴 시간 제한을 비활성화합니다. 선택적으로 사전 시간 제한 알림 간격을 지정합니다.
vpn-session-timeout [**alert-interval**]	최대 사용자 연결 시간(분)을 지정하거나, 무제한 시간의 경우 **none**을 지정합니다. 선택적으로 사전 시간 제한 알림 간격을 지정합니다.
vpn-simultaneous-logins	허용되는 최대 동시 로그인 수를 지정합니다.
vpn-tunnel-protocol	허용되는 터널링 프로토콜을 지정합니다.
webvpn	WebVPN 특성을 구성할 수 있는 username webvpn configuration 모드를 시작합니다.

username webvpn 구성 모드에서 **username attributes** 명령을 입력한 다음 **webvpn** 명령을 입력하여 사용자 이름에 대한 webvpn-mode 특성을 구성합니다. 자세한 내용은 **webvpn** 명령(group-policy attributes 및 username attributes 모드)을 참고하십시오.

예

다음 예에서는 "anyuser" 라는 사용자에 대한 username attributes 구성 모드를 시작하는 방법을 보여 줍니다.

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)#
```

관련 명령

Command(명령)	설명
clear config username	사용자 이름 데이터베이스를 지웁니다.
show running-config username	특정 사용자 또는 모든 사용자에 대한 실행 중인 구성을 표시합니다.
username	ASA 데이터베이스에 사용자를 추가합니다.
webvpn	지정된 그룹에 대한 WebVPN 특성을 구성할 수 있는 webvpn 구성 모드를 시작합니다.

username-from-certificate

권한 부여를 위한 사용자 이름으로 사용할 인증서의 필드를 지정하려면 tunnel-group general-attributes 모드에서 **username-from-certificate** 명령을 사용합니다. 피어 인증서의 DN이 권한 부여를 위한 사용자 이름으로 사용됩니다.

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

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

no username-from-certificate

구문 설명

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

기본값

기본 특성의 기본값은 CN(공통 이름)입니다.

보조 특성의 기본값은 OU(조직 구성 단위)입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
8.0(4)	이 명령이 추가되었습니다.

사용 지침

이 명령은 사용자 이름으로 사용할 인증서의 필드를 선택합니다. 릴리스 8.0(4) 이상에서 더 이상 사용되지 않는 **authorization-dn-attributes** 명령을 대체합니다. **username-from-certificate** 명령은 보안 어플라이언스에서 지정된 인증서 필드를 사용자 이름/비밀번호 권한 부여를 위한 사용자 이름으로 사용하도록 강제합니다.

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

기본 및 보조 특성에 사용할 수 있는 값은 다음과 같습니다.

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

예

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

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

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

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

관련 명령

Command(명령)	설명
pre-fill-username	사용자 이름 미리 채우기 기능을 활성화합니다.
show running-config tunnel-group	지정된 tunnel-group 구성을 표시합니다.
tunnel-group general-attributes	명명된 tunnel-group의 일반 특성을 지정합니다.

username password-date

시스템에서 부팅 시 또는 실행 중인 구성에 파일을 복사할 때 비밀번호 생성 날짜를 복원하도록 하려면 **username pasword-date** 명령을 비 인터랙티브 구성 모드에서 입력합니다. 즉, 이 명령은 이미 존재하는 구성 파일을 부팅하는 경우에만 사용할 수 있습니다. CLI 프롬프트에서는 이 명령을 입력할 수 없습니다.

username *name* **password-date** *date*

구문 설명

name	공백 및 물음표를 제외하고 인쇄 가능 ASCII 문자(문자 코드 32~126)를 조합한 3~64자의 문자열로 사용자 이름을 지정합니다.
date	시스템이 부팅하는 동안 사용자 이름을 읽을 때 비밀번호 생성 날짜를 복원할 수 있도록 합니다. 없는 경우 비밀번호 날짜가 현재 날짜로 설정됩니다. 날짜는 mmm-dd-yyyy 형식입니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
비 인터랙티브	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.1(2)	이 명령이 추가되었습니다.

사용 지침

사용자 이름 비밀번호 날짜를 표시하려면 **show running-config all username** 명령을 사용합니다.

CLI 프롬프트에서는 **username password-date** 값을 입력할 수 없습니다. 비밀번호 날짜는 비밀번호 정책 수명이 0이 아닌 경우에만 시작 구성에 저장됩니다. 즉, 비밀번호 날짜는 비밀번호 만료가 구성된 경우에만 저장됩니다. **password-date** 명령을 사용하여 사용자가 비밀번호 생성 날짜를 변경하지 못하도록 할 수 없습니다.

관련 명령

Command(명령)	설명
aaa authorization command	권한 부여 명령을 구성합니다.
clear config username	특정 사용자 또는 모든 사용자에 대한 컨피그레이션을 지웁니다.
show running-config username	특정 사용자 또는 모든 사용자에 대한 실행 중인 컨피그레이션을 표시합니다.

Command(명령)	설명
username attributes	특정 사용자에 대한 특성을 구성할 수 있는 username attributes 모드를 시작합니다.
webvpn	지정된 그룹에 대한 WebVPN 특성을 구성할 수 있는 config-group-webvpn 모드를 시작합니다.

username-prompt

보안 어플라이언스에 연결할 때 WebVPN 사용자에게 표시되는 WebVPN 페이지 로그인 상자의 사용자 이름 프롬프트를 사용자 지정하려면 webvpn customization 모드에서 **username-prompt** 명령을 사용합니다. 구성에서 명령을 제거하고 값을 상속받도록 하려면 **no** 형식의 다음 명령을 사용합니다.

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

구문 설명

text	텍스트를 변경하도록 지정합니다.
style	스타일을 변경하도록 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자)입니다.

기본값

사용자 이름 프롬프트의 기본 텍스트는 "USERNAME:" 입니다.

사용자 이름 프롬프트의 기본 스타일은 color:black;font-weight:bold;text-align:right입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
webvpn customization	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 유효한 모든 CSS(Cascading Style Sheet) 매개변수로 표현됩니다. 이러한 매개변수에 대한 설명은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트(www.w3.org)에서 CSS 사양을 참고하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수 목록이 포함되어 있습니다.

다음은 WebVPN 페이지에서 수행할 수 있는 가장 일반적인 변경(페이지 색상 변경) 작업에 대한 몇 가지 팁입니다.

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

참고 WebVPN 페이지를 쉽게 사용자 지정하려면 색상 견본 및 미리보기 기능 등 스타일 요소 컨피그레이션에 대한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예에서는 텍스트를 "Corporate Username:" 으로 변경하고, 기본 스타일을 굵기가 증가하는 글꼴 두께로 변경합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# username-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# username-prompt style font-weight:bolder
```

관련 명령

Command(명령)	설명
group-prompt	WebVPN 페이지의 그룹 프롬프트를 맞춤 설정합니다.
password-prompt	WebVPN 페이지의 비밀번호 프롬프트를 맞춤 설정합니다.

validate-attribute~vxlan port 명령

validate-attribute

RADIUS 어카운트 관리를 사용하여 RADIUS 특성을 확인하려면 **inspect radius-accounting** 명령을 사용하여 액세스할 수 있는 radius-accounting 파라미터 구성 모드에서 **validate attribute** 명령을 사용합니다.

이 옵션은 기본적으로 비활성화되어 있습니다.

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

구문 설명

attribute_number	RADIUS 어카운트 관리를 사용하여 확인할 RADIUS 특성입니다. 값 범위는 1~191입니다. 공급업체별 특성은 지원되지 않습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령이 구성된 경우 보안 어플라이언스는 프레임 IP 특성 외에 이러한 특성에서도 일치 작업을 수행합니다. 이 명령의 여러 인스턴스가 허용됩니다.

RADIUS 특성 유형의 목록은 다음 웹사이트에서 확인할 수 있습니다.
http://www.iana.org/assignments/radius-types

예

다음 예에서는 사용자 이름 RADIUS 특성에 대한 RADIUS 어카운트 관리를 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# validate attribute 1
```

관련 명령

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

validate-key

LISP 메시지에 대 한 사전 공유 키를 지정 하려면 파라미터 구성 모드에서 **key validate** 명령을 사용 합니다. 먼저 **policy-map type inspect lisp** 명령을 입력하여 파라미터 구성 모드에 액세스할 수 있습니다. 키를 제거하려면 이 명령의 **no** 형식을 사용합니다.

validate-key *key*

no validate-key *key*

구문 설명

key	LISP 메시지에 대한 사전 공유 키를 지정합니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.5(2)	이 명령이 추가되었습니다.

사용 지침

LISP 사전 공유 키를 지정하여 LISP 메시지 내용을 읽을 수 있도록 합니다.

클러스터 플로우 모빌리티에 대한 LISP 검사 정보

ASA는 위치 변경을 위해 LISP 트래픽을 검사한 다음 원활한 클러스터링 작동을 위해 이 정보를 사용합니다. LISP 통합 시 ASA 클러스터 멤버는 FHR(first hop router)과 ETR 또는 ITR 간에 전달되는 LISP 트래픽을 검사할 수 있으며, 그런 다음 플로우 소유자가 새 사이트에 있도록 변경할 수 있습니다.

클러스터 플로우 모빌리티에는 다음과 같은 여러 상호 관련 구성이 포함됩니다.

1. (선택 사항) Limit inspected EIDs based on the host or server IP address(호스트 또는 서버 IP 주소를 기반으로 검사된 EID 제한) - FHR(first hop router)은 ASA 클러스터와 관련되지 않은 호스트 또는 네트워크에 대한 EID-notify 메시지를 전송할 수 있습니다. 그러면 사용자는 클러스터와 관련된 서버 또는 네트워크로만 EDI를 제한할 수 있습니다. 예를 들어 클러스터와 관련된 사이트가 2개뿐이지만 LISP가 3개 사이트에서 실행 중인 경우, 클러스터와 관련된 2개 사이트에 대한 EID만 포함해야 합니다. **policy-map type inspect lisp**, **allowed-eid,** 및 **validate-key** 명령을 참고하십시오.

2. LISP traffic inspection(LISP 트래픽 검사) - ASA는 FHR(first hop router)과 ITR 또는 ETR 간에 EID-notify 메시지를 보낼 수 있도록 LISP 트래픽을 검사합니다. ASA는 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 관리합니다. 예를 들면, FHR(first hop router)의 소스 IP 주소 및 ITR 또는 ETR의 목적지 주소로 LISP 트래픽을 검사해야 합니다. **inspect lisp** 명령을 참고하십시오.
3. Service Policy to enable flow mobility on specified traffic(지정된 트래픽에서 플로우 모빌리티 활성화를 위한 서비스 정책) - 비즈니스 크리티컬 트래픽에서 플로우 모빌리티를 활성화해야 합니다. 예를 들어 플로우 모빌리티를 HTTPS 트래픽 또는 특정 서버에 대한 트래픽으로 제한할 수 있습니다. **cluster flow-mobility lisp** 명령을 참고하십시오.
4. Site IDs(사이트 ID) - ASA는 각 클러스터 유닛에 대해 사이트 ID를 사용하여 새로운 소유자를 확인합니다. **site-id** 명령을 참고하십시오.
5. Cluster-level configuration to enable flow mobility(플로우 모빌리티 활성화를 위한 클러스터 레벨 구성) - 또한 클러스터 레벨에서 플로우 모빌리티를 활성화해야 합니다. 이 켜기/끄기 토글을 사용하면 특정 클래스의 트래픽 또는 애플리케이션에 대한 플로우 모빌리티를 손쉽게 활성화 또는 비활성화할 수 있습니다. **flow-mobility lisp** 명령을 참고하십시오.

예

다음 예에서는 EID를 10.10.10.0/24 네트워크에 있는 것으로 제한하고 사전 공유 키를 지정합니다.

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

관련 명령

Command(명령)	설명
allowed-eids	IP 주소를 기준으로 검사한 EID를 제한합니다.
clear cluster info flow-mobility counters	플로우 모빌리티 카운터를 지웁니다.
clear lisp eid	ASA EID 테이블에서 EID를 제거합니다.
cluster flow-mobility lisp	서비스 정책에 대한 플로우 모빌리티를 활성화합니다.
flow-mobility lisp	클러스터에 대한 플로우 모빌리티를 활성화합니다.
inspect lisp	LISP 트래픽을 검사합니다.
policy-map type inspect lisp	LISP 검사를 맞춤 설정합니다.
site-id	클러스터 섀시의 사이트 ID를 설정합니다.
show asp table classify domain inspect-lisp	LISP 검사를 위한 ASP 테이블을 표시합니다.
show cluster info flow-mobility counters	플로우 모빌리티 카운터를 표시합니다.
show conn	LISP 흐름 모빌리티에 대한 트래픽 제목을 표시합니다.
show lisp eid	ASA EID 테이블을 표시합니다.
show service-policy	서비스 정책을 표시합니다.

validation-policy

트러스트 포인트를 사용하여 들어오는 사용자 연결과 연계된 인증서를 확인하는 조건을 지정하려면 crypto ca trustpoint 구성 모드에서 **validation-policy** 명령을 사용합니다. 명명된 조건에 트러스트 포인트를 사용할 수 없도록 지정하려면 이 명령의 **no** 형식을 사용합니다.

[no] validation-policy {ssl-client | ipsec-client} [no-chain] [subordinate-only]

구문 설명

ipsec-client	트러스트 포인트와 연계된 CA(인증 기관) 인증서 및 정책을 사용하여 IPsec 연결을 확인할 수 있도록 지정합니다.
no-chain	보안 장치에 없는 하위 인증서 체인을 비활성화합니다.
ssl-client	트러스트 포인트와 연계된 CA(인증 기관) 인증서 및 정책을 사용하여 SSL 연결을 확인할 수 있도록 지정합니다.
subordinate-only	이 트러스트 포인트가 나타내는 CA에서 직접 발급된 클라이언트 인증서의 검증을 비활성화합니다.

기본값

기본값 또는 동작은 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

명령 기록

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
crypto ca trustpoint 컨피그레이션	• 예	• 예	• 예	• 예	—

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

원격 액세스 VPN에서는 배포 요구 사항에 따라 SSL(Secure Sockets Layer), IPsec(IP 보안) 또는 둘 다를 사용하여 거의 모든 네트워크 애플리케이션 또는 리소스에 대한 액세스를 허용합니다. **validation-policy** 명령을 사용하여 온보드 CA 인증서에 액세스할 수 있는 프로토콜 유형을 지정할 수 있습니다.

이 명령에서 **no-chain** 옵션을 사용하면 ASA가 트러스트 포인트로로 구성되지 않은 하위 CA 인증서를 인증하지 않습니다.

ASA에는 CA가 동일한 두 개의 트러스트 포인트가 있을 수 있으며, 이 경우 동일한 CA에서 두 개의 ID 인증서가 생성됩니다. 트러스트 포인트가 이 기능을 활성화한 다른 트러스트 포인트에 이미 연결된 CA에 인증된 경우에는 이 옵션이 자동으로 비활성화됩니다. 따라서 경로 검증 파라미터의 선택

시 모호함이 방지됩니다. 사용자가 이 기능을 활성화한 다른 트러스트 포인트에 이미 연결된 CA에 인증된 트러스트 포인트에서 이 기능을 활성화하려고 하면 작업이 허용되지 않습니다. 두 개의 트러스트 포인트에서 이 설정을 활성화하고 동일한 CA에 인증할 수 없습니다.

예

다음 예에서는 central 트러스트 포인트에 대한 crypto ca trustpoint 구성 모드를 시작하고 이를 SSL 트러스트 포인트로로 지정합니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# validation-policy ssl
ciscoasa(config-ca-trustpoint)#
```

다음 예에서는 checkin1 트러스트 포인트에 대한 crypto ca trustpoint 구성 모드를 시작하고 지정된 트러스트 포인트의 하위 인증서를 허용하도록 설정합니다.

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# validation-policy subordinates-only
ciscoasa(config-ca-trustpoint)#
```

관련 명령

Command(명령)	설명
crypto ca trustpoint	신뢰 지점 컨피그레이션 모드를 시작합니다.
id-usage	트러스트 포인트의 등록된 ID를 사용할 수 있는 방법을 지정합니다.
ssl trust-point	인터페이스에 대한 SSL 인증서를 나타내는 인증서 트러스트 포인트를 지정합니다.

validation-usage

이 트러스트 포인트로로 검증할 수 있는 사용 유형을 지정하려면 crypto ca trustpoint 구성 모드에서 **validation-usage** 명령을 사용합니다. 사용 유형을 지정하지 않으려면 이 명령의 **no** 형식을 사용합니다.

validation-usage ipsec-client | ssl-client | ssl-server

no validation-usage ipsec-client | ssl-client | ssl-server

구문 설명

ipsec-client	이 트러스트 포인트를 사용하여 IPsec 클라이언트 연결을 검증할 수 있음을 나타냅니다.
ssl-client	이 트러스트 포인트를 사용하여 SSL 클라이언트 연결을 검증할 수 있음을 나타냅니다.
ssl-server	이 트러스트 포인트를 사용하여 SSL 서버 인증서를 검증할 수 있음을 나타냅니다.

기본값

ipsec-client, ssl-client

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
crypto ca trustpoint 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.0(1)	client-types 명령을 대체하기 위해 이 명령이 추가되었습니다.

사용 지침

여러 트러스트 포인트가 동일한 CA 인증서와 연결되었을 때 그중 하나만 특정 클라이언트 유형에 대해 구성될 수 있습니다. 그러나 이 트러스트 포인트 중 하나는 한 클라이언트 유형에, 다른 트러스트 포인트는 또 다른 클라이언트 유형에 구성하는 것이 가능합니다.

이미 어떤 클라이언트 유형으로 구성된 CA 인증서에 어떤 트러스트 포인트가 연결될 경우 새 트러스트 포인트는 동일한 클라이언트 유형 설정으로 구성될 수 없습니다. 이 명령의 **no** 형식은 설정을 지워 어떤 클라이언트 검증에서도 트러스트 포인트를 사용할 수 없게 합니다.

원격 액세스 VPN에서는 배포 요구 사항에 따라 SSL(Secure Sockets Layer), IPsec(IP 보안) 또는 둘 다를 사용하여 모든 네트워크 애플리케이션 또는 리소스에 대한 액세스를 허용합니다.

관련 명령

Command(명령)	설명
crypto ca trustpoint	지정된 트러스트 포인트에 대한 crypto ca trustpoint 구성 모드를 시작합니다.

vdi

XenApp 및 XenDesktop VDI 서버가 ASA 서버를 통해 모바일 장치에서 실행되는 Citrix Receiver 애플리케이션에 안전하게 원격 액세스할 수 있도록 하려면 **vdi** 명령을 사용합니다.

vdi type citrix url *url* **domain** *domain* **username** *username* **password** *password*

구문 설명

domain *domain*	가상화 인프라 서버에 로그인하는 데 사용되는 도메인입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
password *password*	가상화 인프라 서버에 로그인하는 데 사용되는 비밀번호입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.
type	VDI의 유형입니다. Citrix Receiver 유형의 경우 이 값은 *citrix*입니다.
url *url*	http 또는 https, 호스트 이름, 포트 번호 및 XML 서비스의 경로를 포함하는 XenApp 또는 XenDesktop 서버의 전체 URL입니다.
username *username*	가상화 인프라 서버에 로그인하는 데 사용되는 사용자 이름입니다. 이 값은 클라이언트리스 매크로일 수 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
webvpn 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.0(1)	이 명령이 추가되었습니다.

사용 지침

VDI 모델의 경우 관리자는 엔터프라이즈 애플리케이션과 함께 미리 로드된 데스크톱을 게시하고 엔드 유저는 이러한 데스크톱에 원격으로 액세스합니다. 이러한 가상화된 리소스는 사용자가 Citrix Access Gateway를 통하지 않고도 액세스할 수 있도록 이메일 등의 다른 리소스와 동일하게 표시됩니다. 사용자가 Citrix Receiver 모바일 클라이언트를 사용하여 ASA에 로그온하면 ASA는 미리 정의된 Citrix XenApp 또는 XenDesktop 서버에 연결합니다. 관리자는 사용자가 Citrix 가상화 리소스에 연결할 때 Citrix 서버의 주소 및 크리덴셜을 가리키는 대신 ASA의 SSL VPN IP 주소 및 크리덴셜을 입력하도록 Citrix 서버의 주소 및 로그온 크리덴셜을 그룹 정책에 구성해야 합니다. ASA에서 크리덴셜을 확인하면 수신기 클라이언트가 ASA를 통해 등록된 애플리케이션 검색을 시작합니다.

지원되는 모바일 디바이스

- iPad — Citrix Receiver 4.x 이상 버전
- iPhone/iTouch — Citrix Receiver 4.x 이상 버전
- Android 2.x 전화 - Citrix Receiver 버전 2.x 이상

- Android 3.x 태블릿 - Citrix Receiver 버전 2.x 이상
- Android 4.0 전화기 — Citrix Receiver 2.x 이상 버전

예

사용자 이름과 그룹 정책을 둘 다 구성한 경우에는 사용자 이름 설정이 그룹 정책보다 우선적으로 적용됩니다.

```
configure terminal
    group-policy DfltGrpPolicy attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>
configure terminal
    username <username> attributes
        webvpn
            vdi type <citrix> url <url> domain <domain> username <username> password
            <password>]
```

관련 명령

Command(명령)	설명
debug webvpn citrix	Citrix 기반 애플리케이션 및 데스크톱을 시작하는 프로세스에 대한 정보를 제공합니다.

verify

파일의 체크섬을 확인하려면 특권 EXEC 모드에서 **verify** 명령을 사용합니다.

verify *path*

verify {**/md5** | **sha-512**} *path* [*expected_value*]

verify /signature running

구문 설명

/md5	지정된 소프트웨어 이미지의 MD5 값을 계산하고 표시합니다. 이 값을 Cisco.com에서 이 이미지에 사용할 수 있는 값과 비교합니다.
/sha-512	지정된 소프트웨어 이미지의 SHA-512 값을 계산하고 표시합니다. 이 값을 Cisco.com에서 이 이미지에 사용할 수 있는 값과 비교합니다.
/signature running	실행 중인 ASA 이미지의 서명을 확인합니다.
expected_value	(선택 사항) 지정된 이미지에 대해 알려진 해시 값입니다. ASA는 해시된 값이 일치하는지 여부를 확인하는 메시지를 표시합니다.
path	• **disk0:/**[*path/*]*filename* 내부 플래시 메모리를 나타냅니다. 또한 **disk0** 대신 별칭이 지정된 **flash**를 사용할 수도 있습니다. • **disk1:/**[*path/*]*filename* 외부 플래시 메모리 카드를 나타냅니다. • **flash:/**[*path/*]*filename* 이 옵션은 내부 플래시 카드를 나타냅니다. **flash**는 **disk0:**의 별칭입니다. • **ftp://**[*user*[**:***password*]**@**]*server*[:*port*]**/**[*path/*]*filename*[**;type=***xx*] **type**은 다음 키워드 중 하나일 수 있습니다. – **ap** - ASCII 패시브 모드 – **an** - ASCII 일반 모드 – **ip** - (기본값) 이진 패시브 모드 – **in** - 이진 일반 모드 • **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]**/**[*path/*]*filename* • **tftp://**[*user*[**:***password*]**@**]*server*[:*port*]**/**[*path/*]*filename*[**;int=***interface_name*] 서버 주소의 경로를 재정의하려면 인터페이스 이름을 지정합니다. 경로 이름은 공백을 포함할 수 없습니다. 경로 이름에 공백이 있으면 **verify** 명령 대신 **tftp-server** 명령에서 경로를 설정합니다. • **system:running-config** 실행 중인 구성에 대한 해시를 계산하거나 확인합니다. • **system:text** ASA 프로세스의 텍스트에 대한 해시를 계산하거나 확인합니다.

기본값

현재 플래시 디바이스가 기본 파일 시스템입니다.

참고

/md5 또는 **/sha-512** 옵션을 지정한 경우 FTP, HTTP, TFTP 등의 네트워크 파일을 소스로 사용할 수 있습니다. **verify** 명령을 **/md5** 또는 **/sha-512** 옵션 없이 사용하면 플래시의 로컬 이미지만 확인할 수 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	—	• 예

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.
9.3(2)	**signature** 키워드가 추가되었습니다.
9.6(2)	**system:text** 옵션이 추가되었습니다.

사용 지침

verify 명령을 사용하여 파일을 사용하기 전에 해당 체크섬을 확인할 수 있습니다.

디스크에 분산되어 있는 각 소프트웨어 이미지는 전체 이미지에 단일 체크섬을 사용합니다. 이 체크섬은 이미지가 플래시 메모리에 복사된 경우에만 표시되며, 이미지 파일이 디스크 간에 복사된 경우에는 표시되지 않습니다.

이미지를 플래시 메모리 또는 서버에 복사할 때 체크섬을 확인하려면 새 이미지를 로드하거나 복제하기 전에 이미지의 체크섬 및 MD5 정보를 기록해야 합니다. 다양한 이미지 정보를 Cisco.com에서 사용할 수 있습니다.

플래시 메모리의 내용을 보려면 **show flash:** 명령을 사용합니다. 플래시 내용 목록에는 개별 파일의 체크섬이 포함되지 않습니다. 이미지를 플래시 메모리에 복사한 후 이미지 체크섬을 다시 계산하고 확인하려면 **verify** 명령을 사용합니다. 그러나 **verify** 명령은 파일 시스템 저장된 이후의 파일 무결성만 확인합니다. 손상된 이미지가 ASA로 전송되어 탐지되지 않은 상태로 파일 시스템에 저장될 수 있습니다. 손상된 이미지가 ASA로 전송된 경우 소프트웨어는 이미지가 손상되었음을 알려 줄 수 없으므로 파일이 성공적으로 확인됩니다.

MD5(message-digest5) 해시 알고리즘을 사용하여 파일을 검증하려면 **/md5** 옵션과 함께 **verify** 명령을 사용합니다. MD5는 고유한 128비트 메시지 다이제스트를 생성하여 데이터 무결성을 확인하는 데 사용되는 알고리즘입니다(RFC 1321에 정의됨). **/md5** 옵션(**verify** 명령과 함께 사용)은 MD5 체크섬 값을 이미지에 대해 알려진 MD5 체크섬 값과 비교하여 ASA 소프트웨어 이미지의 무결성을 확인할 수 있도록 합니다. 이제 로컬 시스템 이미지 값과 비교할 수 있도록 모든 보안 어플라이언스 소프트웨어 이미지의 MD5 값을 Cisco.com에서 사용할 수 있습니다.
SHA-512(**/sha-512**)를 지정할 수도 있습니다.

MD5 또는 SHA-512 무결성 확인을 수행하려면 **/md5** 또는 **/sha-512** 키워드를 사용하여 **verify** 명령을 실행합니다. 예를 들어 **verify /md5 flash:cdisk.bin** 명령을 실행하면 소프트웨어 이미지의 MD5 값이 계산되고 표시됩니다. 이 값을 Cisco.com에서 이 이미지에 사용할 수 있는 값과 비교합니다.

또는 먼저 Cisco.com에서 MD5 값을 가져온 다음 명령 구문에서 이 값을 지정합니다. 예를 들어 **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** 명령을 실행하면 MD5 값이 일치하는지 또는 불일치가 있는지 확인하는 메시지가 표시됩니다. MD5 값의 불일치는 이미지가 손상되었거나 잘못된 MD5 값이 입력되었음을 의미합니다.

예

다음 예에서는 cdisk.bin이라는 이미지 파일에 사용된 **verify** 명령을 보여 줍니다. 일부 텍스트는 명확성을 위해 제거되었습니다.

```
ciscoasa# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
ciscoasa#
```

다음 예에서는 disk0의 서명 이미지에 사용된 **verify** 명령을 보여 줍니다.

```
ciscoasa(config)# verify lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6

Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6


Digital signature successfully validate

ciscoasa(config)# verify /signature lfbff.SSA
Verifying file integrity of disk0:/lfbff.SSA
Computed Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6

Embedded Hash   SHA2: 7d4e8531f4552458b90f8619ca76a76b
                      2c8751668b060981f95ded6fcca92d21
                      e7fc950834209ab162e2b4daaa8b38e4
                      28eaa48e1895919b817b79e4ead0dfd6


Digital signature successfully validated
ciscoasa(config)# verify /signature cdisk.smp
Verifying file integrity of disk0:/cdisk.smp
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!Done!
Embedded Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc
6cc420aadfff8db42fae6088bc74959fcbc11f
```

```
Computed Hash SHA-512:
b4a6195420d336aa4bb99f26ef30005ee45a7e422937e542153731dae03f974757b6a8829fbc509d6114f203cc
6cc420aadfff8db42fae6088bc74959fcbc11f
CCO Hash      SHA-512:
cd5d459b6d2616e3530d9ed7c488b5a1b51269f19ad853fbf9c630997e716ded4fda61fa2afe6e293dc82f0599
7fd787b0ec22839c92a87a37811726e152fade
Signature Verified
ciscoasa(config)#
ciscoasa(config)# verify /signature corrupt.SSA
%ERROR: Signature algorithm not supported for file disk0:/corrupt.SSA.
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
copy	파일을 복사합니다.
dir	시스템의 파일을 나열합니다.

verify-header

알려진 IPv6 확장 헤더만 허용하고 IPv6 확장 헤더의 순서를 적용하려면 파라미터 구성 모드에서 **verify-header** 명령을 사용합니다. 먼저 **policy-map type inspect ipv6** 명령을 입력하여 파라미터 구성 모드에 액세스할 수 있습니다. 이러한 파라미터를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

verify-header {**order** | **type**}

no verify-header {**order** | **type**}

구문 설명

order	RFC 2460 사양에 정의된 대로 IPv6 확장 헤더의 순서를 적용합니다.
type	알려진 IPv6 확장 헤더만 허용합니다.

명령 기본값

order와 type 둘 다 기본적으로 활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		**보안 상황**		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
파라미터 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	**수정 사항**
8.2(1)	이 명령이 추가되었습니다.

사용 지침

이러한 파라미터는 기본적으로 활성화되어 있습니다. 비활성화하려면 no 키워드를 입력합니다.

예

다음 예에서는 IPv6 검사 정책 맵에 대한 order 및 type 파라미터를 비활성화합니다.

```
ciscoasa(config)# policy-map type inspect ipv6 ipv6-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# no verify-header order
ciscoasa(config-pmap-p)# no verify-header type
```

관련 명령

Command(명령)	**설명**
inspect ipv6	IPv6 검사를 활성화합니다.
parameters	검사 정책 맵에 대한 파라미터 구성 모드를 시작합니다.
policy-map type inspect ipv6	IPv6 검색 정책 맵을 만듭니다.

버전

ASA에서 전역적으로 사용되는 RIP 버전을 지정하려면 라우터 구성 모드에서 **version** 명령을 사용합니다. 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

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

no version

구문 설명

1	RIP 버전 1을 지정합니다.
2	RIP 버전 2을 지정합니다.

기본값

ASA는 버전 1 및 버전 2 패킷을 허용하지만 버전 1 패킷만 보냅니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
라우터 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

인터페이스에서 **rip send version** 및 **rip receive version** 명령을 입력하여 인터페이스별로 전역 설정을 재정의할 수 있습니다.

RIP 버전 2를 지정한 경우 네이버 인증을 활성화하고 MD5 기반 암호화를 사용하여 RIP 업데이트를 인증할 수 있습니다.

예

다음 예에서는 ASA가 모든 인터페이스에서 RIP 버전 2 패킷을 보내고 받도록 구성합니다.

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
```

관련 명령

Command(명령)	설명
rip send version	특정 인터페이스에서 업데이트를 전송할 때 사용할 RIP 버전을 지정합니다.
rip receive version	특정 인터페이스에서 업데이트를 수신할 때 허용할 RIP 버전을 지정합니다.
router rip	RIP 라우팅 프로세스를 활성화하고 해당 프로세스에 대해 라우터 구성 모드를 시작합니다.

virtual http

가상 HTTP 서버를 구성하려면 전역 구성 모드에서 **virtual http** 명령을 사용합니다. 가상 서버를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

구문 설명

ip_address	ASA에서 가상 HTTP 서버의 IP 주소를 설정합니다. 이 주소가 ASA로 라우팅되는 사용되지 않는 주소인지 확인합니다.
warning	(선택 사항) HTTP 연결을 ASA로 리디렉션해야 함을 사용자에게 알립니다. 이 키워드는 리디렉션이 자동으로 발생할 수 없는 텍스트 기반 브라우저에만 적용됩니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이전 릴리스에서 사용되는 인라인 기본 HTTP 인증 방법이 리디렉션 방법으로 대체되었으므로 이 명령은 사용이 중단되었습니다. 더 이상 이 명령이 필요하지 않습니다.
7.2(2)	이제 **aaa authentication listener** 명령을 사용하여 기본 HTTP 인증(기본값)과 HTTP 리디렉션 중에 선택할 수 있으므로 이 명령이 다시 사용되었습니다. 리디렉션 방법에는 연속 HTTP 인증을 위한 추가 명령이 필요 없습니다.

사용 지침

ASA에서 HTTP 인증(**aaa authentication match** 또는 **aaa authentication include** 명령 참고)을 사용하는 경우 ASA는 기본적으로 기본 HTTP 인증을 사용합니다. **redirect** 키워드와 함께 **aaa authentication listener** 명령을 사용하여 ASA가 HTTP 연결을 ASA 자체에서 생성한 웹 페이지로 리디렉션하도록 인증 방법을 변경할 수 있습니다.

그러나 기본 HTTP 인증을 계속 사용하는 경우에는 연속 HTTP 인증이 있을 때 **virtual http** 명령이 필요할 수도 있습니다.

대상 HTTP 서버가 ASA 이외에 인증을 요구하는 경우 **virtual http** 명령을 사용하면 ASA(AAA 서버를 통해) 및 HTTP 서버에서 별도로 인증할 수 있습니다. 가상 HTTP를 사용하지 않으면 ASA에 인증하는 데 사용한 동일한 사용자 이름 및 비밀번호가 HTTP 서버로 전송됩니다. HTTP 서버 사용자 이름 및 비밀번호에 대한 프롬프트가 별도로 표시되지 않습니다. 사용자 이름 및 비밀번호가 AAA 서버와 HTTP 서버에 대해 동일하지 않으면 HTTP 인증에 실패합니다.

이 명령은 AAA 인증이 필요한 모든 HTTP 연결을 ASA의 가상 HTTP 서버로 리디렉션합니다. ASA는 AAA 서버 사용자 이름 및 비밀번호를 묻는 프롬프트를 표시합니다. AAA 서버가 사용자를 인증한 후 ASA는 HTTP 연결을 원래 서버로 다시 리디렉션하지만 AAA 서버 사용자 이름 및 비밀번호는 포함하지 않습니다. 사용자 이름 및 비밀번호가 HTTP 패킷에 포함되어 있지 않기 때문에 HTTP 서버는 사용자에게 HTTP 서버 사용자 이름 및 비밀번호에 대한 프롬프트를 별도로 표시합니다.

인바운드 사용자의 경우(낮은 보안 수준에서 높은 보안 수준으로) 소스 인터페이스에 적용되는 액세스 목록에 가상 HTTP 주소를 대상 인터페이스로 포함해야 합니다. 또한 NAT가 필요 없는 경우(**no nat-control** 명령 사용)에도 가상 HTTP IP 주소에 대한 **static** 명령을 추가해야 합니다. ID NAT 명령은 일반적으로 사용됩니다(주소를 자체로 변환하는 경우).

아웃바운드 사용자의 경우 트래픽이 명시적으로 허용되지만 내부 인터페이스에 액세스 목록을 적용할 때는 가상 HTTP 주소에 대한 액세스를 허용해야 합니다. **static** 문은 필요하지 않습니다.

참고 **virtual http** 명령을 사용할 때는 **timeout uauth** 명령 기간을 0초로 설정하지 마십시오. 이 설정은 실제 웹 서버에 대한 HTTP 연결을 방지하기 때문입니다.

예

다음 예에서는 AAA 인증과 함께 가상 HTTP를 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# virtual http 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list ACL-IN remark This is the HTTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list ACL-IN remark This is the virtual HTTP address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
ciscoasa(config)# access-list AUTH remark This is the HTTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
ciscoasa(config)# access-list AUTH remark This is the virtual HTTP address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

관련 명령

Command(명령)	설명
aaa authentication listener http	ASA가 인증하는 방법을 설정합니다.
clear configure virtual	컨피그레이션에서 **virtual** 명령문을 제거합니다.
show running-config virtual	ASA 가상 서버의 IP 주소를 표시합니다.
sysopt uauth allow-http-cache	**virtual http** 명령을 활성화한 경우 이 명령을 통해 브라우저 캐시에서 사용자 이름 비밀번호를 사용하여 가상 서버에 다시 연결할 수 있습니다.
virtual telnet	사용자가 인증이 필요한 다른 유형의 연결을 시작하기 전에 ASA에 인증할 수 있도록 ASA에서 가상 텔넷 서버를 제공합니다.

virtual telnet

ASA에서 가상 텔넷 서버를 구성하려면 전역 구성 모드에서 **virtual telnet** 명령을 사용합니다. ASA가 인증 프롬프트를 제공하지 않는 다른 유형의 트래픽에 대한 인증이 필요한 경우 가상 텔넷 서버에 사용자를 인증해야 할 수도 있습니다. 서버를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

virtual telnet *ip_address*

no virtual telnet *ip_address*

구문 설명

ip_address	ASA에서 가상 텔넷 서버의 IP 주소를 설정합니다. 이 주소가 ASA로 라우팅되는 사용되지 않는 주소인지 확인합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다 .

사용 지침

프로토콜 또는 서비스에 대한 네트워크 액세스 인증을 구성할 수 있지만(**aaa authentication match** 또는 **aaa authentication include** 명령 참고) HTTP, 텔넷 또는 FTP로만 직접 인증할 수 있습니다. 사용자는 인증이 필요한 다른 트래픽이 허용되기 전에 먼저 이러한 서비스 중 하나로 인증해야 합니다. ASA를 통한 HTTP, 텔넷 또는 FTP를 허용하지 않고 다른 유형의 트래픽을 인증하도록 하려는 경우 가상 텔넷을 구성할 수 있습니다. 사용자가 ASA에 구성된 지정된 IP 주소로 텔넷하면 ASA에서 텔넷 프롬프트를 제공합니다.

가상 텔넷 주소뿐만 아니라 **authentication match** 또는 **aaa authentication include** 명령을 사용하여 인증할 다른 서비스에 대한 텔넷 액세스의 인증을 구성해야 합니다.

인증되지 않은 사용자가 가상 텔넷 IP 주소에 연결하면 사용자 이름 및 비밀번호를 묻는 메시지가 나타나며 AAA 서버에서 사용자를 인증해야 합니다. 인증되면 사용자에게 "Authentication Successful(인증 성공)" 메시지가 표시됩니다. 그런 다음 사용자는 인증을 요구하는 다른 서비스에 성공적으로 액세스할 수 있습니다.

인바운드 사용자의 경우(낮은 보안 수준에서 높은 보안 수준으로) 소스 인터페이스에 적용되는 액세스 목록에 가상 텔넷 주소를 대상 인터페이스로 포함해야 합니다. 또한 NAT가 필요 없는 경우(**no nat-control** 명령 사용)에도 가상 텔넷 IP 주소에 대한 **static** 명령을 추가해야 합니다. ID NAT 명령은 일반적으로 사용됩니다(주소를 자체로 변환하는 경우).

아웃바운드 사용자의 경우 트래픽이 명시적으로 허용되지만 내부 인터페이스에 액세스 목록을 적용할 때는 가상 텔넷 주소에 대한 액세스를 허용해야 합니다. **static** 문은 필요하지 않습니다.

ASA에서 로그아웃하려면 가상 텔넷 IP 주소에 다시 연결합니다. 로그아웃할지 묻는 프롬프트가 나타납니다.

예

다음 예에서는 다른 서비스에 대해 AAA 인증과 함께 가상 텔넷을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# virtual telnet 209.165.202.129
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list ACL-IN remark This is the SMTP server on the inside
ciscoasa(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
ciscoasa(config)# access-list ACL-IN remark This is the virtual Telnet address
ciscoasa(config)# access-group ACL-IN in interface outside
ciscoasa(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
ciscoasa(config)# access-list AUTH remark This is the SMTP server on the inside
ciscoasa(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
ciscoasa(config)# access-list AUTH remark This is the virtual Telnet address
ciscoasa(config)# aaa authentication match AUTH outside tacacs+
```

관련 명령

Command(명령)	설명
clear configure virtual	구성에서 **virtual** 명령문을 제거합니다.
show running-config virtual	ASA 가상 서버의 IP 주소를 표시합니다.
virtual http	ASA에서 HTTP 인증을 사용하고 HTTP 서버에서도 인증을 요구하는 경우 이 명령을 통해 ASA 및 HTTP 서버에서 개별적으로 인증할 수 있습니다. 가상 HTTP를 사용하지 않으면 ASA에 인증하는 데 사용한 동일한 사용자 이름 및 비밀번호가 HTTP 서버로 전송됩니다. HTTP 서버 사용자 이름 및 비밀번호에 대한 프롬프트가 별도로 표시되지 않습니다.

vlan (group-policy)

그룹 정책에 VLAN을 할당하려면 group-policy 구성 모드에서 **vlan** 명령을 사용합니다. VLAN을 그룹 정책의 구성에서 제거하고 기본 그룹 정책의 VLAN 설정으로 대체하려면 이 명령의 **no** 형식을 사용합니다.

[**no**] **vlan** {*vlan_id* |**none**}

구문 설명

none	이 그룹 정책과 일치하는 원격 액세스 VPN 세션에 대한 VLAN 할당을 비활성화합니다. 그룹 정책은 기본 그룹 정책에서 vlan 값을 상속하지 않습니다.
vlan_id	이 그룹 정책을 사용하는 원격 액세스 VPN 세션에 할당할 VLAN 수(10진수 형식)입니다. 인터페이스 구성 모드에서 **vlan** 명령을 사용하여 이 ASA에서 VLAN을 구성해야 합니다.

기본값

기본값은 없음입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
8.0(2)	이 명령이 추가되었습니다.

사용 지침

This command specifies the egress VLAN interface for sessions assigned to this group policy.

ASA는 이 그룹의 모든 트래픽을 해당 VLAN으로 전달합니다. 각 그룹 정책에 VLAN을 할당하여 액세스 제어를 간소화할 수 있습니다. ACL을 사용하는 대신 이 명령을 사용하여 세션에서 트래픽을 필터링합니다.

VoIP 검사 엔진(CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), DNS 검사 엔진 또는 DCE RPC 검사 엔진을 vlan mapping 옵션에 사용하지 마십시오. 이러한 검사 엔진은 vlan-mapping 설정을 무시하므로 패킷이 잘못 라우팅될 수 있습니다.

예

다음 명령은 그룹 정책에 VLAN 1을 할당합니다.

```
ciscoasa(config-group-policy)# vlan 1
ciscoasa(config-group-policy)
```

다음 명령은 그룹 정책에서 VLAN 매핑을 제거합니다.

```
ciscoasa(config-group-policy)# vlan none
ciscoasa(config-group-policy)
```

관련 명령

Command(명령)	설명
show vlan	ASA에 구성된 VLAN을 표시합니다.
vlan(인터페이스 구성 모드)	하위 인터페이스에 VLAN ID를 할당합니다.
show vpn-session_summary.db	IPsec, Cisco AnyConnect 및 NAC 세션 수와 사용 중인 VLAN 수를 표시합니다.
show vpn-session.db	VLAN 매핑 및 NAC 결과를 포함하여 VPN 세션에 대한 정보를 표시합니다.

vlan (interface)

하위 인터페이스에 VLAN ID를 할당하려면 인터페이스 구성 모드에서 **vlan** 명령을 사용합니다. VLAN ID를 제거하려면 이 명령의 **no** 형식을 사용합니다. 하위 인터페이스에서 트래픽을 전달하려면 VLAN ID가 필요합니다. VLAN 하위 인터페이스를 사용하면 단일 물리적 인터페이스에서 여러 논리적 인터페이스를 구성할 수 있습니다. VLAN은 지정된 물리적 인터페이스에서 트래픽을 별도로 유지할 수 있도록 해줍니다(예: 다중 보안 상황의 경우).

vlan *id* [**secondary** *vlan_range*]

no vlan [**secondary** ***vlan_range***]

구문 설명

id	1~4094의 정수를 지정합니다. 일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로 스위치 설명서에서 자세한 내용을 확인하십시오.
secondary *vlan_range*	(선택 사항) 하나 이상의 보조 VLAN을 지정합니다. *vlan_id*는 1 ~ 4094의 정수입니다. 일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로 스위치 설명서에서 자세한 내용을 확인하십시오. 보조 VLAN은 공백, 쉼표 및 대시(연속된 범위)로 구분할 수 있습니다. ASA가 보조 VLAN에서 트래픽을 수신할 경우 트래픽을 기본 VLAN에 매핑합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
인터페이스 구성	• 예	• 예	• 예	—	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령은 **interface** 명령 키워드에서 인터페이스 구성 모드 명령으로 이동되었습니다.
9.5(2)	**secondary** 키워드가 추가되었습니다.

사용 지침

기본 VLAN뿐만 아니라 하나 이상의 보조 VLAN을 구성할 수 있습니다. ASA가 보조 VLAN에서 트래픽을 수신할 경우 ASA는 트래픽을 기본 VLAN에 매핑합니다. 각 하위 인터페이스는 VLAN ID가 있어야 트래픽을 전달할 수 있습니다. VLAN ID를 변경하려는 경우 **no** 옵션을 사용하여 이전 VLAN ID를 제거할 필요가 없습니다. 다른 VLAN ID와 함께 **vlan** 명령을 입력하면 ASA가 이전 ID를 변경합니다. 목록에서 보조 VLAN 중 일부를 제거하려면 **no** 명령을 사용하여 제거할 VLAN만 나열하면 됩니다. 나열된 VLAN만 선택적으로 제거할 수 있습니다. 예를 들어, 단일 VLAN을 범위에서 제거할 수는 없습니다.

하위 인터페이스를 활성화하려면 **no shutdown** 명령을 사용하여 물리적 인터페이스를 활성화해야 합니다. 하위 인터페이스를 활성화한 경우 물리적 인터페이스에서도 트래픽을 전달하도록 하지 않는 것이 일반적입니다. 물리적 인터페이스는 태그가 지정되지 않은 패킷을 전달하기 때문입니다. 따라서 인터페이스 수준을 낮춰 트래픽이 물리적 인터페이스를 통해 전달되지 않도록 할 수 없습니다. 대신 **nameif** 명령을 생략하여 물리적 인터페이스가 트래픽을 전달하지 않도록 합니다. 물리적 인터페이스에서 태그가 지정되지 않은 패킷을 전달할 수 있도록 하려면 **nameif** 명령을 평소와 같이 구성하면 됩니다.

최대 하위 인터페이스 수는 플랫폼에 따라 다릅니다. 플랫폼당 최대 하위 인터페이스 수는 CLI 구성 가이드를 참고하십시오.

예

다음 예에서는 하위 인터페이스에 VLAN 101을 할당합니다.

```
ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

다음 예에서는 VLAN을 102로 변경합니다.

```
ciscoasa(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
  vlan 101
  nameif dmz1
  security-level 50
  ip address 10.1.2.1 255.255.255.0

ciscoasa(config)# interface gigabitethernet0/0.1
ciscoasa(config-interface)# vlan 102

ciscoasa(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
  vlan 102
  nameif dmz1
  security-level 50
  ip address 10.1.2.1 255.255.255.0
```

다음 예에서는 보조 VLAN 집합을 VLAN 200에 매핑합니다.

```
interface gigabitethernet 0/6.200
    vlan 200 secondary 500 503 600-700
```

다음 예에서는 보조 VLAN 503을 목록에서 제거합니다.

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
    vlan 200 secondary 500 600-700
    no nameif
    no security-level
    no ip address
```

다음 예에는 VLAN 매핑이 Catalyst 6500에서 작동하는 방식이 나와 있습니다. PVLAN에 노드를 연결하는 방법에 대한 내용은 Catalyst 6500 구성 가이드를 참조하십시오.

ASA 컨피그레이션

```
interface GigabitEthernet1/1
      description Connected to Switch GigabitEthernet1/5
      no nameif
      no security-level
      no ip address
      no shutdown
!
interface GigabitEthernet1/1.70
      vlan 70 secondary 71 72
      nameif vlan_map1
      security-level 50
      ip address 10.11.1.2 255.255.255.0
      no shutdown
!
interface GigabitEthernet1/2
      nameif outside
      security-level 0
      ip address 172.16.171.31 255.255.255.0
      no shutdown
```

Catalyst 6500 구성

```
vlan 70
      private-vlan primary
      private-vlan association 71-72
!
vlan 71
      private-vlan community
!
vlan 72
      private-vlan isolated
!
interface GigabitEthernet1/5
      description Connected to ASA GigabitEthernet1/1
      switchport
      switchport trunk encapsulation dot1q
      switchport trunk allowed vlan 70-72
      switchport mode trunk
!
```

관련 명령

Command(명령)	설명
allocate-interface	인터페이스 및 하위 인터페이스를 보안 상황에 할당합니다.
interface	인터페이스를 구성하고 인터페이스 구성 모드를 시작합니다.
show running-config interface	인터페이스의 현재 구성을 표시합니다.

vpdn group

vpdn 그룹을 만들거나 수정하고 PPPoE 클라이언트 설정을 구성하려면 전역 구성 모드에서 **vpdn group** 명령을 사용합니다. 구성에서 그룹 정책을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpdn group *group_name* {**localname** ***username*** | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

no vpdn group *group_name* {**localname** ***name*** | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

참고 PPPoE는 ASA에 장애 조치가 구성된 경우 또는 다중 상황 모드나 투명 모드에서 지원되지 않습니다. PPPoE는 장애 조치 없는 단일 라우팅 모드에서만 지원됩니다.

구문 설명

localname *username*	인증을 위해 사용자 이름을 vpdn 그룹에 연결하며, **vpdn username** 명령으로 구성된 이름과 일치해야 합니다.
ppp authentication {chap | mschap | pap}}	PPP(Point-to-Point 프로토콜) 인증 프로토콜을 지정합니다. Windows 클라이언트 전화 접속 네트워킹 설정을 통해 사용할 인증 프로토콜(PAP, CHAP 또는 MS-CHAP)을 지정할 수 있습니다. 클라이언트에서 지정한 모든 항목은 보안 어플라이언스에서 사용하는 설정과 일치해야 합니다. PAP(비밀번호 인증 프로토콜)는 PPP 피어가 상호 인증할 수 있도록 해줍니다. PAP는 호스트 이름 또는 사용자 이름을 일반 텍스트로 전달합니다. CHAP(Challenge Handshake Authentication Protocol)는 PPP 피어가 액세스 서버와의 상호 작용을 통해 무단 액세스를 방지할 수 있도록 해줍니다. MS-CHAP는 Microsoft의 파생 CHAP입니다. PIX 방화벽은 MS-CHAP 버전 1만 지원합니다(버전 2.0은 지원하지 않음). 인증 프로토콜이 호스트에 지정되지 않은 경우에는 구성에서 **ppp authentication** 옵션을 지정하지 마십시오.
request dialout pppoe	외부로 전화 접속 PPPoE 요청을 허용하려면 지정합니다.
vpdn group *group_name*	vpdn 그룹의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• **예**		—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

VPDN(Virtual Private Dial-up Networking)은 원격 전화 접속 사용자와 사설 네트워크 간의 장거리 포인트투포인트 연결을 제공하는 데 사용됩니다. 보안 어플라이언스의 VPDN은 계층 2 터널링 기술 PPPoE를 사용하여 공용 네트워크를 통해 원격 사용자와 사설 네트워크 간의 전화 접속 네트워킹 연결을 설정합니다.

PPPoE는 PPP(Point-to-Point 프로토콜) over Ethernet입니다. PPP는 IP, IPX 및 ARA와 같은 네트워크 계층 프로토콜과 함께 작동하도록 설계되었습니다. 또한 PPP는 CHAP 및 PAP를 기본 제공 보안 메커니즘으로 사용합니다.

show vpdn session pppoe 명령은 PPPOE 연결에 대한 세션 정보를 표시합니다. **clear configure vpdn group** 명령은 모든 **vpdn group** 명령을 구성에서 제공하고 모든 활성 L2TP 및 PPPoE 터널을 중지합니다. **clear configure vpdn username** 명령은 모든 **vpdn username** 명령을 구성에서 제거합니다.

PPPoE는 PPP를 캡슐화하기 때문에 PPPoE는 PPP를 기반으로 VPN 터널 내에서 작동하는 클라이언트 세션에 대한 인증 및 ECP/CCP 기능을 수행합니다. 또한 PPP는 PPPoE에 대한 IP 주소를 할당하기 때문에 PPPoE는 DHCP와 함께 지원되지 않습니다.

참고 PPPoE에 대한 VPDN 그룹이 구성되지 않은 경우에는 PPPoE에서 연결을 설정할 수 없습니다.

PPPoE에 사용할 VPDN 그룹을 정의하려면 **vpdn group** *group_name* **request dialout pppoe** 명령을 사용합니다. 그런 다음 인터페이스 구성 모드에서 **pppoe client vpdn group** 명령을 사용하여 특정 인터페이스의 PPPoE 클라이언트와 VPDN 그룹을 연결합니다.

ISP에서 인증을 요구하는 경우 **vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} 명령을 사용하여 ISP에서 사용하는 인증 프로토콜을 선택합니다.

vpdn group *group_name* **localname** *username* 명령을 사용하여 ISP에서 할당한 사용자 이름을 VPDN 그룹과 연결합니다.

vpdn username *username* password *password* 명령을 사용하여 PPPoE 연결을 위한 사용자 이름 및 비밀번호 쌍을 만듭니다. 사용자 이름은 PPPoE용으로 지정된 VPDN 그룹에 이미 연결된 사용자 이름이어야 합니다.

참고 ISP에서 CHAP 또는 MS-CHAP를 사용하는 경우에는 사용자 이름을 원격 시스템 이름이라고 하고, 비밀번호를 CHAP 암호라고 할 수도 있습니다.

PPPoE 클라이언트 기능은 기본적으로 해제되어 있으므로 VPDN 구성 후 **ip address** *if_name* **pppoe** [**setroute**] 명령을 사용하여 PPPoE를 활성화합니다. **setroute** 옵션은 기본 경로가 없는 경우 기본 경로를 생성합니다.

PPPoE가 구성되는 즉시 보안 어플라이언스는 통신할 PPPoE 액세스 집선 장치를 찾습니다. 정상적으로든 비정상적으로든 PPPoE 연결이 종료되면 ASA는 통신할 새 액세스 집선 장치를 찾습니다.

다음 **ip address** 명령은 PPPoE 세션을 종료하므로 PPPoE 세션이 시작된 후 사용해서는 안 됩니다.

- **ip address outside pppoe** - 새 PPPoE 세션을 시작합니다.
- **ip address outside dhcp** - 인터페이스에서 해당 DHCP 구성을 가져올 때까지 인터페이스를 비활성화합니다.
- **ip address outside** *address netmask* - 인터페이스를 정상적으로 초기화된 인터페이스로 가동합니다.

예

다음 예에서는 vdpn 그룹 *telecommuters*를 만들고 PPPoE 클라이언트를 구성합니다.

```
ciscoasa(config)# vpdn group telecommuters request dialout pppoe
ciscoasa(config)# vpdn group telecommuters localname user1
ciscoasa(config)# vpdn group telecommuters ppp authentication pap
ciscoasa(config)# vpdn username user1 password test1
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-subif)# ip address pppoe setroute
```

관련 명령

Command(명령)	설명
clear configure vpdn group	구성에서 모든 vpdn group 명령을 제거합니다.
clear configure vpdn username	구성에서 모든 vpdn username 명령을 제거합니다.
show vpdn group *group_name*	vpdn 그룹 구성을 표시합니다.
vpdn username	PPPoE 연결을 위한 사용자 이름 및 비밀번호 쌍을 만듭니다.

vpdn username

PPPoE 연결을 위한 사용자 이름 및 비밀번호 쌍을 만들려면 전역 구성 모드에서 **vpdn username** 명령을 사용합니다.

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]

참고 PPPoE는 ASA에 장애 조치가 구성된 경우 또는 다중 상황 모드나 투명 모드에서 지원되지 않습니다. PPPoE는 장애 조치 없는 단일 라우팅 모드에서만 지원됩니다.

구문 설명

password	비밀번호를 지정합니다.
store-local	보안 어플라이언스에 있는 NVRAM의 특정 위치에 사용자 이름 및 비밀번호를 저장합니다. Auto Update Server에서 보안 어플라이언스로 clear config 명령을 보내고 이후에 연결이 중단된 경우 보안 어플라이언스는 NVRAM에서 사용자 이름 및 비밀번호를 읽고 액세스 집선 장치에 다시 인증할 수 있습니다.
username	사용자 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다. 사용 지침을 참고하십시오.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예		—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

vpdn 사용자 이름은 **vpdn group** *group_name* **localname** *username* 명령을 통해 지정된 VPDN 그룹과 이미 연결된 사용자 이름이어야 합니다.

clear configure vpdn username 명령은 모든 **vpdn username** 명령을 컨피그레이션에서 제거합니다.

예

다음 예에서는 비밀번호가 *telecommuter9/8*인 vpdn 사용자 이름 *bob_smith*를 만듭니다.

```
ciscoasa(config)# vpdn username bob_smith password telecommuter9/8
```

관련 명령

Command(명령)	설명
clear configure vpdn group	구성에서 모든 **vpdn group** 명령을 제거합니다.
clear configure vpdn username	구성에서 모든 **vpdn username** 명령을 제거합니다.
show vpdn group	VPDN 그룹 구성을 표시합니다.
vpdn group	VPDN 그룹을 만들고 PPPoE 클라이언트 설정을 구성합니다.

vpn-access-hours

구성된 시간 범위 정책과 그룹 정책을 연결하려면 group-policy 구성 모드 또는 username 구성 모드에서 **vpn-access-hours** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션을 사용하면 다른 그룹 정책에서 시간 범위 값을 상속받을 수 있습니다. 값을 상속하지 못하도록 하려면 **vpn-access-hours none** 명령을 사용합니다.

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

구문 설명

none	VPN 액세스 시간을 null 값으로 설정하여 시간 범위 정책을 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 값을 상속받는 것을 방지합니다.
time-range	구성된 시간 범위 정책의 이름을 지정합니다.

기본값

제한 없음

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

예

다음 예에서는 FirstGroup이라는 그룹 정책을 824라는 시간 범위 정책과 연결하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-access-hours 824
```

관련 명령

Command(명령)	설명
time-range	시작 및 종료 날짜를 포함하여 네트워크에 액세스할 요일 및 시간을 설정합니다.

vpn-addr-assign

원격 액세스 클라이언트에 IPv4 주소를 할당할 방법을 지정하려면 전역 구성 모드에서 **vpn-addr-assign** 명령을 사용합니다. 구성에서 이 특성을 제거하려면 이 명령의 **no** 버전을 사용합니다. 구성된 모든 VPN 주소 할당 방법을 ASA에서 제거하려면 인수 없이 이 명령의 **no** 형식을 사용합니다.

vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

no vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

구문 설명

aaa	외부 또는 내부(LOCAL) AAA 인증 서버에서 IPv4 주소를 할당합니다.
dhcp	DHCP를 통해 IP 주소를 가져옵니다.
local	ASA에 구성된 IP 주소 풀에서 IP 주소를 할당하고 이를 터널 그룹에 연결합니다.
reuse-delay *delay*	해지된 IP 주소를 다시 사용할 수 있을 때까지의 지연 시간입니다. 범위는 0~480분입니다. 기본값은 0(비활성화됨)입니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
8.0.3	**reuse-delay** 옵션이 추가되었습니다.
9.5(2)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

사용 지침

DHCP를 선택한 경우 **dhcp-network-scope** 명령을 선택하여 DHCP 서버에서 사용할 수 있는 IP 주소 범위도 정의해야 합니다. DHCP 서버에서 사용하는 IP 주소를 나타내려면 **dhcp-server** 명령을 사용해야 합니다.

local을 선택한 경우 **ip-local-pool** 명령을 사용하여 사용할 IP 주소 범위를 정의해야 합니다. 그런 다음 **vpn-framed-ip-address** 및 **vpn-framed-netmask** 명령을 사용하여 IP 주소 및 넷마스크를 개별 사용자에게 할당합니다.

로컬 풀을 사용하는 경우 **reuse-delay** *delay* 옵션을 사용하여 해제된 IP 주소를 다시 사용할 수 있을 때까지의 지연 시간을 조정할 수 있습니다. 지연 시간을 늘리면 IP 주소가 풀로 반환되고 신속하게 재할당될 때 방화벽에서 발생할 수 있는 문제가 방지됩니다.

AAA를 선택한 경우 이전에 구성된 RADIUS 서버에서 IP 주소를 가져옵니다.

예

다음 예에서는 DHCP를 주소 할당 방법으로 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpn-addr-assign dhcp
```

관련 명령

Command(명령)	설명
dhcp-network-scope	ASA DHCP 서버에서 그룹 정책의 사용자에게 주소를 할당하기 위해 사용해야 하는 IP 주소 범위를 지정합니다.
ip-local-pool	로컬 IP 주소 풀을 만듭니다.
ipv6-addr-assign	원격 액세스 클라이언트에 IPv6 주소를 할당하는 방법을 지정합니다.
vpn-framed-ip-address	특정 사용자에게 할당할 IP 주소를 지정합니다.
vpn-framed-ip-netmask	특정 사용자에게 할당할 넷마스크를 지정합니다.

vpn-mode

클러스터에 대한 VPN 모드를 지정하려면 클러스터 그룹 구성 모드에서 **vpn-mode** 명령을 사용합니다. clustering vpn-mode 명령을 사용하면 관리자가 중앙 집중식 모드 또는 분산 모드 간에 전환할 수 있습니다. VPN 모드를 재설정하려면 이 명령의 no 형식을 사용합니다. CLI의 backup 옵션을 사용하면 관리자가 다른 섀시에 VPN 세션 백업을 생성할지 여부를 구성할 수 있습니다. 이 명령의 no 형식은 구성을 기본값으로 되돌립니다.

vpn-mode [centralized | distributed][backup {flat | remote-chassis}]

[no] vpn-mode [centralized | distributed {flat | remote-chassis}]

기본값

기본 VPN 모드는 centralized입니다. 기본 백업은 flat입니다.

구문 설명

centralized	VPN 세션이 클러스터 마스터 장치에서만 중앙 집중식으로 실행됩니다.
distributed	VPN 세션이 클러스터 전체에 분산됩니다.
flat	백업 세션이 클러스터의 다른 멤버에 할당됩니다.
remote-chassis	백업 세션이 다른 섀시의 멤버에 할당됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
클러스터 컨피그레이션	• 예	• 예	• 예	—	• 예

명령 기록

Release	수정 사항
9.9(1)	이 명령이 추가되었습니다.

사용 지침

균일 백업 모드에서 스탠바이 세션은 다른 클러스터 멤버에서 설정됩니다. 이 경우 사용자가 블레이드 장애로부터 보호될 수 있지만 섀시 장애가 반드시 방지되는 것은 아닙니다.

원격 섀시 백업 모드에서 스탠바이 세션은 클러스터에서 다른 섀시의 멤버에서 설정됩니다. 이 경우 사용자가 블레이드 장애와 섀시 장애로부터 보호됩니다.

원격 섀시가 단일 섀시 환경에서 구성된 경우(의도적으로 또는 장애로 인해 구성된 경우) 다른 섀시가 조인할 때까지 백업이 생성되지 않습니다.

예

```
ciscoasa (cfg-cluster)# vpn-mode distributed

Return the backup strategy of a distributed VPN cluster to default:
no vpn-mode distributed backup
```

관련 명령

Command(명령)	설명
cluster group	클러스터 그룹 설정을 구성합니다.
show cluster vpn-sessiondb distribution	클러스터 멤버 전체에서 활성 및 백업 세션의 분산을 확인합니다.

vpnclient connect

구성된 서버에 대한 Easy VPN Remote 연결을 설정하려면 전역 구성 모드에서 **vpnclient connect** 명령을 사용합니다.

vpnclient connect

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—
특권 실행	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

예

다음 예에서는 구성된 EasyVPN 서버에 대한 Easy VPN Remote 연결을 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient connect
ciscoasa(config)#
```

vpnclient enable

Easy VPN Remote 기능을 활성화하려면 전역 구성 모드에서 **vpnclient enable** 명령을 사용합니다. Easy VPN Remote 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient enable

no vpnclient enable

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN Remote 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

vpn enable 명령을 입력하면 지원되는 ASA가 Easy VPN Remote 하드웨어 클라이언트로 작동합니다.

예

다음 예에서는 Easy VPN Remote 기능을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient enable
ciscoasa(config)#
```

다음 예에서는 Easy VPN Remote 기능을 비활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# no vpnclient enable
ciscoasa(config)#
```

vpnclient ipsec-over-tcp

Easy VPN 하드웨어 클라이언트로 실행되는 ASA를 TCP 캡슐화된 IPsec을 사용하도록 구성하려면 전역 구성 모드에서 **vpnclient ipsec-over-tcp** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

구문 설명

port	(선택 사항) 특정 포트를 사용하도록 지정합니다.
tcp_port	(**por** 키워드를 지정한 경우에 필요합니다.) TCP 캡슐화 된 IPsec 터널에 사용할 TCP 포트 번호를 지정합니다.

기본값

명령에서 포트 번호를 지정하지 않으면 Easy VPN Remote 연결에서 포트 10000을 사용합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

기본적으로 Easy VPN 클라이언트 및 서버는 UDP(사용자 데이터그램 프로토콜) 패킷에서 IPsec을 캡슐화합니다. 특정 방화벽 규칙 또는 NAT 및 PAT 디바이스가 있는 일부 환경에서는 UDP를 금지합니다. 이러한 환경에서 표준 ESP(Encapsulating Security Protocol, Protocol 50) 또는 IKE(인터넷 키 교환국, UDP 500)를 사용하려면 TCP 패킷 내에서 IPsec을 캡슐화하여 보안 터널링을 활성화하도록 클라이언트 및 서버를 구성해야 합니다. 그러나 UDP를 허용하는 환경에서 IPsec over TCP를 구성하면 불필요한 오버헤드가 추가됩니다.

TCP 캡슐화된 IPsec을 사용하도록 ASA를 구성한 경우 다음 명령을 입력하여 외부 인터페이스를 통해 대용량 패킷을 전송할 수 있도록 합니다.

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

이 명령은 캡슐화된 헤더에서 DF(Don't Fragment) 비트를 지웁니다. DF 비트는 패킷을 프래그먼트할 수 있는지 여부를 결정하는 IP 헤더 내의 비트입니다. 이 명령을 사용하면 Easy VPN 하드웨어 클라이언트가 MTU 크기보다 큰 패킷을 전송할 수 있습니다.

예

다음 예에서는 기본 포트 10000을 사용하여 TCP 캡슐화된 IPsec을 사용하도록 Easy VPN Remote 하드웨어 클라이언트를 구성하고 외부 인터페이스를 통해 대용량 패킷을 전송할 수 있도록 하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient ipsec-over-tcp
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

다음 예에서는 포트 10501을 사용하여 TCP 캡슐화된 IPsec을 사용하도록 Easy VPN Remote 하드웨어 클라이언트를 구성하고 외부 인터페이스를 통해 대용량 패킷을 전송할 수 있도록 하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient ipsec-over-tcp port 10501
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

vpnclient mac-exempt

Easy VPN Remote 연결 뒤에 있는 장치를 개별 사용자 인증 요구 사항에서 제외하려면 전역 구성 모드에서 **vpnclient mac-exempt** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

no vpnclient mac-exempt

구문 설명

mac_addr_1	개별 사용자 인증을 제외할 장치의 제조업체 및 일련 번호를 지정하는 MAC 주소(점으로 구분된 16진수 표기법)입니다. 장치가 2대 이상인 경우 공백 및 각 네트워크 마스크로 구분하여 각 MAC 주소를 지정합니다. MAC 주소의 처음 6자는 장치 제조업체를 식별하고 마지막 6자는 일련 번호입니다. 마지막 24비트는 16진수 형식의 장치 일련 번호입니다.
mac_mask_1	해당 MAC 주소에 대한 네트워크 마스크입니다. 공백을 사용하여 네트워크 마스크와 이후의 모든 MAC 주소 및 네트워크 마스크 쌍을 구분할 수 있습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

Cisco IP Phone, 무선 액세스 포인트 및 프린터와 같은 장치에서는 인증을 수행할 수 없으므로 개별 장치 인증이 활성화된 경우 인증하지 않습니다. 개별 사용자 인증이 활성화된 경우 이 명령을 사용하여 이러한 장치를 인증에서 제외할 수 있습니다. 개별 사용자 인증에서 장치를 제외하는 것을 "장치 통과" 라고도 합니다.

이 명령에서 MAC 주소 및 마스크를 지정하는 형식에는 마침표로 구분된 16진수 3개가 사용됩니다. 예를 들어 MAC 마스크 ffff.ffff.ffff는 지정한 MAC 주소와 일치합니다. 모두 0인 MAC 마스크는 일치하는 MAC 주소가 없으며, MAC 마스크 ffff.ff00.0000은 같은 제조업체에서 만든 모든 장치와 일치합니다.

참고 헤드엔드 장치에서 개별 사용자 인증 및 사용자 우회를 구성해야 합니다. 예를 들어 ASA가 헤드엔드인 경우 정책 그룹에서 다음을 구성합니다.

```
ciscoasa(config-group-policy)# user-authentication enable
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

예

Cisco IP Phone은 제조업체 ID가 00036b이므로 다음 명령은 Cisco IP Phone을 포함하여 향후에 추가할 수 있는 모든 Cisco IP Phone을 제외합니다.

```
ciscoasa(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
ciscoasa(config)#
```

다음 예에서는 특정 Cisco IP Phone 하나를 제외하므로 유연성은 떨어지지만 보다 뛰어난 보안을 제공합니다.

```
ciscoasa(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
ciscoasa(config)#
```

vpnclient management

Easy VPN Remote 하드웨어 클라이언트의 관리 액세스를 위한 IPsec 터널을 생성하려면 전역 구성 모드에서 **vpnclient management** 명령을 사용합니다.

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

vpnclient management clear

실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 그러면 **split-tunnel-policy** 및 **split-tunnel-network-list** 명령에 따라 관리용으로만 IPsec 터널이 설정됩니다.

no vpnclient management

구문 설명

clear	일반 라우팅을 사용하여 회사 네트워크에서 Easy VPN 클라이언트로 실행되는 ASA 5505의 외부 인터페이스로의 관리 액세스를 제공합니다. 이 옵션은 관리 터널을 만들지 않습니다. **참고** 클라이언트와 인터넷 사이에서 NAT 장치가 작동하는 경우 이 옵션을 사용합니다.
ip_addr	Easy VPN 하드웨어 클라이언트에서 관리 터널을 만들 호스트 또는 네트워크의 IP 주소입니다. **tunnel** 키워드와 함께 이 인수를 사용합니다. 공백 및 각 네트워크 마스크로 구분하여 하나 이상의 IP 주소를 지정합니다.
ip_mask	해당 IP 주소에 대한 네트워크 마스크입니다. 공백을 사용하여 네트워크 마스크와 이후의 모든 IP 주소 및 네트워크 마스크 쌍을 구분할 수 있습니다.
tunnel	특별히 회사 네트워크에서 Easy VPN 클라이언트로 실행되는 ASA 5505의 외부 인터페이스로의 관리 액세스에 대한 IPsec 터널 설정을 자동화합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

ASA 5505 구성에 다음 명령이 포함된 것으로 가정합니다.

- **vpnclient server** - 피어 지정
- **vpnclient mode** - 클라이언트 모드(PAT) 또는 네트워크 확장 모드 지정

다음 중 하나에 해당합니다.

- **vpnclient vpngroup** - Easy VPN 서버 인증에 사용되는 터널 그룹 및 IKE 사전 공유 키 이름 지정
- **vpnclient trustpoint** - 인증에 사용할 RSA 인증서를 식별하는 트러스트 포인트 이름 지정

참고 NAT 장치에서 정적 NAT 매핑을 추가하지 않은 경우에는 NAT 장치 뒤에 있는 ASA의 공용 주소에 액세스할 수 없습니다.

참고 구성에 관계없이 DHCP 요청(갱신 메시지 포함)은 IPsec 터널을 통해 흐를 수 없습니다. vpnclient 관리 터널에서도 DHCP 트래픽은 금지됩니다.

예

다음 예에서는 ASA 5505의 외부 인터페이스에서 IP 주소/마스크 조합이 192.168.10.10 255.255.255.0인 호스트 사이의 IPsec 터널을 생성하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
ciscoasa(config)#
```

다음 예에서는 IPsec을 사용하지 않고 ASA 5505의 외부 인터페이스에 대한 관리 액세스를 제공하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient management clear
ciscoasa(config)#
```

vpnclient mode

클라이언트 모드 또는 네트워크 확장 모드에 대한 Easy VPN Remote 연결을 구성하려면 전역 구성 모드에서 **vpnclient mode** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient mode {**client-mode** | **network-extension-mode**}

no vpnclient mode

구문 설명

client-mode	클라이언트 모드(PAT)를 사용하도록 Easy VPN Remote 연결을 구성합니다.
network-extension-mode	네트워크 확장 모드(NEM)를 사용하도록 Easy VPN Remote 연결을 구성합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

Easy VPN 클라이언트는 클라이언트 모드 또는 NEM을 지원합니다. 작동 모드에 따라 엔터프라이즈 네트워크에서 터널을 통해 Easy VPN 클라이언트에 상대적인 내부 호스트에 액세스할 수 있는지 여부가 결정됩니다. Easy VPN 클라이언트에는 기본 모드가 없기 때문에 연결을 설정하려면 먼저 작동 모드를 지정해야 합니다.

- 클라이언트 모드에서는 Easy VPN 클라이언트가 해당 내부 호스트에서의 모든 VPN 트래픽에 대해 PAT(포트 주소 변환)를 수행합니다. 이 모드에서는 하드웨어 클라이언트(기본 RFC 1918 주소가 할당됨)의 내부 주소 또는 내부 호스트에 대한 IP 주소 관리가 필요 없습니다. PAT 때문에 엔터프라이즈 네트워크에서 내부 호스트에 액세스할 수 없습니다.
- NEM에서는 내부 네트워크 및 내부 인터페이스의 모든 노드에 엔터프라이즈 네트워크를 통해 라우팅할 수 있는 주소가 할당됩니다. 내부 호스트에는 엔터프라이즈 네트워크에서 터널을 통해 액세스할 수 있습니다. 내부 네트워크의 호스트에는 액세스 가능한 서브넷에서 IP 주소가 할당됩니다(정적으로 또는 DHCP를 통해). 네트워크 확장 모드에서는 VPN 트래픽에 PAT가 적용되지 않습니다.

참고 Easy VPN 하드웨어 클라이언트가 NEM을 사용하고 보조 서버에 연결된 경우 각 헤드엔드 장치에서 **crypto map set reverse-route** 명령을 사용하여 RRI(Reverse Route Injection)를 통한 원격 네트워크의 동적 알림을 구성할 수 있습니다.

예 다음 예에서는 클라이언트 모드에 대한 Easy VPN Remote 연결을 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient mode client-mode
ciscoasa(config)#
```

다음 예에서는 NEM에 대한 Easy VPN Remote 연결을 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient mode network-extension-mode
ciscoasa(config)#
```

vpnclient nem-st-autoconnect

NEM 및 스플릿 터널링이 구성된 경우 IPsec 데이터 터널을 자동으로 시작하도록 Easy VPN Remote 연결을 구성하려면 전역 구성 모드에서 **vpnclient nem-st-autoconnect** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

vpnclient nem-st-autoconnect 명령을 입력하기 전에 하드웨어 클라이언트에 대해 네트워크 확장 모드가 설정되어 있는지 확인합니다. 네트워크 확장 모드에서는 하드웨어 클라이언트가 VPN 터널을 통해 원격 사설 네트워크에 라우팅 가능한 단일 네트워크를 제공할 수 있습니다. IPsec은 하드웨어 클라이언트 뒤에 있는 사설 네트워크의 모든 트래픽을 ASA 뒤에 있는 네트워크에 대해 캡슐화합니다. PAT는 적용되지 않습니다. 따라서 ASA 뒤에 있는 디바이스는 터널을 통해 하드웨어 클라이언트 뒤에 있는 사설 네트워크의 디바이스에 직접 액세스할 수 있으며 이와 반대의 경우에는 터널을 통해서만 가능합니다. 하드웨어 클라이언트에서 터널을 시작해야 합니다. 터널이 가동된 후에는 한 쪽에서 데이터 교환을 시작할 수 있습니다.

참고 또한 네트워크 확장 모드를 활성화하도록 Easy VPN 서버를 구성해야 합니다. 이렇게 하려면 group-policy 구성 모드에서 **nem enable** 명령을 사용합니다.

네트워크 확장 모드에서는 스플릿 터널링이 구성된 경우를 제외하고 IPsec 데이터 터널이 자동으로 시작 및 유지됩니다.

예

다음 예에서는 스플릿 터널링이 구성된 네트워크 확장 모드에서 자동으로 연결되도록 Easy VPN Remote 연결을 구성하는 방법을 보여 줍니다. 네트워크 확장 모드는 FirstGroup 그룹 정책에 대해 활성화되어 있습니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# nem enable
ciscoasa(config)# vpnclient nem-st-autoconnect
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
nem	하드웨어 클라이언트에 대한 네트워크 확장 모드를 활성화합니다.

vpnclient server

Easy VPN Remote 연결을 위한 기본 및 보조 IPsec 서버를 구성하려면 전역 구성 모드에서 **vpnclient server** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient server *ip_primary_address* [*ip_secondary_address_1* ... *ipsecondary_address_10*]

no vpnclient server

구문 설명

ip_primary_address	기본 Easy VPN(IPsec) 서버의 IP 주소 또는 DNS 이름입니다. 모든 ASA 또는 VPN 3000 Concentrator 시리즈는 Easy VPN 서버 역할을 할 수 있습니다.
ip_secondary_address_n	(선택 사항) 최대 10개의 Easy VPN 백업 서버에 대한 IP 주소 또는 DNS 이름 목록입니다. 공백을 사용하여 목록의 항목을 구분합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

연결을 설정하려면 먼저 서버를 구성해야 합니다. **vpnclient server** 명령은 IPv4 주소, 이름 데이터베이스 또는 DNS 이름을 지원하며, 이 순서대로 주소를 확인합니다.

서버의 IP 주소 또는 호스트 이름을 사용할 수 있습니다.

예

다음 예에서는 headend-1이라는 이름을 주소 10.10.10.10에 연결하고 **vpnclient server** 명령을 사용하여 headend-dns.example.com(기본), headend-1(보조) 및 192.168.10.10(보조)의 세 서버를 지정합니다.

```
ciscoasa(config)# names
ciscoasa(config)# 10.10.10.10 headend-1
ciscoasa(config)# vpnclient server headend-dns.example.com headend-1 192.168.10.10
```

```
ciscoasa(config)#
```

다음 예에서는 IP 주소가 10.10.10.15인 VPN 클라이언트 기본 IPsec 서버와 IP 주소가 10.10.10.30 및 192.168.10.45인 보조 서버를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
ciscoasa(config)#
```

vpnclient server-certificate

인증서 맵에 지정된 특정 인증서가 있는 Easy VPN 서버에 대한 연결만 허용하도록 Easy VPN Remote 연결을 구성하려면 전역 구성 모드에서 **vpnclient server-certificate** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

구문 설명

certmap_name	허용되는 Easy VPN 서버 인증서를 지정하는 인증서 맵의 이름을 지정합니다. 최대 길이는 64자입니다.

기본값

Easy VPN 서버 인증서 필터링은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

이 명령을 사용하여 Easy VPN 서버 인증서 필터링을 활성화할 수 있습니다. crypto ca certificate map 및 crypto ca certificate chain 명령을 사용하여 인증서 맵 자체를 정의합니다.

예

다음 예에서는 인증서 맵 이름이 homeservers인 Easy VPN 서버에 대한 연결만 지원하도록 Easy VPN Remote 연결을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient server-certificate homeservers
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
certificate	지정된 인증서를 추가합니다.
vpnclient trustpoint	Easy VPN Remote 연결에서 사용할 RSA ID 인증서를 구성합니다.

vpnclient trustpoint

Easy VPN Remote 연결에서 사용할 RSA ID 인증서를 구성하려면 전역 구성 모드에서 **vpnclient trustpoint** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient trustpoint *trustpoint_name* [**chain**]

no vpnclient trustpoint

구문 설명

chain	전체 인증서 체인을 전송합니다.
trustpoint_name	인증에 사용할 RSA 인증서를 식별하는 트러스트 포인트의 이름을 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

crypto ca trustpoint 명령을 사용하여 트러스트 포인트를 정의합니다. 트러스트 포인트는 CA에서 발급한 인증서에 따라 CA ID 및 가능한 경우 장치 ID를 나타냅니다. 트러스트 포인트 하위 모드 내의 명령은 ASA가 CA 인증서를 가져오는 방법, ASA가 CA에서 해당 인증서를 가져오는 방법 및 CA에서 발급한 사용자 인증서에 대한 인증 정책을 지정하는 CA 관련 구성 파라미터를 제어합니다.

예

다음 예에서는 certificate이라는 특정 ID 인증서를 사용하고 전체 인증서 체인을 보내도록 Easy VPN Remote 연결을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config)# vpnclient trustpoint central chain
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
crypto ca trustpoint	지정된 트러스트 포인트에 대한 트러스트 포인트 하위 모드를 시작하고 트러스트 포인트 정보를 관리합니다.

vpnclient username

Easy VPN Remote 연결을 위한 VPN 사용자 이름 및 비밀번호를 구성하려면 전역 구성 모드에서 **vpnclient username** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient username *xauth_username* **password** *xauth password*

no vpnclient username

구문 설명

xauth_password	XAUTH에 사용할 비밀번호를 지정합니다. 최대 길이는 64자입니다.
xauth_username	XAUTH에 사용할 사용자 이름을 지정합니다. 최대 길이는 64자입니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

XAUTH 사용자 이름 및 비밀번호 파라미터는 보안 장치 인증이 비활성화되고 서버에서 XAUTH 크리덴셜을 요청하는 경우에 사용됩니다. 보안 장치 인증이 활성화된 경우에는 이러한 파라미터가 무시되고 ASA에서 사용자에게 사용자 이름 및 비밀번호를 묻는 프롬프트를 표시합니다.

예

다음 예에서는 XAUTH 사용자 이름 testuser 및 비밀번호 ppurkm1을 사용하도록 Easy VPN Remote 연결을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient username testuser password ppurkm1
ciscoasa(config)#
```

vpnclient vpngroup

Easy VPN Remote 연결을 위한 VPN 터널 그룹 이름 및 비밀번호를 구성하려면 전역 구성 모드에서 **vpnclient vpngroup** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpnclient vpngroup *group_name* **password** *preshared_key*

no vpnclient vpngroup

구문 설명

group_name	Easy VPN 서버에 구성된 VPN 터널 그룹의 이름을 지정합니다. 최대 길이는 64자이고, 공백은 허용되지 않습니다.
preshared_key	Easy VPN 서버에서 인증에 사용되는 IKE 사전 공유 키입니다. 최대 길이는 128자입니다.

기본값

Easy VPN Remote 하드웨어 클라이언트로 실행되는 ASA의 구성에서 터널 그룹을 지정하지 않은 경우에는 클라이언트에서 RSA 인증서를 사용합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 Easy VPN 원격 하드웨어 클라이언트(릴리스 7.2(1)~9.2를 실행하는 ASA 5505 또는 릴리스 9.5(1) 이상을 실행하는 ASA 5506 또는 5508 모델)로 실행 중인 ASA에만 적용됩니다.

사전 공유 키를 비밀번호로 사용합니다.

또한 연결을 설정하기 전에 서버를 구성하고 모드를 지정해야 합니다.

예

다음 예에서는 그룹 이름이 TestGroup1이고 비밀번호가 my_key123인 VPN 터널 그룹으로 Easy VPN Remote 연결을 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# vpnclient vpngroup TestGroup1 password my_key123
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
vpnclient trustpoint	Easy VPN 연결에서 사용할 RSA ID 인증서를 구성합니다.

vpn-filter

VPN 연결에 사용할 ACL 이름을 지정하려면 그룹 정책 또는 사용자 이름 모드에서 **vpn-filter** 명령을 사용합니다. **vpn-filter none** 명령을 발행하여 생성한 null 값을 포함하는 ACL을 제거하려면 이 명령의 **no** 형식을 사용합니다. **no** 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다. 값을 상속하지 못하도록 하려면 **vpn-filter none** 명령을 사용합니다.

이 사용자 또는 그룹 정책에 대한 여러 유형의 트래픽을 허용하거나 거부하도록 ACL을 구성합니다. 그런 다음 **vpn-filter** 명령을 사용하여 이러한 ACL을 적용합니다.

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

구문 설명

none	액세스 목록이 없음을 나타냅니다. null 값을 설정하여 액세스 목록을 허용하지 않습니다. 다른 그룹 정책에서 액세스 목록을 상속하지 못하도록 합니다.
value *ACL name*	이전에 구성된 액세스 목록의 이름을 제공합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.0(1)	IPv4 및 IPv6 ACL에 대한 지원이 추가되었습니다. 다중 컨텍스트 모드에 대한 지원이 추가되었습니다.
9.1.(4)	IPv4 및 IPv6 ACL에 대한 지원이 추가되었습니다. 사용 중단된 **ipv6-vpn-filter** 명령을 실수로 사용하여 IPv6 ACL을 지정한 경우 연결이 종료됩니다.

사용 지침

클라이언트리스 SSL VPN에서는 **vpn-filter** 명령에 정의된 ACL을 사용하지 않습니다.

vpn-filter 기능은 인바운드 방향으로만 필터링되는 트래픽을 허용하도록 설계되었습니다. 아웃바운드 규칙은 자동으로 컴파일됩니다. ICMP 액세스 목록을 만들 때 방향 필터를 사용하려면 ICMP 유형을 액세스 목록 형식으로 지정하지 마십시오.

예

다음 예에서는 FirstGroup이라는 정책 그룹에 대해 acl_vpn이라는 액세스 목록을 호출하는 필터를 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-filter value acl_vpn
```

관련 명령

Command(명령)	설명
access-list	액세스 목록을 생성하거나 다운로드 가능한 액세스 목록을 사용합니다.
ipv6-vpn-filter	이전에 IPv6 ACL을 지정하는 데 사용된 사용 중단된 명령입니다.

vpn-framed-ip-address

개별 사용자에게 할당할 IPv4 주소를 지정하려면 사용자 이름 모드에서 **vpn-framed-ip-address** 명령을 사용합니다. IP 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpn-framed-ip-address {*ip_address*} {*subnet_mask*}

no vpn-framed-ip-address

구문 설명

ip_address	이 사용자에 대한 IP 주소를 제공합니다.
subnet_mask	서브넷 마스크를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
username 컨피그레이션	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

예

다음 예에서는 anyuser라는 사용자에 대한 IP 주소를 10.92.166.7로 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-framed-ip-address 10.92.166.7 255.255.255.254
```

vpn-framed-ipv6-address

사용자 모드에서 **vpn-framed-ipv6-address** 명령을 사용하여 사용자에게 전용 IPv6 주소를 할당할 수 있습니다. IP 주소를 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpn-framed-ipv6-address *ip_address/subnet_mask*

no vpn-framed-ipv6-address *ip_address/subnet_mask*

구문 설명

ip_address	이 사용자에 대한 IP 주소를 제공합니다.
subnet_mask	서브넷 마스크를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
username 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
9.0(1)	이 명령이 추가되었습니다.

예

다음 예에서는 *anyuser*라는 사용자에 대한 IP 주소 및 넷마스크를 2001::3000:1000:2000:1/64로 설정하는 방법을 보여 줍니다. 이 주소는 2001:0000:0000:0000의 앞에 붙은 값과 3000:1000:2000:1의 인터페이스 ID를 나타냅니다.

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
ciscoasa(config-username)
```

관련 명령

Command(명령)	설명
vpn-framed-ip-address	개별 사용자에게 할당할 IPv4 주소를 지정합니다.

vpn-group-policy

사용자가 구성된 그룹 정책에서 특성을 상속하도록 하려면 username 구성 모드에서 **vpn-group-policy** 명령을 사용합니다. 사용자 구성에서 그룹 정책을 제거하려면 이 명령의 **no** 버전을 사용합니다. 이 명령을 사용하면 사용자가 사용자 이름 수준에서 구성되지 않은 특성을 상속할 수 있습니다.

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

구문 설명

group-policy name	그룹 정책의 이름을 제공합니다.

기본값

기본적으로 VPN 사용자는 그룹 정책 연계가 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
username 컨피그레이션	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

사용자 이름 모드에서 구성하여 특정 사용자에 대해 그룹 정책의 특성 값을 재정의할 수 있습니다(해당 특성을 사용자 이름 모드에서 사용할 수 있는 경우).

예

다음 예는 이름이 FirstGroup인 그룹 정책의 특성을 사용하도록 이름이 anyuser인 사용자를 구성하는 방법을 보여줍니다.

```
ciscoasa(config)# username anyuser attributes
ciscoasa(config-username)# vpn-group-policy FirstGroup
```

관련 명령

Command(명령)	설명
group-policy	ASA 데이터베이스에 그룹 정책을 추가합니다.
group-policy attributes	그룹 정책에 대한 AVP를 구성할 수 있는 group-policy attributes 모드를 시작합니다.
username	ASA 데이터베이스에 사용자를 추가합니다.
username attributes	특정 사용자에 대한 AVP를 구성할 수 있는 username attributes 모드를 시작합니다.

vpn-idle-timeout

사용자 시간 제한을 구성하려면 group-policy 구성 모드 또는 username 구성 모드에서 **vpn-idle-timeout** 명령을 사용합니다. 이 기간 동안 연결을 통한 통신 활동이 없는 경우 ASA는 연결을 종료합니다. 선택적으로 시간 제한 알림 간격을 기본 1분에서 연장할 수 있습니다.

실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션을 사용하면 다른 그룹 정책에서 시간 제한 값을 상속하도록 허용됩니다. 값을 상속하지 못하도록 하려면 **vpn-idle-timeout none** 명령을 사용합니다.

vpn-idle-timeout {*minutes* **| none} [alert-interval** *minutes***]**

no vpn-idle-timeout

no vpn-idle-timeout alert-interval

구문 설명

minutes	시간 제한(분) 및 시간 제한 알림 전까지의 경과 시간(분)을 지정합니다. 1~35791394의 정수를 사용합니다.
none	AnyConnect(SSL IPsec/IKEv2): **ciscoasa(config-webvpn)# default-idle-timeout** 명령의 전역 WebVPN default-idle-timeout 값(초)을 사용합니다. WebVPN **default-idle-timeout** 명령에서 이 값에 대한 범위는 60-86400초이며, 기본 전역 WebVPN 유휴 시간 제한(초)의 기본값은 1800초(30분)입니다. **참고** 0이 아닌 유휴 시간 제한 값은 모든 AnyConnect 연결을 위한 ASA에 필요합니다. WebVPN 사용자의 경우 vpn-idle-timeout none이 그룹 정책/사용자 이름 특성에 설정된 경우에만 **default-idle-timeout** 값이 적용됩니다. Site-to-Site(IKEv1, IKEv2) 및 IKEv1 원격 액세스: 시간 제한을 비활성화하고 무제한 유휴 기간을 허용합니다.

기본값

30분입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

AnyConnect 클라이언트는 SSL 및 IKEv2 연결에 대한 세션 다시 시작을 지원합니다. 이 기능을 사용하면 엔드 유저 장치가 절전 모드로 전환되거나 해당 WiFi가 끊어지는 등의 상황이 발생한 후 복구 시 동일한 연결을 다시 시작할 수 있습니다.

예

다음 예에서는 "FirstGroup" 이라는 그룹 정책에 대한 VPN 유휴 시간 제한을 15분으로 설정하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-idle-timeout 30
```

보안 어플라이언스에서는 사용자에 대한 유휴 시간 제한이 정의되지 않은 경우, vpn-idle-timeout 값이 0인 경우 또는 값이 유효한 범위에 속하지 않는 경우 default-idle-timeout 값을 사용합니다.

관련 명령

default-idle-timeout	전역 WebVPN 기본 유휴 시간 제한을 지정합니다.
group-policy	그룹 정책을 만들거나 수정합니다.
vpn-session-timeout	VPN 연결에 허용되는 최대 기간을 구성합니다. 구성된 기간의 마지막에서 ASA는 연결을 종료합니다.

vpn load-balancing

VPN 부하 균형 및 관련 기능을 구성할 수 있는 vpn load-balancing 모드를 시작하려면 전역 구성 모드에서 **vpn load-balancing** 명령을 사용합니다.

vpn load-balancing

참고 VPN 부하 균형을 사용하려면 ASA 5510 Plus 라이선스 또는 ASA 5520 이상이 있어야 합니다. VPN 로드 밸런싱에도 활성 3DES/AES 라이선스가 필요합니다. 보안 어플라이언스는 로드 밸런싱을 활성화하기 전에 이러한 암호화 라이선스가 있는지 확인합니다. 활성 3DES 또는 AES 라이선스가 탐지되지 않는 경우 보안 어플라이언스가 로드 밸런싱의 활성화를 방지하며 라이선스에서 허용할 때까지 로드 밸런싱을 통한 3DES의 내부 구성을 방지합니다.

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
8.0(2)	Plus 라이선스를 사용하는 ASA 5510 및 5520 이상 모델에 대한 지원이 추가되었습니다.

사용 지침

부하 균형 클러스터는 보안 어플라이언스 모델 5510(Plus 라이선스) 또는 ASA 5520 이상을 포함할 수 있습니다. 또한 VPN 3000 Series Concentrator를 클러스터에 포함할 수 있습니다. 혼합된 구성을 사용할 수 있는 경우 일반적으로 클러스터의 종류가 같으면 관리가 더 간단합니다.

vpn load-balancing 명령을 사용하여 vpn load-balancing 모드를 시작할 수 있습니다. 다음 명령은 vpn load-balancing 모드에서 사용할 수 있습니다.

- **cluster encryption**
- **cluster ip address**
- **cluster key**
- **cluster port**
- **interface**

- **nat**
- **participate**
- **priority**
- **redirect-fqdn**

자세한 내용은 개별 명령 설명을 참고하십시오.

예

다음은 **vpn load-balancing** 명령의 예입니다. 프롬프트의 변경 사항에 주의하십시오.

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)#
```

다음은 클러스터의 공용 인터페이스를 "test" 로 지정하고 클러스터의 사설 인터페이스를 "foo" 로 지정하는 인터페이스 명령이 포함된 VPN 부하 균형 명령 시퀀스의 예입니다.

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
```

관련 명령

Command(명령)	설명
clear configure vpn load-balancing	로드 밸런싱 런타임 구성을 제거하고 로드 밸런싱을 비활성화합니다.
show running-config vpn load-balancing	현재 VPN 로드 밸런싱 가상 클러스터 구성을 표시합니다.
show vpn load-balancing	VPN 로드 밸런싱 런타임 통계를 표시합니다.

vpn-session-db

최대 VPN 세션 또는 AnyConnect 클라이언트 VPN 세션 수를 지정하려면 전역 구성 모드에서 **vpn-session-db** 명령을 사용합니다. 구성에서 이 제한을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpn-sessiondb {**max-anyconnect-premium-or-essentials-limit** *number* | **max-other-vpn-limit** *number*}

구문 설명

max-anyconnect-premium-or-essentials-limit *number*	최대 AnyConnect 세션 수를 1에서 라이선스에서 허용하는 최대 세션 수 사이로 지정합니다.
max-other-vpn-limit *number*	AnyConnect 클라이언트 세션이 아닌 최대 VPN 세션 수를 1에서 라이선스에서 허용하는 최대 세션 수 사이로 지정합니다. 여기에는 Cisco VPN 클라이언트(IPsec IKEv1) 및 LAN-to-LAN VPN 세션이 포함됩니다.

기본값

기본적으로 ASA는 라이선스 최대값보다 낮은 VPN 세션 수를 제한하지 않습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
8.4(1)	다음 키워드가 변경되었습니다. • **max-session-limit가 max-anyconnect-premium-or-essentials-limit**로 대체되었습니다. • **max-webvpn-session-limit가 max-other-vpn-limit**로 대체되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

예

다음 예에서는 최대 AnyConnect 세션 수를 200으로 설정합니다.

```
ciscoasa(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 200
```

관련 명령

Command(명령)	설명
vpn-sessiondb logoff	모든 유형 또는 특정 유형의 IPsec VPN 및 WebVPN 세션을 로그오프합니다.
vpn-sessiondb max-webvpn-session-limit	최대 WebVPN 세션 수를 설정합니다.

vpn-sessiondb logoff

모든 VPN 세션 또는 선택한 VPN 세션을 로그오프하려면 전역 구성 모드에서 **vpn-sessiondb logoff** 명령을 사용합니다.

vpn-sessiondb logoff {**all | anyconnect | email-proxy | index** ***index_number*** **|**
ipaddress *IPaddr* | **l2l** | **name** *username* **| protocol** *protocol-name* **| ra-ikev1-ipsec |**
ra-ikev2-ipsec | tunnel-group *groupname* **| vpn-lb | webvpn**} [**noconfirm**]

구문 설명

all	모든 VPN 세션을 로그오프합니다.
anyconnect	모든 AnyConnect VPN 클라이언트 세션을 로그오프합니다.
email-proxy	(사용되지 않음) 모든 이메일 프록시 세션을 기록합니다.
index *index_number*	인덱스 번호별로 단일 세션을 로그오프합니다. 세션의 인덱스 번호를 지정합니다. **show vpn-sessiondb detail** 명령을 사용하여 각 세션의 인덱스 번호를 확인할 수 있습니다.
ipaddress *IPaddr*	지정한 IP 주소에 대한 세션을 로그오프합니다.
l2l	모든 LAN-to-LAN 세션을 로그오프합니다.
name *username*	지정한 사용자 이름에 대한 세션을 로그오프합니다.
protocol *protocol-name*	지정한 프로토콜에 대한 세션을 로그오프합니다. 프로토콜은 다음과 같습니다. • ikev1 - IKEv1(인터넷 키 교환국 버전 1) 프로토콜을 사용하는 세션입니다. • ikev2 - IKEv2(인터넷 키 교환국 버전 2) 프로토콜을 사용하는 세션입니다. • ipsec - IKEv1 또는 IKEv2를 사용하는 IPsec 세션입니다. • ipseclan2lan — IPsec LAN-to-LAN 세션. • ipseclan2lanovernatt — NAT-T를 통한 IPsec LAN-to-LAN 세션. • ipsecovernatt — NAT-T를 통한 IPsec 세션. • ipsecovertcp — TCP를 통한 IPsec 세션. • ipsecoverudp — UDP를 통한 IPsec 세션. • l2tpOverIpSec - L2TP over IPsec 세션입니다. • l2tpOverIpsecOverNatT - NAT-T를 통한 IPsec을 통한 L2TP 세션. • webvpn — 클라이언트 리스 SSL VPN 세션. • imap4s - IMAP4 세션입니다. • pop3s - POP3 세션입니다. • smtps - SMTP 세션입니다. • anyconnectParent - 세션에 사용되는 프로토콜에 상관없는 AnyConnect 클라이언트 세션입니다(AnyConnect IPsec IKEv2 및 SSL 세션을 종료함). • ssltunnel - SSL을 사용하는 AnyConnect 세션 및 클라이언트리스 SSL VPN 세션을 비롯한 SSL VPN 세션입니다. • dtlstunnel - DTLS가 활성화된 AnyConnect 클라이언트 세션입니다.

ra-ikev1-ipsec	모든 IPsec IKEv1 원격 액세스 세션을 로그오프합니다.
ra-ikev2-ipsec	모든 IPsec IKEv2 원격 액세스 세션을 로그오프합니다.
tunnel-group *groupname*	지정한 터널 그룹(연결 프로파일)에 대한 세션을 로그오프합니다.
webvpn	모든 클라이언트리스 SSL VPN 세션을 로그오프합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
8.4(1)	다음 **프로토콜** 키워드가 변경되거나 추가되었습니다. • **remote**가 **ra-ikev1-ipsec**으로 변경되었습니다. • **ike**가 **ikev1**로 변경되었습니다. • **ikev2**가 추가되었습니다. • **anyconnectParent**가 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.
9.3(2)	**ra-ikev2-ipsec** 키워드가 추가되었습니다.
9.8(1)	**email-proxy** 옵션은 사용이 중단되었습니다.

예

다음 예에서는 모든 AnyConnect 클라이언트 세션을 로그오프하는 방법을 보여 줍니다.

```
ciscoasa# vpn-sessiondb logoff anyconnect
```

다음 예에서는 모든 IPsec 세션을 로그오프하는 방법을 보여 줍니다.

```
ciscoasa# vpn-sessiondb logoff protocol IPsec
```

vpn-session-timeout

VPN 연결에 허용되는 최대 기간을 구성하려면 group-policy 구성 모드 또는 username 구성 모드에서 **vpn-session-timeout** 명령을 사용합니다. 구성된 기간의 마지막에서 ASA는 연결을 종료합니다. 선택적으로 시간 제한 알림 간격을 기본 1분에서 연장할 수 있습니다.

실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션을 사용하면 다른 그룹 정책에서 시간 제한 값을 상속하도록 허용됩니다. 값을 상속하지 못하도록 하려면 **vpn-session-timeout none** 명령을 사용합니다.

vpn-session-timeout {*minutes* | **none**} [**alert-interval** *minutes*]

no vpn-session-timeout

no vpn-session-timeout alert-interval

구문 설명

minutes	시간 제한(분) 및 시간 제한 알림 전까지의 경과 시간(분)을 지정합니다. 1~35791394의 정수를 사용합니다.
none	무제한 세션 시간 제한을 허용합니다. null 값으로 세션 시간 제한을 설정하여 세션 시간 제한을 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 값을 상속받는 것을 방지합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.
9.7(1)	**alert-interval**이 AnyConnect VPN에 적용되었습니다.

예

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 180분의 VPN 세션 시간 제한을 설정하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-session-timeout 180
```

관련 명령

group-policy	그룹 정책을 만들거나 수정합니다.
vpn-idle-timeout	사용자 시간 제한을 구성합니다. 이 기간 동안 연결을 통한 통신 활동이 없는 경우 ASA는 연결을 종료합니다.

vpnsetup

ASA에서 VPN 연결을 구성하기 위한 단계 목록을 표시하려면 전역 구성 모드에서 **vpnsetup** 명령을 사용합니다.

vpnsetup {**ipsec-remote-access** | **l2tp-remote-access** | **site-to-site** | **ssl-remote-access**} **steps**

구문 설명

ipsec-remote-access	IPsec 연결을 허용하도록 ASA를 구성하는 단계를 표시합니다.
l2tp-remote-access	L2TP 연결을 허용하도록 ASA를 구성하는 단계를 표시합니다.
site-to-site	LAN-to-LAN 연결을 허용하도록 ASA를 구성하는 단계를 표시합니다.
ssl-remote-access	SSL 연결을 허용하도록 ASA를 구성하는 단계를 표시합니다.
steps	연결 유형에 대한 단계를 표시하도록 지정합니다.

기본값

이 명령에는 기본 설정이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
8.0(3)	이 명령이 추가되었습니다.
9.0(1)	다중 컨텍스트 모드에 대한 지원이 추가되었습니다.

예

다음 예에서는 **vpnsetup ssl-remote-access steps** 명령의 출력을 보여 줍니다.

```
ciscoasa(config-t)# vpnsetup ssl-remote-access steps

Steps to configure a remote access SSL VPN remote access connection and AnyConnect with
examples:

1. Configure and enable interface

    interface GigabitEthernet0/0
     ip address 10.10.4.200 255.255.255.0
     nameif outside
     no shutdown

    interface GigabitEthernet0/1
     ip address 192.168.0.20 255.255.255.0
     nameif inside
     no shutdown
```

```
2. Enable WebVPN on the interface

    webvpn
     enable outside

3. Configure default route

    route outside 0.0.0.0 0.0.0.0 10.10.4.200

4. Configure AAA authentication and tunnel group

    tunnel-group DefaultWEBVPNGroup type remote-access
    tunnel-group DefaultWEBVPNGroup general-attributes
     authentication-server-group LOCAL

5. If using LOCAL database, add users to the Database

    username test password t3stP@ssw0rd
    username test attributes
     service-type remote-access

Proceed to configure AnyConnect VPN client:

6. Point the ASA to an AnyConnect image

    webvpn
     svc image anyconnect-win-2.1.0148-k9.pkg

7. enable AnyConnect

    svc enable

8. Add an address pool to assign an ip address to the AnyConnect client

    ip local pool client-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

9. Configure group policy

    group-policy DfltGrpPolicy internal
    group-policy DfltGrpPolicy attributes
     vpn-tunnel-protocol svc webvpn

ciscoasa(config-t)#
```

관련 명령

Command(명령)	설명
show running-config	ASA의 실행 중인 구성을 표시합니다.

vpn-simultaneous-logins

사용자에게 허용되는 동시 로그인 수를 구성하려면 group-policy 구성 모드 또는 username 구성 모드에서 **vpn-simultaneous-logins** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 옵션을 사용하면 다른 그룹 정책에서 값을 상속받을 수 있습니다. 0을 입력하여 로그인을 비활성화하고 사용자 액세스를 방지합니다.

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

구문 설명

integer	0에서 2147483647 사이의 숫자입니다.

기본값

기본값은 3개의 동시 로그인입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

0을 입력하여 로그인을 비활성화하고 사용자 액세스를 방지합니다.

참고 동시 로그인 수에 대한 최대 한계치는 매우 높지만 여러 개의 동시 로그인을 허용하면 보안이 손상되고 성능에 영향을 미칠 수 있습니다.

"새" 세션이 동일한 사용자 이름으로 설정된 경우에도 기존 AnyConnect, IPsec 클라이언트 또는 클라이언트리스 세션(비정상적으로 종료된 세션)이 세션 데이터베이스에 그대로 남을 수 있습니다.

vpn-simultaneous-logins 값이 1인 경우 비정상 종료 후 동일한 사용자가 다시 로그인하면 시간이 경과된 세션이 데이터베이스에서 제거되고 새 세션이 설정됩니다. 그러나 기존 세션이 계속 활성 연결 상태이며 동일한 사용자가 다른 PC에서 다시 로그인하는 경우, 첫 번째 세션이 로그오프되고 데이터베이스에서 제거되며 새 세션이 설정됩니다.

동시 로그인 수가 1보다 큰 값인 경우 최대 수에 도달한 후에 다시 로그인을 시도하면 유휴 시간이 가장 긴 세션이 로그오프됩니다. 모든 현재 세션이 동일하게 오랜 시간 동안 유휴 상태인 경우 가장 오래된 세션이 로그오프됩니다. 이 동작은 세션을 비우고 새 로그인을 허용합니다.

예

다음 예는 이름이 FirstGroup인 그룹 정책에 대해 최대 4개의 동시 로그인을 허용하는 방법을 보여줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

VPN 터널 유형(IKEv1 또는 IKEv2 사용 IPsec, L2TP over IPsec, SSL 또는 클라이언트리스 SSL)을 구성하려면 group-policy 구성 모드 또는 username 구성 모드에서 **vpn-tunnel-protocol** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vpn-tunnel-protocol {**ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless**}

no vpn-tunnel-protocol {**ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless**}

구문 설명

ikev1	두 피어(원격 액세스 클라이언트 또는 다른 보안 게이트웨이) 간에 IKEv1을 사용하는 IPsec 터널을 협상합니다. 인증, 암호화, 캡슐화 및 키 관리를 제어하는 보안 연계를 생성합니다.
ikev2	두 피어(원격 액세스 클라이언트 또는 다른 보안 게이트웨이) 간에 IKEv2을 사용하는 IPsec 터널을 협상합니다. 인증, 암호화, 캡슐화 및 키 관리를 제어하는 보안 연계를 생성합니다.
l2tp-ipsec	L2TP 연결에 대해 IPsec 터널을 협상합니다.
ssl-client	SSL VPN 클라이언트와 SSL VPN 터널을 협상합니다.
ssl-clientless	HTTPS 지원 웹 브라우저를 통해 원격 사용자에게 VPN 서비스를 제공하며, 클라이언트는 필요하지 않습니다.

기본값

기본값은 IPsec입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

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

명령 기록

Release	**수정 사항**
7.0(1)	이 명령이 추가되었습니다.
7.2(1)	**l2tp-ipsec** 키워드가 추가되었습니다.
7.3(1)	**svc** 키워드가 추가되었습니다.
8.4(1)	**ipsec** 키워드가 **ikev1** 및 **ikev2** 키워드로 대체되었습니다.

사용 지침

이 명령을 사용하여 하나 이상의 터널링 모드를 구성할 수 있습니다. 사용자가 VPN 터널을 통해 연결하려면 하나 이상의 터널링 모드를 구성해야 합니다.

참고 IPsec에서 SSL로의 대체를 지원하려면 **vpn-tunnel-protocol** 명령에서 **svc** 및 **ipsec** 인수를 둘 다 구성해야 합니다.

예

다음 예에서는 "FirstGroup" 이라는 그룹 정책에 대한 WebVPN 및 IPsec 터널링 모드를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# vpn-tunnel-protocol webvpn
ciscoasa(config-group-policy)# vpn-tunnel-protocol IPsec
```

관련 명령

Command(명령)	설명
address pools	원격 클라이언트에 주소를 할당하기 위한 주소 풀 목록을 지정합니다.
show running-config group-policy	모든 그룹 정책 또는 특정 그룹 정책에 대한 구성을 표시합니다.

vtep-nve

VXLAN VNI인터페이스를 VTEP 소스 인터페이스와 연결하려면 인터페이스 구성 모드에서 **vtep-nve** 명령을 사용합니다. 연결을 제거하려면 이 명령의 **no** 형식을 사용합니다.

vtep-nve 1

no vtep-nve 1

구문 설명

1	NVE 인스턴스를 지정합니다. 이 인스턴스는 항상 1입니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
인터페이스 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.4(1)	이 명령이 추가되었습니다.

사용 지침

ASA 또는 보안 상황별로 1개의 VTEP 소스 인터페이스를 구성할 수 있습니다. 이 VTEP 소스 인터페이스를 지정하는 NVE 인스턴스 1개를 구성할 수 있습니다. 모든 VNI 인터페이스는 이 NVE 인스턴스와 연결되어야 합니다.

예

다음 예에서는 GigabitEthernet 1/1 인터페이스를 VTEP 소스 인터페이스로 구성하고 VNI 1 인터페이스를 이 인터페이스와 연결합니다.

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

관련 명령

Command(명령)	설명
debug vxlan	VXLAN 트래픽을 디버깅합니다.
default-mcast-group	VTEP 소스 인터페이스와 연결된 모든 VIN 인터페이스에 대한 기본 멀티캐스트 그룹을 지정합니다.
encapsulation vxlan	NVE 인스턴스를 VXLAN 캡슐화로 설정합니다.
inspect vxlan	표준 VXLAN 헤더 형식 준수를 적용합니다.
interface vni	VXLAN 태그 지정을 위한 VNI 인터페이스를 생성합니다.
mcast-group	VNI 인터페이스에 대한 멀티캐스트 그룹 주소를 설정합니다.
nve	네트워크 가상화 엔드포인트 인스턴스를 지정합니다.
nve-only	VXLAN 소스 인터페이스를 NVE 전용으로 지정합니다.
peer ip	피어 VTEP IP 주소를 수동으로 지정합니다.
segment-id	VNI 인터페이스에 대한 VXLAN 세그먼트 ID를 지정합니다.
show arp vtep-mapping	원격 세그먼트 도메인에 위치한 IP 주소 및 원격 VTEP IP 주소의 VNI 인터페이스에서 캐시된 MAC 주소를 표시합니다.
show interface vni	VNI 인터페이스의 파라미터, 상태 및 통계, 브리지된 인터페이스(구성된 경우)의 상태, 연결된 NVE 인터페이스를 표시합니다.
show mac-address-table vtep-mapping	원격 VTEP IP 주소의 VNI 인터페이스에 있는 레이어 2 포워딩 테이블(MAC 주소 테이블)을 표시합니다.
show nve	NVE 인터페이스의 파라미터, 상태 및 통계, 그 캐리어 인터페이스(소스-인터페이스)의 상태, 캐리어 인터페이스의 IP 주소, 이 NVE를 VXLAN VTEP로 사용하는 VNI, 이 NVE 인터페이스와 연결된 피어 VTEP IP 주소를 표시합니다.
show vni vlan-mapping	투명 모드에서 VNI 세그먼트 ID와 VLAN 인터페이스 또는 물리적 인터페이스 간의 매핑을 표시합니다.
source-interface	VTEP 소스 인터페이스를 지정합니다.
vxlan port	VXLAN UDP 포트를 설정합니다. 기본적으로, VTEP 소스 인터페이스는 UDP 포트 4789에 대해 VXLAN 트래픽을 승인합니다.

vxlan port

VXLAN UDP 포트를 설정하려면 전역 구성 모드에서 **vxlan port** 명령을 사용합니다. 기본 포트를 복원하려면 이 명령의 **no** 형식을 사용합니다.

vxlan port *udp_port*

no vxlan port *udp_port*

구문 설명

udp_port	VXLAN UDP 포트를 설정합니다. 기본값은 4789입니다.

명령 기본값

기본 포트는 4789입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
nve 구성	• 예	• 예	• 예	—	• 예

명령 기록

Release	수정 사항
9.4(1)	이 명령이 추가되었습니다.

사용 지침

기본적으로, VTEP 소스 인터페이스는 UDP 포트 4789에 대해 VXLAN 트래픽을 승인합니다. 네트워크에서 비표준 포트를 사용하는 경우 변경할 수 있습니다.

예

예를 들면 다음과 같습니다.

```
ciscoasa(config)# vxlan port 5678
```

관련 명령

Command(명령)	설명
debug vxlan	VXLAN 트래픽을 디버깅합니다.
default-mcast-group	VTEP 소스 인터페이스와 연결된 모든 VIN 인터페이스에 대한 기본 멀티캐스트 그룹을 지정합니다.
encapsulation vxlan	NVE 인스턴스를 VXLAN 캡슐화로 설정합니다.
inspect vxlan	표준 VXLAN 헤더 형식 준수를 적용합니다.
interface vni	VXLAN 태그 지정을 위한 VNI 인터페이스를 생성합니다.
mcast-group	VNI 인터페이스에 대한 멀티캐스트 그룹 주소를 설정합니다.

Command(명령)	설명
nve	네트워크 가상화 엔드포인트 인스턴스를 지정합니다.
nve-only	VXLAN 소스 인터페이스를 NVE 전용으로 지정합니다.
peer ip	피어 VTEP IP 주소를 수동으로 지정합니다.
segment-id	VNI 인터페이스에 대한 VXLAN 세그먼트 ID를 지정합니다.
show arp vtep-mapping	원격 세그먼트 도메인에 위치한 IP 주소 및 원격 VTEP IP 주소의 VNI 인터페이스에서 캐시된 MAC 주소를 표시합니다.
show interface vni	VNI 인터페이스의 파라미터, 상태 및 통계, 브리지된 인터페이스(구성된 경우)의 상태, 연결된 NVE 인터페이스를 표시합니다.
show mac-address-table vtep-mapping	원격 VTEP IP 주소의 VNI 인터페이스에 있는 레이어 2 포워딩 테이블(MAC 주소 테이블)을 표시합니다.
show nve	NVE 인터페이스의 파라미터, 상태 및 통계, 그 캐리어 인터페이스(소스-인터페이스)의 상태, 캐리어 인터페이스의 IP 주소, 이 NVE를 VXLAN VTEP로 사용하는 VNI, 이 NVE 인터페이스와 연결된 피어 VTEP IP 주소를 표시합니다.
show vni vlan-mapping	투명 모드에서 VNI 세그먼트 ID와 VLAN 인터페이스 또는 물리적 인터페이스 간의 매핑을 표시합니다.
source-interface	VTEP 소스 인터페이스를 지정합니다.
vtep-nve	VNI 인터페이스를 VTEP 소스 인터페이스와 연결합니다.

5장

wccp~zone-member 명령

wccp

서비스 그룹에 참여하기 위해 공간을 할당하고 지정된 WCCP(Web Cache Communication Protocol) 서비스의 지원을 활성화하려면 전역 구성 모드에서 **wccp** 명령을 사용합니다. 서비스 그룹을 비활성화하고 공간 할당을 취소하려면 이 명령의 no 형식을 사용합니다.

wccp {**web-cache** | ***service-number***} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]

no wccp {**web-cache** | ***service-number***} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]]

구문 설명

access-list	액세스 목록의 이름을 지정합니다.
group-list	(선택 사항) 서비스 그룹에 참여할 수 있는 웹 캐시를 결정하는 액세스 목록입니다. access-list 인수는 액세스 목록을 지정하는 64자 이내의 문자열(이름 또는 숫자)로 구성되어야 합니다.
password	(선택 사항) 서비스 그룹에서 수신된 메시지에 대한 MD5(Message Digest 5) 인증을 지정합니다. 인증에서 허용되지 않은 메시지는 삭제됩니다.
password	인증에 사용할 비밀번호를 지정합니다. password 인수는 최대 7자일 수 있습니다.
redirect-list	(선택 사항) 이 서비스 그룹으로 리디렉션되는 트래픽을 제어하는 액세스 목록과 함께 사용됩니다. access-list 인수는 액세스 목록을 지정하는 64자 이내의 문자열(이름 또는 숫자)로 구성되어야 합니다. 액세스 목록은 네트워크 주소만 포함해야 합니다. 포트 관련 항목은 지원되지 않습니다.
service-number	서비스 정의가 캐시에 의해 지정됨을 의미하는 동적 서비스 식별자입니다. 동적 서비스 번호는 0~254이며, 최대 255개일 수 있습니다. 최대 허용 개수는 256이며, 여기에는 **web-cache** 키워드로 지정되는 웹 캐시 서비스가 포함됩니다.
web-cache	웹 캐시 서비스를 지정합니다. **참고** 웹 캐시는 하나의 서비스로 계산됩니다. service-number 인수로 할당된 서비스를 포함하여 최대 서비스 수는 256개입니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다 .

예

다음 예에서는 서비스 그룹에 참여할 수 있도록 WCCP를 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

관련 명령

명령	설명
show wccp	WCCP 구성을 표시합니다.
wccp redirect	WCCP 리디렉션 지원을 활성화합니다.

wccp redirect

WCCP(Web Cache Communication Protocol)를 사용하여 인터페이스의 이그레스에서 패킷 리디렉션을 활성화하려면 **wccp redirect** 명령을 사용합니다. WCCP 리디렉션을 비활성화하려면 이 명령의 no 형식을 사용합니다.

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

구문 설명

in	이 인터페이스로 패킷이 들어올 때의 리디렉션을 지정합니다.
interface_name	패킷을 리디렉션해야 하는 인터페이스의 이름입니다.
service	서비스 그룹을 지정합니다. **web-cache** 키워드를 지정하거나, 서비스의 식별 번호(0~99)를 지정할 수 있습니다.

기본값

이 명령은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

예

다음 예에서는 웹 캐시 서비스의 내부 인터페이스에서 WCCP 리디렉션을 활성화하는 방법을 보여 줍니다.

```
ciscoasa(config)# wccp interface inside web-cache redirect in
```

관련 명령

명령	설명
show wccp	WCCP 컨피그레이션을 표시합니다.
wccp	서비스 그룹에 대한 WCCP 지원을 활성화합니다.

web-agent-url(사용되지 않음)

참고 마지막으로 이 명령을 지원하는 릴리스는 버전 9.3(1)이었습니다.

ASA에서 SiteMinder 유형 SSO 인증을 요청할 SSO 서버 URL을 지정하려면 config-webvpn-sso-siteminder 모드에서 **web-agent-url** 명령을 사용합니다.

SSO 서버 인증 URL을 제거하려면 이 명령의 **no** 형식을 사용합니다.

web-agent-url *url*

no web-agent-url *url*

참고 이 명령은 SiteMinder-type SSO 인증에 필요합니다.

구문 설명

url	SiteMinder-type SSO 서버의 인증 URL을 지정합니다. http:// 또는 https://를 포함해야 합니다.

기본값

기본적으로 인증 URL은 구성되지 않습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
config-webvpn-sso-siteminder	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.
9.5(2)	이 명령은 SAML 2.0 지원으로 인해 사용이 중단되었습니다.

사용 지침

SSO(WebVPN에만 제공) 지원을 통해 사용자가 사용자 이름 및 비밀번호를 단 한 번만 입력하여 여러 서버에서 다양한 보안 서비스에 액세스할 수 있습니다. SSO 서버는 인증 요청을 처리하는 URL이 있습니다.

이 명령은 SiteMinder 유형 SSO 서버에만 적용됩니다.

web-agent-url 명령을 사용하여 이 URL로 인증을 보내도록 ASA를 구성할 수 있습니다. 인증 URL을 구성하기 전에 **sso-server** 명령을 사용하여 SSO 서버를 생성해야 합니다.

보안 어플라이언스와 SSO 서버 간의 https 통신에서는 SSL 암호화 설정이 양쪽에서 일치하는지 확인합니다. 보안 어플라이언스에서는 **ssl encryption** 명령을 사용하여 이를 확인합니다.

예

config-webvpn-sso-siteminder 모드에서 입력된 다음 예에서는 인증 URL을 http://www.example.com/webvpn으로 지정합니다.

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
ciscoasa(config-webvpn-sso-siteminder)#
```

관련 명령

Command(명령)	설명
max-retry-attempts	실패한 SSO 인증 시도에 대해 ASA에서 재시도할 횟수를 구성합니다.
policy-server-secret	SiteMinder-type SSO 서버에 대한 인증 요청을 암호화하는 데 사용되는 비밀 키를 생성합니다.
request-timeout	시간 초과로 인해 SSO 인증 시도가 실패하는 시간(초)을 지정합니다.
show webvpn sso-server	보안 디바이스에 구성된 모든 SSO 서버에 대한 운영 통계를 표시합니다.
ssl encryption	SSL/TLS 프로토콜에서 사용하는 암호화 알고리즘을 지정합니다.
sso-server	SSO(Single Sign-On) 서버를 생성합니다.

web-applications

인증된 WebVPN 사용자에게 표시되는 WebVPN 홈 페이지의 Web Application(웹 애플리케이션) 상자를 사용자 지정하려면 webvpn customization 모드에서 **web-applications** 명령을 사용합니다.

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

구성에서 명령을 제거하고 값을 상속받도록 하려면 **no** 형식의 다음 명령을 사용합니다.

구문 설명

title	제목을 변경하도록 지정합니다.
message	제목 아래에 표시되는 메시지를 변경하도록 지정합니다.
dropdown	드롭다운 상자를 변경하도록 지정합니다.
text	텍스트를 변경하도록 지정합니다.
style	HTML 스타일을 변경하도록 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 파라미터(최대 256자)입니다.

기본값

기본 제목 텍스트는 "Web Application" 입니다.

기본 제목 스타일은 background-color:#99CCCC;color:black;font-weight:bold;text-transform: uppercase

기본 메시지 텍스트는 "Enter Web Address (URL)" 입니다.

기본 메시지 스타일은 background-color:#99CCCC;color:maroon;font-size:smaller입니다.

기본 드롭다운 텍스트는 "Web Bookmarks" 입니다.

기본 드롭다운 스타일은 border:1px solid black;font-weight:bold;color:black;font-size:80%입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅 됨**	**투명**	**단일**	**상황**	**시스템**
webvpn customization	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 유효한 모든 CSS(Cascading Style Sheet) 파라미터로 표현됩니다. 이러한 파라미터에 대한 설명은 이 문서의 범위를 벗어납니다. CSS 파라미터에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트(www.w3.org)에서 CSS 사양을 참고하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 파라미터 목록이 포함되어 있습니다.

다음은 WebVPN 페이지에서 수행할 수 있는 가장 일반적인 변경(페이지 색상 변경) 작업에 대한 몇 가지 팁입니다.

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

참고 WebVPN 페이지를 쉽게 사용자 지정하려면 색상 견본 및 미리보기 기능 등 스타일 요소 구성에 대한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예에서는 제목을 "Applications"로 변경하고 텍스트 색상으로 파란색으로 변경합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-applications title text Applications
ciscoasa(config-webvpn-custom)# web-applications title style color:blue
```

관련 명령

Command(명령)	설명
application-access	WebVPN 홈 페이지의 Application Access(애플리케이션 액세스) 상자를 맞춤 설정합니다.
browse-networks	WebVPN 홈 페이지의 Browse Networks(네트워크 찾아보기) 상자를 맞춤 설정합니다.
web-bookmarks	WebVPN 홈 페이지에서 Web Bookmarks(웹 책갈피) 제목 또는 링크를 맞춤 설정합니다.
file-bookmarks	WebVPN 홈 페이지에서 File Bookmarks(파일 책갈피) 제목 또는 링크를 맞춤 설정합니다.

web-bookmarks

인증된 WebVPN 사용자에게 표시되는 WebVPN 홈 페이지의 Web Bookmarks(웹 책갈피) 제목 또는 링크를 사용자 지정하려면 webvpn customization 모드에서 **web-bookmarks** 명령을 사용합니다.

web-bookmarks {**link** {**style** *value*} **| title** {**style** *value* **| text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} **| title** {**style** *value* **| text** *value*}}

구성에서 명령을 제거하고 값을 상속받도록 하려면 **no** 형식의 다음 명령을 사용합니다.

구문 설명

link	링크를 변경하도록 지정합니다.
title	제목을 변경하도록 지정합니다.
style	HTML 스타일을 변경하도록 지정합니다.
text	텍스트를 변경하도록 지정합니다.
value	표시할 실제 텍스트(최대 256자) 또는 CSS(Cascading Style Sheet) 매개변수(최대 256자)입니다.

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 "Web Bookmarks" 입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
webvpn customization	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.1(1)	이 명령이 추가되었습니다.

사용 지침

style 옵션은 유효한 모든 CSS(Cascading Style Sheet) 매개변수로 표현됩니다. 이러한 매개변수에 대한 설명은 이 문서의 범위를 벗어납니다. CSS 매개변수에 대한 자세한 내용은 W3C(World Wide Web Consortium) 웹사이트(www.w3.org)에서 CSS 사양을 참고하십시오. CSS 2.1 사양의 부록 F(www.w3.org/TR/CSS21/propidx.html)에는 CSS 매개변수 목록이 포함되어 있습니다.

다음은 WebVPN 페이지에서 수행할 수 있는 가장 일반적인 변경(페이지 색상 변경) 작업에 대한 몇 가지 팁입니다.

- 쉼표로 구분된 RGB 값, HTML 색상 값 또는 색상 이름(HTML에서 인식되는 경우)을 사용할 수 있습니다.

- RGB 형식은 0,0,0이며, 각 색상(빨간색, 녹색, 파란색)의 십진수 범위는 0~255입니다. 여기서 쉼표로 구분된 항목은 다른 색상과 조합할 각 색상의 강도를 나타냅니다.
- HTML 형식은 16진수 형식의 6자리 숫자인 #000000입니다. 여기서 첫 번째와 두 번째는 빨간색, 세 번째와 네 번째는 녹색, 다섯 번째와 여섯 번째는 파란색을 나타냅니다.

참고 WebVPN 페이지를 쉽게 사용자 지정하려면 색상 견본 및 미리보기 기능 등 스타일 요소 컨피그레이션에 대한 편리한 기능이 있는 ASDM을 사용하는 것이 좋습니다.

예

다음 예에서는 Web Bookmarks(웹 책갈피) 제목을 "Corporate Web Bookmarks"로 맞춤 설정합니다.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

관련 명령

Command(명령)	설명
application-access	WebVPN 홈 페이지의 Application Access(애플리케이션 액세스) 상자를 맞춤 설정합니다.
browse-networks	WebVPN 홈 페이지의 Browse Networks(네트워크 찾아보기) 상자를 맞춤 설정합니다.
file-bookmarks	WebVPN 홈 페이지에서 File Bookmarks(파일 책갈피) 제목 또는 링크를 맞춤 설정합니다.
web-applications	WebVPN 홈 페이지의 Web Application(웹 애플리케이션) 상자를 맞춤 설정합니다.

webvpn (global)

webvpn 모드를 시작하려면 전역 구성 모드에서 **webvpn** 명령을 입력합니다. 이 명령과 함께 입력된 모든 명령을 제거하려면 **no webvpn** 명령을 사용합니다. 이러한 **webvpn** 명령은 모든 WebVPN 사용자에게 적용됩니다.

이러한 **webvpn** 명령을 통해 AAA 서버, 기본 그룹 정책, 기본 유휴 시간 제한, http 및 https 프록시, WebVPN용 NBNS 서버, 엔드 유저에게 표시되는 WebVPN 화면의 모양 등을 구성할 수 있습니다.

webvpn

no webvpn

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

WebVPN은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예		—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 WebVPN 모드에서는 WebVPN에 대한 전역 설정을 구성할 수 있습니다. group-policy 모드 또는 username 모드에서 시작된 WebVPN 모드에서는 특정 사용자 또는 그룹 정책에 대한 WebVPN 구성을 사용자 지정할 수 있습니다. ASA 클라이언트리스 SSL VPN 구성에서는 http-proxy와 https-proxy 명령을 각각 하나씩만 지원합니다.

참고 WebVPN이 작동하려면 브라우저 캐싱을 활성화해야 합니다.

예

다음 예에서는 WebVPN 명령 모드를 시작하는 방법을 보여 줍니다.

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

webvpn (group-policy attributes, username attributes)

이 webvpn 모드를 시작하려면 group-policy attributes 구성 모드 또는 username attributes 구성 모드에서 **webvpn** 명령을 사용합니다. webvpn 모드에서 입력된 모든 명령을 제거하려면 이 명령의 **no** 형식을 사용합니다. 이 webvpn 명령은 이 명령을 구성한 사용자 이름 또는 그룹 정책에 적용됩니다.

그룹 정책 및 사용자 이름에 대한 Webvpn 명령은 WebVPN을 통한 파일, MAPI 프록시, URL 및 TCP 애플리케이션 액세스를 정의합니다. 또한 필터링할 ACL 및 트래픽 유형을 식별합니다.

webvpn

no webvpn

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

WebVPN은 기본적으로 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
group-policy 속성 구성	• 예	—	• 예		—
Username 속성 구성	• 예	—	• 예		—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

전역 구성 모드에서 시작된 Webvpn 모드에서는 WebVPN에 대한 전역 설정을 구성할 수 있습니다. group-policy attributes 구성 모드 또는 username attributes 구성 모드의 **webvpn** 명령은 webvpn 명령에 지정된 설정을 상위 명령에 지정된 그룹 또는 사용자에게 적용합니다. 즉, 이 섹션에 설명되고 group-policy 또는 username 모드에서 시작된 webvpn 모드에서는 특정 사용자 그룹 정책에 대한 WebVPN 구성을 사용자 지정할 수 있습니다.

group-policy attributes 모드에서 특정 그룹 정책에 적용한 webvpn 특성은 기본 그룹 정책에 지정된 특성을 재정의합니다. username attributes 모드에서 특정 사용자에게 적용한 WebVPN 특성은 기본 그룹 정책 및 해당 사용자가 속한 그룹 정책에 지정된 특성을 모두 재정의합니다. 기본적으로 이러한 명령을 사용하면 기본 그룹 또는 지정된 그룹 정책에서 상속되는 설정을 조정할 수 있습니다. WebVPN 설정에 대한 자세한 내용은 전역 구성 모드의 **webvpn** 명령에 대한 설명을 참고하십시오.

다음 표에는 webvpn group-policy attributes 및 username attributes 모드에서 구성할 수 있는 특성이 나와 있습니다. 자세한 내용은 개별 명령 설명을 참고하십시오.

속성	설명
auto-signon	WebVPN 사용자에 대한 SSO(Single Sign-On) 방법을 제공하여 WebVPN 사용자 로그인 크리덴셜을 내부 서버로 자동으로 전달하도록 ASA를 구성합니다.
customization	적용할 사전 구성된 WebVPN 맞춤 설정을 지정합니다.
deny-message	액세스가 거부된 경우 사용자에게 표시할 메시지를 지정합니다.
filter	WebVPN 연결에 사용할 액세스 목록을 식별합니다.
functions	파일 액세스 및 파일 검색, MAPI 프록시, WebVPN을 통한 URL 입력을 구성합니다.
homepage	WebVPN 사용자가 로그인할 때 표시되는 웹 페이지의 URL을 설정합니다.
html-content-filter	WebVPN 세션에 대해 필터링할 Java, ActiveX, 이미지, 스크립트 및 쿠키를 식별합니다.
http-comp	사용할 HTTP 압축 알고리즘을 지정합니다.
keep-alive-ignore	세션 업데이트 시 무시할 최대 개체 크기를 지정합니다.
port-forward	WebVPN 애플리케이션 액세스를 활성화합니다.
port-forward-name	엔드 유저에 대한 TCP 포트 전달을 식별하는 표시 이름을 구성합니다.
sso-server	SSO 서버 이름을 구성합니다.
svc	SSL VPN 클라이언트 특성을 구성합니다.
url-list	사용자가 WebVPN을 통해 액세스할 수 있는 서버 및 URL 목록을 식별합니다.

예

다음 예에서는 "FirstGroup"이라는 그룹 정책에 대한 webvpn 모드를 시작하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-webvpn)#
```

다음 예에서는 "test"라는 사용자 이름에 대한 webvpn 모드를 시작하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy test attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-webvpn)#
```

관련 명령

clear configure group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대한 구성을 제거합니다.
group-policy attributes	지정된 그룹 정책에 대한 특성 및 값을 구성하거나, webvpn 모드를 시작하여 그룹에 대한 webvpn 특성을 구성할 수 있는 config-group-policy 모드를 시작합니다.
show running-config group-policy	특정 그룹 정책 또는 모든 그룹 정책에 대한 실행 중인 구성을 표시합니다.
webvpn	지정된 그룹에 대한 WebVPN 특성을 구성할 수 있는 config-group-webvpn 모드를 시작합니다.

whitelist

Cloud Web Security의 경우 트래픽의 클래스에 대한 화이트리스트 작업을 수행하려면 클래스 구성 모드에서 **whitelist** 명령을 사용합니다. 먼저 **policy-map type inspect scansafe** 명령을 입력한 다음 **parameters** 명령을 입력하여 클래스 구성 모드에 액세스할 수 있습니다. 화이트리스트를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

whitelist

no whitelist

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
클래스 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.0(1)	이 명령이 추가되었습니다.

사용 지침

class-map type inspect scansafe 명령을 사용하여 허용 목록에 추가할 트래픽을 식별합니다. **policy-map type inspect scansafe** 명령에서 검사 클래스 맵을 사용하고 해당 클래스에 대해 **whitelist** 작업을 지정합니다. **inspect scansafe** 명령에서 검사 정책 맵을 호출합니다.

예

다음 예에서는 HTTP 및 HTTPS 검사 정책 맵에 대해 동일한 사용자 및 그룹을 화이트리스트에 추가합니다.

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

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

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

관련 명령

Command(명령)	설명
class-map type inspect scansafe	허용 목록의 사용자 및 그룹에 대한 검사 클래스 맵을 생성합니다.
default user group	ASA에서 ASA에 연결하는 사용자의 ID를 확인할 수 없는 경우 기본 사용자 이름 및/또는 그룹을 지정합니다.
http[**s**](parameters)	검사 정책 맵의 서비스 유형(HTTP 또는 HTTPS)을 지정합니다.
inspect scansafe	클래스에서 트래픽에 대한 Cloud Web Security 검사를 활성화합니다.
license	요청을 보낸 조직을 나타내기 위해 ASA에서 Cloud Web Security 프록시 서버로 보내는 인증 키를 구성합니다.
match user group	화이트리스트를 기준으로 사용자 또는 그룹을 확인합니다.
policy-map type inspect scansafe	규칙의 필수 파라미터를 구성하고 선택적으로 허용 목록을 식별할 수 있도록 검사 정책 맵을 생성합니다.
retry-count	Cloud Web Security 프록시 서버를 폴링하여 가용성 여부를 확인하기까지 ASA에서 대기하는 시간인 재시도 카운터 값을 입력합니다.
scansafe	다중 컨텍스트 모드에서는 컨텍스트 단위로 Cloud Web Security를 허용합니다.
scansafe general-options	일반 Cloud Web Security 서버 옵션을 구성합니다.
server {**primary** | **backup**}	기본 또는 백업 Cloud Web Security 프록시 서버의 FQDN(Fully Qualified Domain Name) 또는 IP 주소를 구성합니다.
show conn scansafe	대문자 Z 플래그를 지정하여 모든 Cloud Web Security 연결을 표시합니다.
show scansafe server	서버의 상태, 즉 현재 활성 서버인지, 백업 서버인지 또는 도달할 수 없는 서버인지 표시합니다.
show scansafe statistics	총 HTTP 연결 수와 현재 HTTP 연결 수를 표시합니다.
user-identity monitor	지정된 사용자 또는 그룹 정보를 AD 에이전트에서 다운로드합니다.

who

ASA의 활성 Telnet 관리 세션을 표시하려면 특권 EXEC 모드에서 **who** 명령을 사용합니다.

who [*local_ip*]

구문 설명

local_ip	(선택 사항) 하나의 내부 IP 주소 또는 네트워크 주소(IPv4 또는 IPv6)로 목록을 제한하려면 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

who 명령을 사용하면 현재 ASA에 로그인된 각 Telnet 클라이언트의 TTY_ID 및 IP 주소를 표시할 수 있습니다.

예

다음 예에서는 클라이언트가 Telnet 세션을 통해 ASA에 로그인한 경우 **who** 명령의 출력을 표시합니다.

```
ciscoasa# who
0: 100.0.0.2
ciscoasa# who 100.0.0.2
0: 100.0.0.2
ciscoasa#
```

관련 명령

Command(명령)	설명
kill	Telnet 세션을 종료합니다.
telnet	Telnet 액세스를 ASA 콘솔에 추가하고 유휴 시간 제한을 설정합니다.

window-variation

창 크기 변형과의 연결을 끊으려면 tcp-map 구성 모드에서 **window-variation** 명령을 사용합니다. 이 사양을 제거하려면 이 명령의 **no** 형식을 사용합니다.

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

구문 설명

allow-connection	연결을 허용합니다.
drop-connection	연결을 끊습니다.

기본값

기본 동작은 연결을 허용하는 것입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
tcp-map 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

tcp-map 명령은 Modular Policy Framework 인프라와 함께 사용됩니다. **class-map** 명령을 사용하여 트래픽의 클래스를 정의하고, **tcp-map** 명령을 사용하여 TCP 검사를 맞춤 설정합니다. **policy-map** 명령을 사용하여 새 TCP 맵을 적용합니다. **service-policy** 명령을 사용하여 TCP 검사를 활성화합니다.

tcp-map 명령을 사용하여 tcp-map 구성 모드를 시작할 수 있습니다. tcp-map 구성 모드에서 **window-variation** 명령을 사용하여 창 크기가 축소된 모든 연결을 끊을 수 있습니다.

기간 크기 메커니즘은 TCP에서 지나치게 많은 데이터를 허용하지 않고도 큰 기간을 보급하고 이후에 훨씬 작은 기간을 보급할 수 있도록 합니다. TCP 사양에서는 "기간 축소"가 권장되지 않습니다. 이 조건이 탐지되면 연결이 삭제될 수 있습니다.

예

다음 예에서는 창 크기가 다양한 모든 연결을 끊는 방법을 보여 줍니다.

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# window-variation drop-connection
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

Command(명령)	설명
class	트래픽 분류에 사용할 클래스 맵을 지정합니다.
policy-map	정책, 즉 트래픽 클래스와 하나 이상의 작업 연계를 구성합니다.
set connection	연결 값을 구성합니다.
tcp-map	TCP 맵을 만들고 tcp-map 구성 모드에 대한 액세스를 허용합니다.

wins-server

기본 및 보조 WINS 서버의 IP 주소를 설정하려면 group-policy 구성 모드에서 **wins-server** 명령을 사용합니다. 실행 중인 구성에서 특성을 제거하려면 **no** 형식의 이 명령을 입력합니다. 이 옵션을 사용하면 다른 그룹 정책에서 WINS 서버를 상속하도록 허용됩니다. 서버를 상속하지 못하도록 하려면 **wins-server none** 명령을 사용합니다.

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

구문 설명

none	wins-server를 null 값으로 설정하여 WINS 서버를 허용하지 않습니다. 기본 또는 지정된 그룹 정책에서 값을 상속받는 것을 방지합니다.
value *ip_address*	기본 및 보조 WINS 서버의 IP 주소를 설정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
group-policy 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

wins-server 명령을 입력할 때마다 기존 설정을 덮어씁니다. 예를 들어 WINS 서버 x.x.x.x를 구성한 후 WINS 서버 y.y.y.y를 구성하는 경우 두 번째 명령이 첫 번째 명령을 덮어쓰고, y.y.y.y가 유일한 WINS 서버가 됩니다. 다중 서버의 경우도 마찬가지입니다. 이전에 구성한 서버를 덮어쓰지 않고 WINS 서버를 추가하려면 이 명령을 입력할 때 모든 WINS 서버의 IP 주소를 포함하십시오.

예

다음 예에서는 FirstGroup이라는 그룹 정책에 대해 IP 주소가 10.10.10.15, 10.10.10.30 및 10.10.10.45인 WINS 서버를 구성하는 방법을 보여 줍니다.

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

without-csd

group-urls 테이블의 항목 중 하나를 입력하여 VPN 세션을 설정한 경우 연결 프로파일 단위로 실행 중인 Cisco Secure Desktop의 Hostscan 애플리케이션에서 특정 사용자를 제외하려면 tunnel webvpn 구성 모드에서 **without-csd** 명령을 사용합니다. 구성에서 이 명령을 제거하려면 **no** 형식의 명령을 사용합니다.

without-csd [**anyconnect**]

no without-csd [**anyconnect**]

구문 설명

anyconnect	(선택 사항) AnyConnect 연결에만 영향을 주도록 명령을 변경합니다.

기본값

기본값은 없습니다. 설치된 경우 Hostscan이 사용됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
tunnel webvpn 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
8.2(1)	이 명령이 추가되었습니다.
9.2(1)	**anyconnect** 키워드가 추가되었습니다.

사용 지침

이 명령은 사용자가 이 연결 프로파일(CLI에서는 터널 그룹이라고 함)에 구성된 url-group 목록에 URL을 입력한 경우 Cisco Secure Desktop의 Hostscan 애플리케이션이 엔드포인트에서 실행되지 못하도록 합니다. 이 명령을 입력하면 해당 세션에 대한 엔드포인트 상태 감지를 방지하므로 DAP(Dynamic Access Policy: 동적 액세스 정책) 구성을 조정해야 할 수도 있습니다.

예

다음 예의 첫 번째 명령은 "example.com" 이 ASA의 도메인이고 "no-csd" 가 URL의 고유한 부분인 group-url을 만듭니다. 사용자가 이 URL을 입력하면 ASA에서 세션에 이 연결 프로파일을 할당합니다. **without-csd** 명령을 적용하려면 **group-url** 명령이 필요합니다. **without-csd** 명령은 실행 중인 Cisco Secure Desktop에서 사용자를 제외합니다.

```
ciscoasa(config-tunnel-webvpn)# group-url https://example.com/no-csd enable
ciscoasa(config-tunnel-webvpn)# without-csd
ciscoasa(config-tunnel-webvpn)#
```

관련 명령

Command(명령)	설명
csd enable	without-csd 명령이 없는 모든 연결 프로파일에 대해 Cisco Secure Desktop을 활성화합니다.
csd image	명령에 이름이 지정된 Cisco Secure Desktop 이미지를 경로에 지정된 플래시 드라이브에서 실행 중인 구성과으로 복사합니다.
group-url	이 연결 프로파일에 고유한 group-url을 만듭니다.

write erase

시작 구성을 지우려면 특권 EXEC 모드에서 **write erase** 명령을 사용합니다. 실행 중인 구성은 그대로 유지됩니다.

write erase

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	—	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 보안 컨텍스트 내에서 지원되지 않습니다. 상황 시작 구성은 시스템 구성에서 **config-url** 명령으로 식별됩니다. 상황 구성을 삭제하려면 원격 서버(지정된 경우)에서 파일을 수동으로 제거하거나, 시스템 실행 공간에서 **delete** 명령을 사용하여 플래시 메모리에서 파일을 지우면 됩니다.

ASAv에서 이 명령을 사용하면 **다시 로드** 후 구축 구성(초기 가상 구축 설정)이 복원됩니다. 컨피그레이션을 완전히 지우려면 **clear configure all** 명령을 사용합니다. ASA 어플라이언스에 대해 구축 구성을 지우고 ASA 어플라이언스에 적용되는 것과 동일한 공장 기본 구성을 적용하려면 **configure factory-default**를 참고하십시오.

참고 ASAv는 현재 실행 중인 이미지를 부팅하므로 원래 부트 이미지로 되돌아가지 않습니다.

다시 로드하기 전에 구성을 저장하지 마십시오.

장애 조치 쌍의 ASAv에서는 먼저 스탠바이 장치의 전원을 끕니다. 스탠바이 유닛이 활성화되지 않도록 하려면 전원을 꺼야 합니다. 전원을 계속 켜두면 액티브 유닛 컨피그레이션을 지울 때 스탠바이 유닛이 활성화됩니다. 장애 조치 링크를 통해 이전 액티브 유닛이 다시 로드되고 연결될 경우, 새 액티브 유닛에서 기존 컨피그레이션이 동기화되어 사용자가 원하는 구축 컨피그레이션이 지워집니다. 액티브 유닛이 다시 로드되면 스탠바이 유닛의 전원을 켤 수 있습니다. 구축 구성은 스탠바이 유닛에 동기화됩니다.

예

다음 예에서는 시작 구성을 지웁니다.

```
ciscoasa# write erase
Erase configuration in flash memory? [confirm] y
```

관련 명령

Command(명령)	설명
configure net	지정된 TFTP URL의 구성 파일을 실행 중인 구성과 병합합니다.
delete	플래시 메모리에서 파일을 제거합니다.
show running-config	실행 중인 구성을 표시합니다.
write memory	실행 중인 구성을 시작 구성에 저장합니다.

write memory

실행 중인 구성을 시작 구성에 저장하려면 특권 EXEC 모드에서 **write memory** 명령을 사용합니다.

write memory [**all** [**/noconfirm**]]

구문 설명

/noconfirm	**all** 키워드를 사용한 경우 확인 프롬프트를 제거합니다.
all	다중 컨텍스트 모드의 시스템 실행 공간에서 이 키워드는 모든 컨텍스트 구성 및 시스템 구성을 저장합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.2(1)	이제 **all** 키워드를 사용하여 모든 상황 구성을 저장할 수 있습니다.

사용 지침

실행 중인 구성은 명령줄에서 적용한 모든 변경 사항을 포함하여 메모리에서 현재 실행되고 있는 구성입니다. 변경 사항은 시작 구성(시작 시 실행 중인 메모리로 로드되는 구성)에 저장한 경우 재부팅 간에만 유지됩니다. **boot config** 명령을 사용하여 단일 컨텍스트 모드에 대한 시작 구성 위치 및 다중 컨텍스트 모드의 시스템에 대한 시작 구성 위치를 기본 위치(숨겨진 파일)에서 선택한 위치로 변경할 수 있습니다. 다중 컨텍스트 모드의 경우 상황 시작 구성은 시스템 구성에서 **config-url** 명령으로 지정한 위치에 있습니다.

다중 컨텍스트 모드에서는 각 상황에서 **write memory** 명령을 입력하여 현재 상황 구성을 저장할 수 있습니다. 모든 상황 구성을 저장하려면 시스템 실행 공간에서 **write memory all** 명령을 입력합니다. 컨텍스트 시작 컨피그레이션은 외부 서버에 상주할 수 있습니다. 이 경우 ASA는 구성을 서버로 다시 저장할 수 없는 HTTP 및 HTTPS URL을 제외하고는 **config-url** 명령으로 지정된 서버로 구성을 다시 저장합니다. **write memory all** 명령을 통해 ASA가 각 상황을 저장한 후에는 다음과 같은 메시지가 표시됩니다.

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

오류로 인해 컨텍스트가 저장되지 않는 경우가 있습니다. 오류에 대한 내용은 다음 정보를 참조하십시오.

- 적은 메모리로 인해 컨텍스트가 저장되지 않은 경우 다음과 같은 메시지가 표시됩니다.

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- 원격 대상에 연결할 수 없어 저장되지 않는 상황의 경우 다음 메시지가 표시됩니다.

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- 컨텍스트가 잠겨 있어 컨텍스트가 저장되지 않은 경우 다음과 같은 메시지가 표시됩니다.

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context ‘a’ , context ‘x’ , context ‘z’ .
  ```

  컨텍스트는 다른 사용자가 컨피그레이션을 이미 저장하고 있거나 컨텍스트를 삭제하는 중인 경우에만 잠깁니다.

- 시작 컨피그레이션이 읽기 전용(예: HTTP 서버)이라 컨텍스트가 저장되지 않은 경우, 모든 다른 메시지의 하단에 다음과 같은 메시지 보고가 출력됩니다.

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- 플래시 메모리의 불량 섹터로 인해 컨텍스트가 저장되지 않은 경우 다음과 같은 메시지가 표시됩니다.

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

시스템에서는 관리 상황 인터페이스를 사용하여 상황 시작 구성에 액세스하기 때문에 **write memory** 명령에서도 관리 상황 인터페이스를 사용합니다. 그러나 **write net** 명령은 상황 인터페이스를 사용하여 구성을 TFTP 서버에 기록합니다.

write memory 명령은 **copy running-config startup-config** 명령과 같습니다.

예

다음 예에서는 실행 중인 구성을 시작 구성에 저장합니다.

```
ciscoasa# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
ciscoasa#
```

관련 명령

Command(명령)	설명
admin-context	관리 컨텍스트를 설정합니다.
configure memory	시작 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다.
config-url	컨텍스트 구성 위치를 지정합니다.
copy running-config startup-config	실행 중인 구성을 시작 구성에 복사합니다.
write net	실행 중인 컨피그레이션을 TFTP 서버에 복사합니다.

write net

실행 중인 구성을 TFTP 서버에 복사하려면 특권 EXEC 모드에서 **write net** 명령을 사용합니다.

write net [*server***:[***filename***] | :***filename***]**

구문 설명

:*filename*	경로 및 파일 이름을 지정합니다. 이미 **tftp-server** 명령으로 파일 이름을 설정한 경우 이 인수는 선택 사항입니다. 이 명령에서 파일 이름을 지정하고 **tftp-server** 명령에서 이름을 지정한 경우 ASA는 **tftp-server** 명령의 파일 이름을 디렉터리로 처리하고, **write net** 명령의 파일 이름을 디렉터리 아래에 파일로 추가합니다. **tftp-server** 명령 값을 재정의하려면 경로 및 파일 이름 앞에 슬래시를 입력합니다. 슬래시는 경로가 tftpboot 디렉터리에 상대적인 것이 아니라 절대 경로임을 나타냅니다. 이 파일에 대해 생성된 URL에는 파일 이름 경로 앞에 이중 슬래시(//)가 포함됩니다. 원하는 파일이 tftpboot 디렉터리에 있는 경우 tftpboot 디렉터리의 경로를 파일 이름 경로에 포함할 수 있습니다. TFTP 서버가 이 유형의 URL을 지원하지 않으면 **copy running-config tftp** 명령을 대신 사용합니다. **tftp-server** 명령을 사용하여 TFTP 서버 주소를 지정한 경우 콜론(:) 뒤에 파일 이름만 입력할 수 있습니다.
*server***:**	TFTP 서버 IP 주소 또는 이름을 설정합니다. 이 주소는 **tftp-server** 명령에서 설정한 주소가 있다면 이를 재정의합니다. 기본 게이트웨이 인터페이스는 최상위 보안 인터페이스입니다. 그러나 **tftp-server** 명령을 사용하여 다른 인터페이스 이름을 설정할 수 있습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

실행 중인 컨피그레이션은 명령줄에서 적용한 모든 변경 사항을 포함하여 메모리에서 현재 실행되고 있는 컨피그레이션입니다.

다중 상황 모드에서 이 명령은 현재 구성만 저장합니다. 단일 명령으로 모든 상황을 저장할 수는 없습니다. 시스템 및 각 상황에 대해 이 명령을 개별적으로 입력해야 합니다. 그러나 **write net** 명령은 상황 인터페이스를 사용하여 구성을 TFTP 서버에 기록합니다. 반면, **write memory** 명령은 관리 상황 인터페이스를 사용하여 시작 구성에 저장합니다. 시스템에서는 관리 상황 인터페이스를 사용하여 상황 시장 구성에 액세스하기 때문입니다.

write net 명령은 **copy running-config tftp** 명령과 같습니다.

예

다음 예에서는 **tftp-server** 명령에서 TFTP 서버 및 파일 이름을 설정합니다.

```
ciscoasa# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
ciscoasa# write net
```

다음 예에서는 **write net** 명령에서 서버 및 파일 이름을 설정합니다. **tftp-server** 명령은 채워지지 않습니다.

```
ciscoasa# write net 10.1.1.1:/configs/contextbackup.cfg
```

다음 예에서는 **write net** 명령에서 서버 및 파일 이름을 설정합니다. **tftp-server** 명령은 디렉터리 이름을 제공하므로 서버 주소가 재정의됩니다.

```
ciscoasa# tftp-server 10.1.1.1 configs
ciscoasa# write net 10.1.2.1:context.cfg
```

관련 명령

Command(명령)	설명
configure net	지정된 TFTP URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과 병합합니다.
copy running-config tftp	실행 중인 구성을 TFTP 서버에 복사합니다.
show running-config	실행 중인 구성을 표시합니다.
tftp-server	다른 명령에 사용할 기본 TFTP 서버 및 경로를 설정합니다.
write memory	실행 중인 구성을 시작 구성에 저장합니다.

write standby

ASA 또는 상황 실행 중인 구성을 장애 조치 스탠바이 장치에 복사하려면 특권 EXEC 모드에서 **write standby** 명령을 사용합니다.

write standby

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

스탠바이 장치 또는 장애 조치 그룹의 구성이 활성 장치 또는 장애 조치 그룹의 구성과 동기화되지 않는 경우에만 이 명령을 사용해야 합니다. 이는 일반적으로 스탠바이 장치 또는 장애 조치 그룹에서 명령을 직접 입력한 경우에 발생합니다.

액티브/스탠바이 장애 조치의 경우 활성 장치에서 입력된 **write standby** 명령은 활성 장애 조치 장치의 실행 중인 구성을 스탠바이 장치의 실행 중인 구성에 기록합니다.

활성/활성 장애 조치의 경우 **write standby** 명령은 다음과 같이 동작합니다.

- 시스템 실행 공간에서 **write standby** 명령을 입력한 경우 ASA의 모든 단일 컨텍스트에 대한 구성 및 시스템 구성이 피어 장치에 기록됩니다. 여기에는 대기 상태에 있는 보안 컨텍스트에 대한 구성 정보가 포함됩니다. 장애 조치 그룹 1이 활성 상태에 있는 장치에서는 시스템 실행 공간에서 명령을 입력해야 합니다.
- 보안 컨텍스트에서 **write standby** 명령에 입력하면 보안 컨텍스트에 대한 구성만 피어 장치에 기록됩니다. 보안 컨텍스트가 활성 상태로 표시되는 장치에서는 보안 컨텍스트에서 명령을 입력해야 합니다.

write standby 명령은 피어 장치의 실행 중인 구성에 구성을 복제합니다. 구성을 시작 구성에 저장하지 않습니다. 구성 변경을 시작 구성에 저장하려면 **write standby** 명령을 입력한 동일한 장치에서 **copy running-config startup-config** 명령을 사용합니다. 이 명령은 피어 장치에 복제되고 구성은 시작 구성에 저장됩니다.

상태 저장 장애 조치가 활성화된 경우 **write standby** 명령은 구성 복제가 완료된 후 상태 정보를 스탠바이 장치에 복제합니다. 다중 컨텍스트 모드에서는 상태 정보를 복제할 상황 내에서 **write standby**를 입력합니다.

참고 **write standby** 명령을 입력한 후 구성이 다시 동기화되는 동안 장애 조치 인터페이스가 일시적으로 중지됩니다. 이로 인해 장애 조치 상태 인터페이스의 일시적 오류가 탐지될 수도 있습니다.

예

다음 예에서는 현재 실행 중인 구성을 스탠바이 장치에 기록합니다.

```
ciscoasa# write standby
Building configuration...
[OK]
ciscoasa#
```

관련 명령

Command(명령)	설명
failover reload-standby	스탠바이 장치를 강제로 재부팅합니다.

write terminal

터미널에서 실행 중인 구성을 표시하려면 특권 EXEC 모드에서 **write terminal** 명령을 사용합니다.

write terminal

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	• 예	• 예

명령 기록

Release	수정 사항
7.0(1)	이 명령이 추가되었습니다.

사용 지침

이 명령은 **show running-config** 명령과 같습니다.

예

다음 예에서는 실행 중인 컨피그레이션을 터미널에 기록합니다.

```
ciscoasa# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

관련 명령

Command(명령)	설명
configure net	지정된 TFTP URL의 컨피그레이션 파일을 실행 중인 컨피그레이션과과 병합합니다.
show running-config	실행 중인 구성을 표시합니다.
write memory	실행 중인 구성을 시작 구성에 저장합니다.

xlate block-allocation

캐리어 등급 또는 대규모 PAT에 대한 포트 블록 할당 속성을 구성하려면 전역 구성 모드에서 **xlate block-allocation** 명령을 사용합니다. 기본값으로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

xlate block-allocation {**size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds*}

no xlate block-allocation {**size** *value* | **maximum-per-host** *number* | **pba-interim-logging** *seconds*}

구문 설명

size *value*	각 블록의 포트 수인 블록 할당 크기입니다. 범위는 32~4096입니다. 기본값은 512입니다. 기본값을 사용하지 않는 경우 선택한 크기가 64,512(1024-65535 범위의 포트 수)로 균등하게 나뉘어 있는지 확인합니다. 기본값을 사용하는 경우 할당할 수 없는 포트가 있습니다. 예를 들어 100을 지정하는 경우 사용되지 않는 포트가 12개 있습니다.
maximum-per-host *number*	호스트 당 할당할 수 있는 최대 블록 수입니다. 제한은 프로토콜에 따라 다르기 때문에 4개의 제한은 호스트당 최대 4개의 UDP 블록, 4개의 TCP 블록 및 4개의 ICMP 블록을 의미합니다. 범위는 1-8이며, 기본값은 4입니다.
pba-interim-logging *seconds*	중간 기록을 활성화합니다. 기본적으로 시스템이 포트 블록 생성 및 삭제를 수행하는 동안 syslog 메시지를 생성합니다. 중간 로깅을 활성화하면 지정하는 간격으로 시스템에서 메시지 305017을 생성합니다. 메시지에서는 프로토콜(ICMP, TCP, UDP), 소스 및 대상 인터페이스, IP 주소, 포트 블록 등 당시 할당된 모든 활성 포트 블록을 보고합니다. 21600-604800초(6시간~7일) 사이의 간격을 지정할 수 있습니다.

명령 기본값

기본 할당 크기는 512입니다. 기본 호스트당 최대값은 4입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	수정 사항
9.5(1)	이 명령이 추가되었습니다.
9.12(1)	**pba-interim-logging** 명령이 추가되었습니다.

사용 지침

통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 포트 블록을 할당하는 경우 호스트의 후속 연결은 블록 내에서 무작위로 선택된 새 포트를 사용합니다. 호스트에 원래 블록의 모든 포트에 대한 활성 연결이 설정되어 있으면 필요에 따라 추가 블록이 할당됩니다. 블록에서 포트를 사용하는 마지막 xlate가 제거되면 블록이 해제됩니다.

포트 블록은 1024~65535 범위에서만 할당됩니다. 따라서 애플리케이션에 낮은 포트 번호(1~1023)가 필요한 경우 작동하지 않을 수 있습니다. 예를 들어 포트 22(SSH)를 요청하는 애플리케이션은 1024~65535 범위 내에서 호스트에 할당된 블록 내에서 매핑된 포트를 가져옵니다.

xlate block-allocation 명령은 이러한 포트 블록의 특성을 구성합니다. PAT 풀 사용 시 PAT 규칙당 포트 블록 할당을 활성화하려면 **nat** 명령의 block-allocation 키워드를 사용합니다.

예

다음 예에서는 포트 블록 할당 특성을 변경하고 개체 NAT 규칙의 PAT 풀에 대한 포트 블록 할당을 구현합니다.

```
xlate block-allocation size 128
xlate block-allocation maximum-per-host 6
xlate block-allocation pba-interim-logging 21600

object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
object network src_host
  host 10.111.10.15
object network src_host
  nat dynamic pat-pool mapped-pat-pool block-allocation
```

관련 명령

Command(명령)	설명
nat (global)	두 배 NAT 규칙을 추가합니다.
nat (object)	개체 NAT 규칙을 추가합니다.
show local-host	호스트에 할당된 포트 블록을 표시합니다.
show running-config xlate	**xlate** 구성을 표시합니다.

xlate per-session

다중 세션 PAT를 사용하려면 전역 구성 모드에서 **xlate per-session** 명령을 사용합니다. 다중 세션 PAT 규칙을 제거하려면 이 명령의 **no** 형식을 사용합니다.

xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port*

no xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port*

구문 설명

deny	거부 규칙을 만듭니다.
destination_ip	대상 IP 주소에 대해 다음을 구성할 수 있습니다. • **host** *ip_address* - IPv4 호스트 주소를 지정합니다. • *ip_address mask* - IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다. • *ipv6-address*|*prefix-length* - IPv6 호스트 또는 네트워크 주소 및 접두사를 지정합니다. • **any4** 및 **any6** - **any4**는 IPv4 트래픽만 지정하고, **any6**은 any6 트래픽을 지정합니다.
operator dest_port	*operator*는 대상에서 사용하는 포트 번호와 일치합니다. 허용되는 연산자는 다음과 같습니다. • lt — 다음보다 작음 • gt — 다음보다 큼 • eq — 다음과 같음 • neq - 같지 않음 • range - 경계를 포함하는 값 범위. 이 연산자를 사용할 경우 다음과 같이 두 개의 포트 번호를 지정합니다. `range 100 200`
operator ***src_port***	(선택 사항) *operator*는 소스에서 사용하는 포트 번호와 일치합니다. 허용되는 연산자는 다음과 같습니다. • lt — 다음보다 작음 • gt — 다음보다 큼 • eq — 다음과 같음 • neq - 같지 않음 • range - 경계를 포함하는 값 범위. 이 연산자를 사용할 경우 다음과 같이 두 개의 포트 번호를 지정합니다. `range 100 200`
permit	허용 규칙을 만듭니다.

source_ip	소스 IP 주소에 대해 다음을 구성할 수 있습니다. • **host** *ip_address* - IPv4 호스트 주소를 지정합니다. • *ip_address mask* - IPv4 네트워크 주소 및 서브넷 마스크를 지정합니다. • *ipv6-address*|*prefix-length* - IPv6 호스트 또는 네트워크 주소 및 접두사를 지정합니다. • **any4** 및 **any6** - **any4**는 IPv4 트래픽만 지정하고, **any6**은 any6 트래픽을 지정합니다.
tcp	TCP 트래픽을 지정합니다.
udp	UDP 트래픽을 지정합니다.

명령 기본값

기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽에서는 세션당 PAT xlate를 사용합니다. 다음 기본 규칙이 설치됩니다.

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

참고 이러한 규칙은 제거할 수 없으며, 항상 수동으로 만든 모든 규칙 뒤에 존재합니다. 규칙은 순서대로 평가되므로 기본 규칙을 재정의할 수 있습니다. 예를 들어 이러한 규칙을 완전히 무시하려면 다음 거부 규칙을 추가하면 됩니다.

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		**보안 상황**		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	• 예	• 예	• 예	—

명령 기록

Release	**수정 사항**
9.0(1)	이 명령이 추가되었습니다.

사용 지침

세션당 PAT 기능은 PAT의 확장성을 개선하며, 클러스터링의 경우 각 구성원 장치가 PAT 연결을 소유할 수 있도록 합니다. 다중 세션 PAT 연결은 마스터 장치에서 전달하고 소유해야 합니다. 세션당 PAT 세션이 끝나면 ASA에서 재설정을 전송하고 xlate를 즉시 제거합니다. 이 재설정으로 인해 종단 노드의 연결이 즉시 해제되므로 TIME_WAIT 상태가 방지됩니다. 반면, 다중 세션 PAT에서는 PAT 시간 제한(기본적으로 30초)을 사용합니다. HTTP 또는 HTTPS와 같은 "hit-and-run" 트래픽의 경우 세션당 기능은 하나의 주소에서 지원하는 연결 속도를 크게 증가시킬 수 있습니다. 세션당 기능을 사용하지 않을 경우 IP 프로토콜의 단일 주소에 대한 최대 연결 속도는 약 2000/초입니다. 세션당 기능을 사용할 경우 IP 프로토콜의 단일 주소에 대한 연결 속도는 65535/*평균 수명*입니다.

기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽에서는 세션당 PAT xlate를 사용합니다. H.323, SIP 또는 Skinny와 같이 다중 세션 PAT가 유용할 수 있는 트래픽의 경우 세션별 PAT를 비활성화하여 세션별 거부 규칙을 생성할 수 있습니다.

세션별 PAT 규칙을 추가한 경우 이 규칙은 기본 규칙 위에서 수동으로 만든 다른 모든 규칙 아래에 배치됩니다. 적용할 순서대로 규칙을 만들어야 합니다.

예

다음 예에서는 다중 세션 PAT를 사용하도록 H.323 트래픽에 대한 거부 규칙을 만듭니다.

```
ciscoasa(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
ciscoasa(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

관련 명령

Command(명령)	설명
clear configure xlate	**xlate per-session** 규칙을 지웁니다.
nat (global)	두 배 NAT 규칙을 추가합니다.
nat (object)	개체 NAT 규칙을 추가합니다.
show running-config xlate	**xlate per-session** 규칙을 표시합니다.

zone

트래픽 영역을 추가하려면 전역 구성 모드에서 **zone** 명령을 사용합니다. 영역을 제거하려면 이 명령의 **no** 형식을 사용합니다.

zone *name*

no zone *name*

구문 설명

name	최대 48자의 영역 이름을 설정합니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	• 예	—

명령 기록

Release	수정 사항
9.3(2)	이 명령이 추가되었습니다.

사용 지침

기존 플로우의 트래픽이 영역 내 모든 인터페이스에서 ASA로 들어가거나 나갈 수 있도록 *트래픽 영역*에 여러 인터페이스를 할당할 수 있습니다. 이 기능을 사용하여 ASA에서 ECMP(Equal-Cost Multi-Path) 라우팅이 허용되며, ASA로의 트래픽에 대한 외부 로드 밸런싱을 여러 인터페이스에 분산시킬 수 있습니다.

영역은 해당 영역 내 인터페이스에서 트래픽이 들어오고 나갈 수 있도록 하지만 보안 정책 자체(액세스 규칙, NAT 등)는 영역별이 아니라 여전히 인터페이스별로 적용됩니다. 영역 내의 모든 인터페이스에 대해 동일한 보안 정책을 구성한 경우 해당 트래픽에 대한 ECMP 및 로드 밸런싱을 성공적으로 구현할 수 있습니다.

최대 256개의 영역을 만들 수 있습니다.

예

다음 예에서는 4개의 멤버 인터페이스가 있는 외부 영역을 구성합니다.

```
zone outside
interface gigabitethernet0/0
 zone-member outside
interface gigabitethernet0/1
 zone-member outside
interface gigabitethernet0/2
 zone-member outside
interface gigabitethernet0/3
 zone-member outside
```

관련 명령

Command(명령)	설명
clear configure zone	영역 구성을 지웁니다.
clear conn zone	영역 연결을 지웁니다.
clear local-host zone	영역 호스트를 지웁니다.
show asp table routing	디버깅을 위해 가속화된 보안 경로 테이블을 표시하며 각 경로와 연계된 영역을 표시합니다.
show asp table zone	디버깅을 위해 가속화된 보안 경로 테이블을 표시합니다.
show conn long	영역에 대한 연결 정보를 표시합니다.
show local-host zone	영역 내 로컬 호스트의 네트워크 상태를 표시합니다.
show nameif zone	인터페이스 이름 및 영역 이름을 표시합니다.
show route zone	영역 인터페이스에 대한 경로를 표시합니다.
show running-config zone	영역 구성을 표시합니다.
show zone	영역 ID, 컨텍스트, 보안 레벨, 멤버를 표시합니다.
zone-member	트래픽 영역에 인터페이스를 할당합니다.

zonelabs-integrity fail-close

ASA와 Zone Labs Integrity Firewall Server 간의 연결에 실패한 경우 VPN 클라이언트 연결이 닫히도록 ASA를 구성하려면 전역 구성 모드에서 **zonelabs-integrity fail-close** 명령을 사용합니다. Zone Labs 연결 실패 시 VPN 연결이 열린 상태로 유지되는 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

구문 설명설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 연결은 실패 시 열린 상태로 유지됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

기본 Zone Labs Integrity Firewall Server가 ASA에 응답하지 않는 경우 ASA는 기본적으로 사설 네트워크에 대한 VPN 클라이언트 연결을 설정합니다. 또한 기존 연결을 열린 상태로 유지합니다. 이는 방화벽 서버 실패로 인해 엔터프라이즈 VPN이 중단되지 않도록 합니다. 그러나 Zone Labs Integrity Firewall Server 실패 시 VPN 연결을 작동 상태로 유지하지 않으려면 **zonelabs-integrity fail-close** 명령을 사용합니다.

Zone Labs Integrity Firewall Server에 대한 연결이 실패한 경우 ASA에서 클라이언트 VPN 연결을 유지하는 기본 조건으로 돌아가려면 **zonelabs-integrity fail-open** 명령을 사용합니다.

예

다음 예에서는 Zone Labs Integrity Firewall Server가 응답하지 않거나 연결이 중단된 경우 VPN 클라이언트 연결을 닫도록 ASA를 구성합니다.

```
ciscoasa(config)# zonelabs-integrity fail-close
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity fail-open	ASA와 Zone Labs Integrity Firewall Server 간의 연결에 실패한 후에도 ASA에 대한 VPN 클라이언트 연결이 열린 상태로 유지되도록 지정합니다.
zonelabs-integrity fail-timeout	ASA가 응답하지 않는 Zone Labs Integrity Firewall Server를 연결할 수 없는 것으로 선언하기 전까지의 경과 시간(초)을 지정합니다.
zonelabs-integrity server-address	ASA 구성에 Zone Labs Integrity Firewall Server를 추가합니다.

zonelabs-integrity fail-open

ASA와 Zone Labs Integrity Firewall Server 간의 연결에 실패한 후에도 ASA에 대한 원격 VPN 클라이언트 연결을 열린 상태로 유지하려면 전역 구성 모드에서 **zonelabs-integrity fail-open** 명령을 사용합니다. Zone Labs 서버 연결 실패 시 VPN 클라이언트에 대한 연결을 닫으려면 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 원격 VPN 연결은 ASA가 Zone Labs Integrity Firewall Server에 대한 연결을 설정하거나 유지하지 않는 경우 열린 상태로 유지됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

기본 Zone Labs Integrity Firewall Server가 ASA에 응답하지 않는 경우 ASA는 기본적으로 사설 네트워크에 대한 VPN 클라이언트 연결을 설정합니다. 또한 기존 연결을 열린 상태로 유지합니다. 이는 방화벽 서버 실패로 인해 엔터프라이즈 VPN이 중단되지 않도록 합니다. 그러나 Zone Labs Integrity Firewall Server 실패 시 VPN 연결을 작동 상태로 유지하지 않으려면 **zonelabs-integrity fail-close** 명령을 사용합니다. 그런 다음 Zone Labs Integrity Firewall Server 연결에 실패한 경우 ASA에서 클라이언트 VPN 연결을 유지하는 기본 조건으로 되돌리려면 **zonelabs-integrity fail-open** 명령 또는 **no zonelabs-integrity fail-open** 명령을 사용합니다.

예

다음 예에서는 Zone Labs Integrity Firewall Server 연결에 실패한 경우 VPN 클라이언트 연결이 열린 상태로 유지되는 기본 조건으로 복원합니다.

```
ciscoasa(config)# zonelabs-integrity fail-open
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity fail-close	ASA와 Zone Labs Integrity Firewall Server 간의 연결에 실패한 경우 ASA에서 VPN 클라이언트 연결을 닫도록 지정합니다.
zonelabs-integrity fail-timeout	ASA가 응답하지 않는 Zone Labs Integrity Firewall Server를 연결할 수 없는 것으로 선언하기 전까지의 경과 시간(초)을 지정합니다.

zonelabs-integrity fail-timeout

ASA가 응답하지 않는 Zone Labs Integrity Firewall Server를 연결할 수 없는 것으로 선언하기 전까지의 경과 시간(초)을 지정하려면 전역 구성 모드에서 **zonelabs-integrity fail-timeout** 명령을 사용합니다. 기본 시간 제한 10초를 복원하려면 인수 없이 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

구문 설명

timeout	ASA가 응답하지 않는 Zone Labs Integrity Firewall Server를 연결할 수 없는 것으로 선언하기 전까지의 경과 시간(초)입니다. 허용되는 범위는 5~20초입니다.

기본값

기본 시간 제한 값은 10초입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ASA가 지정된 시간(초) 동안 Zone Labs 서버의 응답 없이 대기한 경우 이 서버는 응답하지 않는 것으로 선언됩니다. VPN 클라이언트 연결은 기본적으로 또는 **zonelabs-integrity fail-open** 명령을 사용하여 구성된 경우 열린 상태로 유지됩니다. 그러나 **zonelabs-integrity fail-close** 명령이 실행된 경우 ASA에서 무결성 서버를 응답하지 않는 것으로 선언하면 연결이 닫힙니다.

예

다음 예에서는 12초 후 활성 Zone Labs Intergrity Server를 연결할 수 없는 것으로 선언하도록 ASA를 구성합니다.

```
ciscoasa(config)# zonelabs-integrity fail-timeout 12
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity fail-open	ASA와 Zone Labs Integrity Firewall Server 간의 연결에 실패한 후에도 ASA에 대한 VPN 클라이언트 연결이 열린 상태로 유지되도록 지정합니다.
zonelabs-integrity fail-close	ASA와 Zone Labs Integrity Firewall Server 간의 연결에 실패한 경우 ASA에서 VPN 클라이언트 연결을 닫도록 지정합니다.
zonelabs-integrity server-address	ASA 컨피그레이션에 Zone Labs Integrity Firewall Server를 추가합니다.

zonelabs-integrity interface

Zone Labs Integrity Server와 통신할 ASA 인터페이스를 지정하려면 전역 구성 모드에서 **zonelabs-integrity interface** 명령을 사용합니다. Zone Labs Integrity Firewall Server 인터페이스를 기본값인 none으로 재설정하려면 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

구문 설명

interface	Zone Labs Integrity Firewall Server가 통신하는 ASA 인터페이스를 지정합니다. 이는 **nameif** 명령으로 만든 인터페이스 이름인 경우가 많습니다.

기본값

기본적으로 Zone Labs Integrity Firewall Server 인터페이스는 none으로 설정됩니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

예

다음 예에서는 IP 주소 범위 10.0.0.5~10.0.0.7을 사용하여 세 개의 Zone Labs Intergrity Server를 구성합니다. 또한 포트 300 및 inside라는 인터페이스에서 서버를 수신 대기하도록 ASA를 구성합니다.

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)# zonelabs-integrity interface inside
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity port	Zone Labs Integrity Firewall Server와 통신할 ASA의 포트를 지정합니다.
zonelabs-integrity server-address	ASA 컨피그레이션에 Zone Labs Integrity Firewall Server를 추가합니다.
zonelabs-integrity ssl-certificate-port	SSL 인증서를 검색할 때 Zone Labs Integrity Firewall Server에서 연결할 ASA 포트를 지정합니다.
zonelabs-integrity ssl-client-authentication	ASA에 의한 Zone Labs Integrity Firewall Server SSL 인증서 인증을 활성화합니다.

zonelabs-integrity port

Zone Labs Integrity Firewall Server와 통신할 ASA의 포트를 지정하려면 전역 구성 모드에서 **zonelabs-integrity port** 명령을 사용합니다. Zone Labs Integrity Firewall Server의 기본 포트인 5054로 되돌리려면 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

구문 설명

port	ASA에서 Zone Labs Integrity Firewall Server 포트를 지정합니다.
port_number	Zone Labs Integrity Firewall Server 포트 번호입니다. 10에서 10000 사이일 수 있습니다.

기본값

기본 Zone Labs Integrity Firewall Server 포트는 5054입니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ASA는 각각 **zonelabs-integrity port** 및 **zonelabs-integrity interface** 명령으로 구성된 포트 및 인터페이스에서 Zone Labs Integrity Firewall Server를 수신 대기합니다.

참고 사용자 인터페이스에서 최대 5개의 Integrity 서버 구성을 지원하지만 ASA의 현재 릴리스는 한 번에 하나의 Integrity 서버를 지원합니다. 활성 서버가 실패한 경우 ASA에서 다른 Integrity 서버를 구성한 다음 클라이언트 VPN 세션을 다시 설정합니다.

예

다음 예에서는 IP 주소 10.0.0.5를 사용하여 Zone Labs Integrity Server를 구성합니다. 또한 기본 5054 포트 대신 포트 300에서 활성 Zone Labs 서버를 수신 대기하도록 ASA를 구성합니다.

```
ciscoasa(config)# zonelabs-integrity server-address 10.0.0.5
ciscoasa(config)# zonelabs-integrity port 300
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity interface	활성 Zone Labs Integrity Server와 통신하는 ASA 인터페이스를 지정합니다.
zonelabs-integrity server-address	ASA 컨피그레이션에 Zone Labs Integrity Firewall Server를 추가합니다.
zonelabs-integrity ssl-certificate-port	SSL 인증서를 검색할 때 Zone Labs Integrity Firewall Server에서 연결할 ASA 포트를 지정합니다.
zonelabs-integrity ssl-client-authentication	ASA에 의한 Zone Labs Integrity Firewall Server SSL 인증서 인증을 활성화합니다.

zonelabs-integrity server-address

ASA 구성에 Zone Labs Integrity Firewall Server를 추가하려면 전역 구성 모드에서 **zonelabs-integrity server-address** 명령을 사용합니다. IP 주소 또는 호스트 이름으로 Zone Labs 서버를 지정합니다.

실행 중인 구성에서 Zone Labs Integrity Firewall Server를 제거하려면 인수 없이 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

참고 사용자 인터페이스에서는 여러 무결성 서버 구성을 지원하지만 현재 릴리스의 ASA는 한 번에 하나의 무결성 서버만 지원합니다.

구문 설명

hostname	Zone Labs Integrity Firewall Server의 호스트 이름을 지정합니다. 호스트 이름 지침은 **name** 명령을 참고하십시오.
ip-address	Zone Labs Integrity Firewall Server의 IP 주소를 지정합니다.

명령 기본값

기본적으로 Zone Labs Integrity Firewall Server는 구성되지 않습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

이 릴리스에서는 하나의 Zone Labs Integrity Firewall Server를 구성할 수 있습니다. 이 서버가 실패한 경우 먼저 다른 무결성 서버를 구성한 다음 클라이언트 VPN 세션을 설정합니다.

호스트 이름으로 서버를 지정하려면 먼저 **name** 명령을 사용하여 Zone Labs 서버 이름을 구성해야 합니다. **name** 명령을 사용하기 전에 **names** 명령을 사용하여 활성화합니다.

참고 사용자 인터페이스에서 최대 5개의 Integrity 서버 구성을 지원하지만 보안 어플라이언스의 현재 릴리스는 한 번에 하나의 Integrity 서버를 지원합니다. 활성 서버가 실패한 경우 ASA에서 다른 Integrity 서버를 구성한 다음 클라이언트 VPN 세션을 다시 설정합니다.

예

다음 예에서는 IP 주소 10.0.0.5에 서버 이름 ZL-Integrity-Svr을 할당하고 해당 이름을 사용하여 Zone Labs Intergrity Server를 구성합니다.

```
ciscoasa(config)# names
ciscoasa(config)# name 10.0.0.5 ZL-Integrity-Svr
ciscoasa(config)# zonelabs-integrity server-address ZL-Integrity-Svr
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity fail-close	ASA와 Zone Labs Integrity Firewall Server 간의 연결에 실패한 경우 ASA에서 VPN 클라이언트 연결을 닫도록 지정합니다.
zonelabs-integrity interface	활성 Zone Labs Integrity Server와 통신하는 ASA 인터페이스를 지정합니다.
zonelabs-integrity port	Zone Labs Integrity Firewall Server와 통신할 ASA의 포트를 지정합니다.
zonelabs-integrity ssl-certificate-port	SSL 인증서를 검색할 때 Zone Labs Integrity Firewall Server에서 연결할 ASA 포트를 지정합니다.
zonelabs-integrity ssl-client-authentication	ASA에 의한 Zone Labs Integrity Firewall Server SSL 인증서 인증을 활성화합니다.

zonelabs-integrity ssl-certificate-port

SSL 인증서를 검색할 때 Zone Labs Integrity Firewall Server에서 연결할 ASA 포트를 지정하려면 전역 구성 모드에서 **zonelabs-integrity ssl-certificate-port** 명령을 사용합니다. 기본 포트 번호(80)로 되돌리려면 인수 없이 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

구문 설명

cert-port-number	SSL 인증서를 요청할 때 Zone Labs Integrity Firewall Server에서 연결해야 하는 ASA의 포트 번호를 지정합니다.

기본값

기본적으로 ASA에서는 Zone Labs Integrity Firewall Server가 포트 80에서 SSL 인증서를 요청해야 합니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ASA와 Zone Labs Integrity Firewall Server 간의 SSL 통신에서 ASA는 SSL 서버이고 Zone Labs 서버는 SSL 클라이언트입니다. SSL 연결을 시작할 때 클라이언트(Zone Labs 서버)에서 SSL 서버(ASA)의 인증서를 인증해야 합니다. **zonelabs-integrity ssl-certificate-port** 명령은 SSL 서버 인증서를 요청할 때 Zone Labs 서버에서 연결할 포트를 지정합니다.

예

다음 예에서는 Zone Labs Integrity Server의 SSL 인증서 요청을 받도록 ASA의 포트 30을 구성합니다.

```
ciscoasa(config)# zonelabs-integrity ssl-certificate-port 30
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity port	Zone Labs Integrity Firewall Server와 통신할 ASA의 포트를 지정합니다.
zonelabs-integrity interface	활성 Zone Labs Integrity Server와 통신하는 ASA 인터페이스를 지정합니다.
zonelabs-integrity server-address	ASA 컨피그레이션에 Zone Labs Integrity Firewall Server를 추가합니다.
zonelabs-integrity ssl-client-authentication	ASA에 의한 Zone Labs Integrity Firewall Server SSL 인증서 인증을 활성화합니다.

zonelabs-integrity ssl-client-authentication

ASA에 의한 Zone Labs Integrity Firewall Server SSL 인증서 인증을 활성화하려면 *enable* 인수와 함께 전역 구성 모드에서 **zonelabs-integrity ssl-client-authentication** 명령을 사용합니다. Zone Labs SSL 인증서 인증을 비활성화하려면 *disable* 인수를 사용하거나 인수 없이 이 명령의 **no** 형식을 사용합니다.

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

구문 설명

disable	Zone Labs Integrity Firewall Server의 IP 주소를 지정합니다.
enable	ASA가 Zone Labs Integrity Firewall Server의 SSL 인증서를 인증하도록 지정합니다.

기본값

기본적으로 ASA의 Zone Labs Integrity Firewall Server SSL 인증서 인증은 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• 예	—	• 예	—	—

명령 기록

Release	수정 사항
7.2(1)	이 명령이 추가되었습니다.

사용 지침

ASA와 Zone Labs Integrity Firewall Server 간의 SSL 통신에서 ASA는 SSL 서버이고 Zone Labs 서버는 SSL 클라이언트입니다. SSL 연결을 시작할 때 클라이언트(Zone Labs 서버)에서 SSL 서버(ASA)의 인증서를 인증해야 합니다. 그러나 클라이언트 인증서 인증은 선택 사항입니다. **zonelabs-integrity ssl-client-authentication** 명령을 사용하여 ASA의 Zone Labs 서버(SSL 클라이언트) 인증서 인증을 활성화하거나 비활성화할 수 있습니다.

예

다음 예에서는 Zone Labs Integrity Server의 SSL 인증서를 인증하도록 ASA를 구성합니다.

```
ciscoasa(config)# zonelabs-integrity ssl-client-authentication enable
ciscoasa(config)#
```

관련 명령

Command(명령)	설명
zonelabs-integrity interface	활성 Zone Labs Integrity Server와 통신하는 ASA 인터페이스를 지정합니다.
zonelabs-integrity port	Zone Labs Integrity Firewall Server와 통신할 ASA의 포트를 지정합니다.
zonelabs-integrity server-address	ASA 컨피그레이션에 Zone Labs Integrity Firewall Server를 추가합니다.
zonelabs-integrity ssl-certificate-port	SSL 인증서를 검색할 때 Zone Labs Integrity Firewall Server에서 연결할 ASA 포트를 지정합니다.

zone-member

트래픽 영역에 인터페이스를 추가하려면 인터페이스 구성 모드에서 **zone-member** 명령을 사용합니다. 인터페이스를 제거하려면 이 명령의 **no** 형식을 사용합니다.

zone-member *name*

no zone-member *name*

구문 설명

name	**zone** 명령으로 설정한 영역 이름을 식별합니다.

명령 기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
전역 구성	• **예**	—	• **예**	• **예**	—

명령 기록

Release	수정 사항
9.3(2)	이 명령이 추가되었습니다.

사용 지침

이름, IP 주소, 보안 레벨 등 모든 인터페이스 매개변수를 구성합니다. 영역에 추가한 첫 번째 인터페이스는 영역의 보안 레벨을 결정합니다. 모든 추가 인터페이스는 보안 레벨이 동일해야 합니다. 영역에서 인터페이스의 보안 레벨을 변경하려면 하나의 인터페이스를 제외하고 모든 인터페이스를 제거한 다음 보안 레벨을 변경하고 인터페이스를 다시 추가해야 합니다.

영역에 인터페이스를 할당하면 해당 인터페이스의 모든 연결이 삭제됩니다. 연결을 다시 설정해야 합니다.

영역에서 인터페이스를 제거하면 해당 인터페이스를 기본 인터페이스로 사용하는 모든 연결이 삭제됩니다. 연결을 다시 설정해야 합니다. 인터페이스가 현재 인터페이스인 경우 ASA는 연결을 기본 인터페이스로 다시 이동합니다. 또한 영역 경로 테이블이 새로 고쳐집니다.

영역에 다음 유형의 인터페이스를 추가할 수 있습니다.

- 물리적
- VLAN
- EtherChannel
- 이중화

다음 유형의 인터페이스는 추가할 수 없습니다.

- 관리 전용

- 관리 액세스
- 장애 조치 또는 상태 링크
- 클러스터 제어 링크
- EtherChannel 또는 이중 인터페이스의 멤버 인터페이스

인터페이스는 하나의 영역에만 속할 수 있습니다.

영역당 최대 8개의 인터페이스를 포함할 수 있습니다.

예

다음 예에서는 4개의 멤버 인터페이스가 있는 외부 영역을 구성합니다.

```
zone outside
interface gigabitethernet0/0
 zone-member outside
interface gigabitethernet0/1
 zone-member outside
interface gigabitethernet0/2
 zone-member outside
interface gigabitethernet0/3
 zone-member outside
```

관련 명령

Command(명령)	설명
clear configure zone	영역 컨피그레이션을 지웁니다.
clear conn zone	영역 연결을 지웁니다.
clear local-host zone	영역 호스트를 지웁니다.
show asp table routing	디버깅을 위해 가속화된 보안 경로 테이블을 표시하며 각 경로와 연계된 영역을 표시합니다.
show asp table zone	디버깅을 위해 가속화된 보안 경로 테이블을 표시합니다.
show conn long	영역에 대한 연결 정보를 표시합니다.
show local-host zone	영역 내 로컬 호스트의 네트워크 상태를 표시합니다.
show nameif zone	인터페이스 이름 및 영역 이름을 표시합니다.
show route zone	영역 인터페이스에 대한 경로를 표시합니다.
show running-config zone	영역 컨피그레이션을 표시합니다.
show zone	영역 ID, 컨텍스트, 보안 레벨, 멤버를 표시합니다.
zone	트래픽 영역을 구성합니다.

파 트 2

다음에 대한 Cisco IOS 명령 ASA Services Module

ASASM에 대한 Cisco IOS 명령

clear diagnostics loopback

온라인 진단 테스트 구성을 제거하려면 특권 EXEC 모드에서 **clear diagnostic loopback** 명령을 사용합니다.

clear diagnostics loopback

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

특권 실행

사용 지침

clear diagnostics loopback 명령은 온라인 진단 테스트 구성을 지웁니다.

예

다음은 **clear diagnostics loopback** 명령의 샘플 출력입니다.

```
ciscoasa# clear diagnostics loopback

Port    Test    Pkts-received  Failures
0       0       0              0
1       0       0              0
```

관련 명령

Command(명령)	설명
show diagnostics loopback	PC 루프백 테스트, 실행한 테스트 횟수, 받은 루프백 패킷 수 및 탐지된 실패 횟수와 관련된 정보를 표시합니다.

firewall autostate

자동 상태 메시징을 활성화하려면 전역 구성 모드에서 **firewall autostate** 명령을 사용합니다. 자동 상태를 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

firewall autostate

no firewall autostate

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 자동 상태는 비활성화되어 있습니다.

명령 모드

전역 구성

사용 지침

자동 상태 메시징은 ASA가 스위치 인터페이스의 장애 또는 가동 상태를 신속하게 탐지할 수 있도록 해줍니다. 수퍼바이저 엔진은 ASA VLAN과 연결된 물리적 인터페이스의 상태에 대한 자동 상태 메시지를 ASA로 보낼 수 있습니다. 예를 들어 VLAN과 연결된 모든 물리적 인터페이스가 중단된 경우 자동 상태 메시지는 ASA에 VLAN이 중단되었음을 알려 줍니다. 이 정보를 통해 ASA는 VLAN을 중단된 것으로 선언하여 일반적으로 링크 오류가 발생한 쪽을 확인하는 데 필요한 인터페이스 모니터링 테스트를 우회합니다. 자동 상태 메시징은 ASA가 링크 오류를 탐지하는 데 걸리는 시간을 대폭(최대 45초에서 몇 밀리초로) 단축합니다.

스위치 수퍼바이저는 다음과 같은 경우에 ASA로 자동 상태 메시지를 보냅니다.

- VLAN에 속한 마지막 인터페이스가 중단된 경우
- VLAN에 속한 첫 번째 인터페이스가 가동된 경우

예

다음 예에서는 자동 상태 메시징을 활성화합니다.

```
Router(config)# firewall autostate
```

관련 명령

Command(명령)	설명
show firewall autostate	자동 상태 기능의 설정을 표시합니다.

firewall module

ASA에 방화벽 그룹을 할당하려면 전역 구성 모드에서 **firewall module** 명령을 입력합니다. 그룹을 제거하려면 이 명령의 **no** 형식을 사용합니다.

firewall module *module_number* **vlan-group** *firewall_group*

no firewall module *module_number* **vlan-group** *firewall_group*

구문 설명

module_number	모듈 번호를 지정합니다. **show module** 명령을 사용하여 설치된 모듈과 해당 번호를 볼 수 있습니다.
vlan-group *firewall_group*	**firewall vlan-group** 명령으로 정의된 대로 하나 이상의 그룹 번호를 지정합니다. • 단일 번호(*n*) • 범위(*n-x*) 번호 또는 범위를 쉼표로 구분합니다. 예를 들어 다음 번호를 입력합니다. `5,7-10`

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

전역 구성

사용 지침

- 각 ASASM에 최대 16개의 방화벽 VLAN 그룹을 할당할 수 있습니다. (Cisco IOS 소프트웨어에서는 VLAN 그룹을 16개 넘게 생성할 수 있지만, ASASM당 16개만 할당할 수 있습니다.) 그룹을 생성하려면 **firewall vlan-group** 명령을 참고하십시오. 예를 들어 모든 VLAN을 하나의 그룹에 할당하거나, 내부 그룹과 외부 그룹을 생성하거나, 각 고객에 대한 그룹을 생성할 수 있습니다.
- 그룹당 VLAN 수에는 제한이 없지만 ASASM에서는 ASASM 시스템 제한 이내의 VLAN만 사용할 수 있습니다(자세한 내용은 ASASM 라이센싱 설명서 참고).
- 여러 방화벽 그룹에 동일한 VLAN을 할당할 수 없습니다.
- 단일 방화벽 그룹을 여러 ASASM에 할당할 수 있습니다. 예를 들어 여러 ASASM에 할당하려는 VLAN은 각 ASASM에 고유한 VLAN과 별도의 그룹에 상주할 수 있습니다.
- 동일한 스위치 섀시 내에서 ASASM 장애 조치를 사용하는 경우 장애 조치 및 상태 저장 통신용으로 예약된 VLAN을 스위치 포트에 할당하지 마십시오. 그러나 섀시 간에 장애 조치를 사용하는 경우에는 섀시 간의 트렁크 포트에 VLAN을 포함해야 합니다.
- VLAN을 ASASM에 할당하기 전에 스위치에 추가하지 않은 경우에는 VLAN이 수퍼바이저 엔진 데이터베이스에 저장되며, 스위치에 추가되는 즉시 ASASM으로 전송됩니다.
- 스위치에 할당되기 전에 ASASM 구성에서 VLAN을 구성할 수 있습니다. 스위치가 ASASM으로 VLAN을 보내면 ASASM 구성에서 종료했는지 여부에 상관없이 기본적으로 ASASM에서 VLAN이 관리자에 의해 가동됩니다. 이 경우 다시 종료해야 합니다.

예

다음 예에서는 각 ASA에 대한 그룹과 두 ASA에 할당된 VLAN을 포함하는 그룹, 이렇게 3개의 방화벽 VLAN 그룹을 만드는 방법을 보여 줍니다.

```
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 모든 VLAN 그룹을 표시하는 **show firewall module** 명령의 샘플 출력입니다.

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

관련 명령

Command(명령)	설명
firewall vlan-group	VLAN 그룹에 VLAN을 할당합니다.
show firewall module vlan-group	VLAN 그룹 및 해당 그룹에 할당된 VLAN을 표시합니다.
show module	설치된 모든 모듈을 표시합니다.

firewall multiple-vlan-interfaces

둘 이상의 SVI를 ASA에 추가하도록 허용하려면 전역 구성 모드에서 **firewall multiple-vlan-interfaces** 명령을 사용합니다. 이 기능을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

firewall multiple-vlan-interfaces

no firewall multiple-vlan-interfaces

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 여러 SVI는 허용되지 않습니다.

명령 모드

전역 구성

사용 지침

MSFC에 정의된 VLAN을 스위치 가상 인터페이스라고 합니다. SVI에 사용된 VLAN을 ASA에 할당한 경우 MSFC는 ASA와 다른 Layer 3 VLAN 간에 라우팅됩니다. 보안상, 기본적으로 MSFC와 ASA 간에는 하나의 SVI만 존재할 수 있습니다. 예를 들어 여러 SVI로 시스템을 잘못 구성한 경우 내부 및 외부 VLAN을 MSFC에 할당하여 실수로 트래픽이 ASA를 통과하도록 허용할 수 있습니다.

그러나 일부 네트워크 시나리오에서는 ASA를 우회해야 할 수도 있습니다. 예를 들어 동일한 이더넷 세그먼트의 IPX 호스트를 IP 호스트로 사용하는 경우 여러 SVI가 필요합니다. 라우팅된 방화벽 모드의 ASA는 IP 트래픽만 처리하고 IPX와 같은 다른 프로토콜 트래픽은 삭제하기 때문에(투명 방화벽 모드에서는 선택적으로 비 IP 트래픽을 허용할 수 있음) IPX 트래픽에 대해 ASA를 우회할 수 있습니다. IPX 트래픽만 VLAN에서 전달되도록 허용하는 액세스 목록을 사용하여 MSFC를 구성해야 합니다.

다중 상황 모드의 투명 방화벽에서는 각 상황에서 해당 외부 인터페이스에 고유한 VLAN이 있어야 하므로 여러 SVI를 사용해야 합니다. 외부 인터페이스에 대해 단일 VLAN을 공유하지 않아도 되도록 라우팅 모드에서 여러 SVI를 사용하도록 선택할 수도 있습니다.

예

다음 예에서는 여러 SVI를 사용하는 일반적인 구성을 보여 줍니다.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

다음은 **show interface** 명령의 샘플 출력입니다.

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
```

```
Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
Internet address is 55.1.1.1/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type:ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:08, output hang never
Last clearing of "show interface" counters never
Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
Queueing strategy:fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
L3 out Switched:ucast:0 pkt, 0 bytes
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   4 packets output, 256 bytes, 0 underruns
   0 output errors, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹을 정의합니다.

firewall vlan-group

방화벽 그룹에 VLAN을 할당하려면 전역 구성 모드에서 **firewall vlan-group** 명령을 입력합니다. VLAN을 제거하려면 이 명령의 **no** 형식을 사용합니다.

firewall [**switch** {**1** |**2**}] **vlan-group** *firewall_group vlan_range*

no firewall [**switch** {**1** |**2**}] **vlan-group** *firewall_group vlan_range*

구문 설명

firewall_group	그룹 ID를 정수로 지정합니다.
vlan_range	그룹에 할당된 VLAN을 지정합니다. *vlan_range* 값은 다음 방법 중 하나로 식별되는 하나 이상의 VLAN(2~1000 및 1025~4094)일 수 있습니다. • 단일 번호(*n*) • 범위(*n-x*) 번호 또는 범위를 쉼표로 구분합니다. 예를 들어 다음 번호를 입력합니다. `5,7-10,13,45-100` **참고** 라우팅된 포트와 WAN 포트는 내부 VLAN을 사용하므로 1020~1100 범위의 VLAN이 이미 사용 중일 수 있습니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

전역 구성

사용 지침

- **firewall module** 명령을 사용하여 각 ASASM에 최대 16개의 방화벽 VLAN 그룹을 할당할 수 있습니다. (Cisco IOS 소프트웨어에서는 VLAN 그룹을 16개 넘게 생성할 수 있지만, ASASM당 16개만 할당할 수 있습니다.) 예를 들어 모든 VLAN을 하나의 그룹에 할당하거나, 내부 그룹과 외부 그룹을 생성하거나, 각 고객에 대한 그룹을 생성할 수 있습니다.
- 그룹당 VLAN 수에는 제한이 없지만 ASASM에서는 ASASM 시스템 제한 이내의 VLAN만 사용할 수 있습니다(자세한 내용은 ASASM 라이센싱 설명서 참고).
- 여러 방화벽 그룹에 동일한 VLAN을 할당할 수 없습니다.
- 단일 방화벽 그룹을 여러 ASASM에 할당할 수 있습니다. 예를 들어 여러 ASASM에 할당하려는 VLAN은 각 ASASM에 고유한 VLAN과 별도의 그룹에 상주할 수 있습니다.
- 2~1000 및 1025~4094의 VLAN ID를 사용합니다.
- 라우팅된 포트와 WAN 포트는 내부 VLAN을 사용하므로 1020~1100 범위의 VLAN이 이미 사용 중일 수 있습니다.
- 예약된 VLAN은 사용할 수 없습니다.
- VLAN 1은 사용할 수 없습니다.

- 동일한 스위치 섀시 내에서 ASASM 장애 조치를 사용하는 경우 장애 조치 및 상태 저장 통신용으로 예약된 VLAN을 스위치 포트에 할당하지 마십시오. 그러나 섀시 간에 장애 조치를 사용하는 경우에는 섀시 간의 트렁크 포트에 VLAN을 포함해야 합니다.
- VLAN을 ASASM에 할당하기 전에 스위치에 추가하지 않은 경우에는 VLAN이 수퍼바이저 엔진 데이터베이스에 저장되며, 스위치에 추가되는 즉시 ASASM으로 전송됩니다.
- 스위치에 할당되기 전에 ASASM 구성에서 VLAN을 구성할 수 있습니다. 스위치가 ASASM으로 VLAN을 보내면 ASASM 구성에서 종료했는지 여부에 상관없이 기본적으로 ASASM에서 VLAN이 관리자에 의해 가동됩니다. 이 경우 다시 종료해야 합니다.

예

다음 예에서는 각 ASA에 대한 그룹과 두 ASA에 할당된 VLAN을 포함하는 그룹, 이렇게 3개의 방화벽 VLAN 그룹을 만드는 방법을 보여 줍니다.

```
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 모든 VLAN 그룹을 표시하는 **show firewall module** 명령의 샘플 출력입니다.

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
show firewall vlan-group	VLAN 그룹 및 해당 그룹에 할당된 VLAN을 표시합니다.
show module	설치된 모든 모듈을 표시합니다.

service-module session

스위치 CLI에서 ASASM에 대한 콘솔 액세스 권한을 얻으려면 특권 EXEC 모드에서 **service-module session** 명령을 입력합니다.

service-module session [**switch** {**1** | **2**}] **slot** *number*

구문 설명

slot *number*	ASASM의 슬롯 번호를 지정합니다. 모듈 슬롯 번호를 보려면 스위치 프롬프트에서 **show module** 명령을 입력합니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

특권 실행

사용 지침

service-module session 명령을 사용하여 ASASM에 대한 가상 콘솔 연결을 생성하며, 여기에는 실제 콘솔 연결의 이점과 제한 사항이 모두 포함됩니다.

장점은 다음과 같습니다.

- 다시 로드하더라도 연결이 유지되며 시간 초과되지 않습니다.
- ASASM에서 다시 로드하는 동안 연결된 상태를 유지하고 시작 메시지를 볼 수 있습니다.
- ASASM에서 이미지를 로드할 수 없는 경우 ROMMON에 액세스할 수 있습니다.

제한 사항은 다음과 같습니다.

- 연결이 느립니다(9600보드).
- 한 번에 하나의 콘솔 연결만 활성 상태로 유지할 수 있습니다.

참고 ASASM에서 올바르게 로그아웃하지 않을 경우 연결 상태가 계속 유지되어 의도한 시간보다 오래 연결이 지속될 수 있습니다. 다른 사람이 로그인하려면 기존 연결을 끊어야 합니다. 자세한 내용은 CLI 구성 가이드를 참조하십시오.

예

다음 예에서는 슬롯 3에서 ASASM에 대한 콘솔 액세스 권한을 얻는 방법을 보여 줍니다.

```
Router# service-module session slot 3
ciscoasa>
```

관련 명령

명령	설명
session	백플레인을 통해 ASASM으로 텔넷합니다.

session

백플레인을 통해 스위치 CLI에서 ASASM으로 텔넷하려면 특권 EXEC 모드에서 **session** 명령을 사용합니다.

session [**switch** {**1** | **2**}] **slot** *number* **processor 1**

구문 설명

processor 1	프로세서 번호를 지정합니다(항상 1).
slot *number*	슬롯 번호를 지정합니다. 모듈 슬롯 번호를 보려면 스위치 프롬프트에서 **show module** 명령을 입력합니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

특권 실행

사용 지침

session 명령을 사용하면 ASASM에 대한 텔넷 연결을 만들 수 있습니다.

장점은 다음과 같습니다.

- ASASM에 대한 세션을 동시에 유지할 수 있습니다.
- 텔넷 세션은 빠른 연결입니다.

제한 사항은 다음과 같습니다.

- ASASM을 다시 로드하면 텔넷 세션이 종료되고 시간 초과될 수 있습니다.
- 완전히 로드할 때까지 ASASM에 액세스할 수 없습니다. ROMMON에 액세스할 수 없습니다.

참고 다른 서비스 모듈에서 지원되는 **session** *slot* **processor 0** 명령은 ASASM에서 지원되지 않습니다. ASASM에는 프로세서 0이 없습니다.

로그인 비밀번호를 묻는 메시지가 표시됩니다. ASASM에 로그인 비밀번호를 입력합니다. 기본적으로 비밀번호는 **cisco**입니다.

사용자 EXEC 모드에 액세스할 수 있습니다.

예

다음 예에서는 프로세서 1에서 ASASM으로 텔넷합니다.

```
Router# session slot number processor 1
ciscoasa passwd: cisco
ciscoasa>
```

관련 명령

Command(명령)	설명
service-module session	스위치 CLI에서 ASASM에 대한 콘솔 액세스 권한을 가져옵니다.

show boot device

기본 부트 파티션을 보려면 **show boot device** 명령을 사용합니다.

show boot device [*mod_num*]

구문 설명

mod_num	(선택 사항) 모듈 번호를 지정합니다. **show module** 명령을 사용하여 설치된 모듈과 해당 번호를 볼 수 있습니다.

기본값

기본 부트 파티션은 cf:4입니다.

명령 모드

특권 실행

예

다음은 Cisco IOS 소프트웨어의 설치된 각 ASA에 대한 부트 파티션을 표시하는 **show boot device** 명령의 샘플 출력입니다.

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

관련 명령

Command(명령)	설명
boot device (IOS)	기본 부트 파티션을 설정합니다.
show module (IOS)	설치된 모든 모듈을 표시합니다.

show diagnostic loopback

실행한 테스트 횟수, 받은 루프백 패킷 수, 탐지된 실패 횟수 등 PC 루프백 테스트와 관련된 정보를 표시하려면 특권 EXEC 모드에서 **show diagnostics loopback** 명령을 사용합니다.

show diagnostics loopback

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	•	•	•	—	•

명령 기록

Release	수정 사항
12.2 (18) SXF5	이 명령이 추가되었습니다.

사용 지침

show diagnostics loopback 명령은 실행한 테스트 횟수, 받은 루프백 패킷 수, 탐지된 실패 횟수 등 PC 루프백 테스트와 관련된 정보를 제공합니다.

예

다음은 **show diagnostics loopback** 명령의 샘플 출력입니다.

```
ciscoasa# show diagnostics loopback

Port    Test    Pkts-received  Failures
0       447     447            0
1       447     447            0
```

관련 명령

Command(명령)	설명
clear diagnostics loopback	온라인 진단 테스트 구성을 지웁니다.
firewall autostate	자동 상태 기능을 활성화합니다.

show firewall autostate

자동 상태 기능의 설정을 보려면 특권 EXEC 모드에서 **show firewall autostate** 명령을 사용합니다.

show firewall autostate

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본적으로 자동 상태는 비활성화되어 있습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	•	•	•	•	•

사용 지침

Cisco IOS 소프트웨어의 자동 상태 메시징은 ASA가 스위치 인터페이스의 장애 또는 가동 상태를 신속하게 탐지할 수 있도록 해줍니다. 스위치 수퍼바이저는 다음과 같은 경우에 ASA로 자동 상태 메시지를 보냅니다.

- VLAN에 속한 마지막 인터페이스가 중단된 경우
- VLAN에 속한 첫 번째 인터페이스가 가동된 경우

관련 명령

Command(명령)	설명
clear diagnostics loopback	온라인 진단 테스트 구성을 지웁니다.
firewall autostate	자동 상태 기능을 활성화합니다.

show firewall module

각 ASA에 할당된 VLAN 그룹을 보려면 특권 EXEC 모드에서 **show firewall module** 명령을 입력합니다.

show firewall [**switch** {**1** | **2**}] **module** [*module_number*]

구문 설명

module_number	(선택 사항) 모듈 번호를 지정합니다. **show module** 명령을 사용하여 설치된 모듈과 해당 번호를 볼 수 있습니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	•	•	•	•	•

예

다음은 모든 VLAN 그룹을 표시하는 **show firewall module** 명령의 샘플 출력입니다.

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹에 VLAN을 할당합니다.
show firewall module vlan-group	VLAN 그룹 및 해당 그룹에 할당된 VLAN을 표시합니다.
show module	설치된 모든 모듈을 표시합니다.

show firewall module state

각 ASA의 상태를 보려면 특권 EXEC 모드에서 **show firewall module state** 명령을 입력합니다.

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **state**

구문 설명

module_number	(선택 사항) 모듈 번호를 지정합니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	•	•	•	•	•

예

다음은 **show firewall module state** 명령의 샘플 출력입니다.

```
Router# show firewall module 11 state
Firewall module 11:

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹에 VLAN을 할당합니다.
show firewall module vlan-group	VLAN 그룹 및 해당 그룹에 할당된 VLAN을 표시합니다.
show module	설치된 모든 모듈을 표시합니다.

show firewall module traffic

각 ASA를 통한 트래픽 흐름을 보려면 특권 EXEC 모드에서 **show firewall module traffic** 명령을 입력합니다.

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **traffic**

구문 설명

module_number	(선택 사항) 모듈 번호를 지정합니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	•	•	•	•	•

예

다음은 **show firewall module traffic** 명령의 샘플 출력입니다.

```
Router# show firewall module 11 traffic
Firewall module 11:

Specified interface is up line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹에 VLAN을 할당합니다.
show firewall module vlan-group	VLAN 그룹 및 해당 그룹에 할당된 VLAN을 표시합니다.
show module	설치된 모든 모듈을 표시합니다.

show firewall module version

ASA Services Module의 소프트웨어 버전 번호를 확인하려면 특권 EXEC 모드에서 **show firewall module version** 명령을 입력합니다.

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **version**

구문 설명

module_number	(선택 사항) 모듈 번호를 지정합니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	• 예	• 예	• 예	• 예	• 예

예

다음은 **show firewall module version** 명령의 샘플 출력입니다.

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:

Sw Version: 100.7(8)19
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹을 생성합니다.
show module	설치된 모든 모듈을 표시합니다.

show firewall module vlan-group

ASA에 할당할 수 있는 VLAN 그룹을 보려면 특권 EXEC 모드에서 **show firewall module vlan-group** 명령을 입력합니다.

show firewall [**switch** {**1** | **2**}] **module** [*module_number*] **vlan-group** [*firewall_group*]

구문 설명

firewall_group	(선택 사항) 그룹 ID를 지정합니다.
module_number	(선택 사항) 모듈 번호를 지정합니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	•	•	•	•	•

예

다음은 **show firewall module vlan-group** 명령의 샘플 출력입니다.

```
Router# show firewall module vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹을 생성합니다.
show module	설치된 모든 모듈을 표시합니다.

show firewall multiple-vlan-interfaces

ASASM에 대한 여러 방화벽 VLAN 인터페이스의 상태를 보려면 특권 EXEC 모드에서 **show firewall multiple-vlan-interfaces** 명령을 입력합니다.

show firewall multiple-vlan-interfaces

구문 설명

이 명령에는 인수 또는 키워드가 없습니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	라우팅됨	투명	단일	상황	시스템
특권 실행	•	•	•	•	•

예

다음은 **show firewall multiple-vlan-interfaces** 명령의 샘플 출력입니다.

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA 에 할당합니다 .
firewall vlan-group	VLAN 그룹을 생성합니다 .
show module	설치된 모든 모듈을 표시합니다 .

show module

스위치에서 ASASM을 인식하고 온라인 상태로 전환했는지 확인하려면 특권 EXEC 모드에서 **show module** 명령을 사용합니다.

show module [**switch** {**1** | **2**}] [*mod-num* | **all**]

구문 설명

all	(선택 사항) 모든 모듈을 지정합니다.
mod_num	(선택 사항) 모듈 번호를 지정합니다.
switch {**1** | **2**}	(선택 사항) VSS 구성에 대해 스위치 번호를 지정합니다.

기본값

기본 동작 또는 기본값이 없습니다.

명령 모드

다음 표에는 명령을 입력할 수 있는 모드가 나와 있습니다.

	방화벽 모드		보안 상황		
				다중	
명령 모드	**라우팅됨**	**투명**	**단일**	**상황**	**시스템**
특권 실행	•	•	•	•	•

예

다음은 **show module** 명령의 샘플 출력입니다.

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
 2    3  ASA Service Module                       WS-SVC-ASA-SM1     SAD143502E8
 4    3  ASA Service Module                       WS-SVC-ASA-SM1     SAD135101Z9
 5    5  Supervisor Engine 720 10GE (Active)      VS-S720-10G        SAL12426KB1
 6   16  CEF720 16 port 10GE                      WS-X6716-10GE      SAL1442WZD1

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok

Mod  Sub-Module                  Model               Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok

Base PID:
Mod  Model            Serial No.
---- -----------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
```

```
 4 TRIFECTA           SAD135101Z9

Mod  Online Diag Status
---- -------------------
 2   Pass
2/0  Not Applicable
 4   Not Applicable
4/0  Not Applicable
 5   Pass
 6   Pass
```

관련 명령

Command(명령)	설명
firewall module	VLAN 그룹을 ASA에 할당합니다.
firewall vlan-group	VLAN 그룹을 생성합니다.

파 트 3

참조

명령줄 인터페이스 사용

이 장에서는 ASA에서 CLI를 사용하는 방법을 설명하며, 다음 섹션으로 구성되어 있습니다.

참고 CLI는 Cisco IOS CLI와 유사한 구문 및 규칙을 사용하지만 ASA 운영 체제는 Cisco IOS 소프트웨어 버전이 아닙니다. Cisco IOS CLI 명령이 ASA와 함께 작동하거나 동일한 기능을 갖추었다고 가정하지 마십시오.

방화벽 모드 및 보안 상황 모드

ASA는 다음 모드의 조합에서 실행됩니다.

- 투명 방화벽 또는 라우팅 방화벽 모드

  방화벽 모드는 ASA가 계층 2 방화벽으로 실행되는지 또는 계층 3 방화벽으로 실행되는지를 결정합니다.
- 다중 상황 또는 단일 상황 모드

보안 상황 모드에서는 ASA가 단일 디바이스 또는 가상 디바이스 역할을 하는 다중 보안 상황으로 실행되는지 결정합니다.

일부 명령은 특정 모드에서만 사용할 수 있습니다.

명령 모드 및 프롬프트

ASA CLI에는 명령 모드가 포함되어 있습니다. 일부 명령은 특정 모드에서만 입력할 수 있습니다. 예를 들어 민감한 정보를 표시하는 명령을 입력하려면 비밀번호를 입력하고 특권 모드로 전환해야 합니다. 그런 다음 구성 변경을 실수로 입력하는 일이 없도록 우선 구성 모드로 전환해야 합니다. 상위 모드에서는 모든 하위 명령을 입력할 수 있습니다. 예를 들어 전역 구성 모드에서 특권 EXEC 명령을 입력할 수 있습니다.

참고 여러 유형의 프롬프트는 모두 기본 프롬프트이며, 구성된 경우에는 다를 수 있습니다.

- 시스템 구성 또는 단일 상황 모드에서는 프롬프트가 호스트 이름으로 시작합니다.

  ```
  ciscoasa
  ```

- 프롬프트 문자열을 인쇄할 때는 프롬프트 구성이 구문 분석되고 구성 키워드 값이 **prompt** 명령을 설정한 순서대로 인쇄됩니다. 키워드 인수는 hostname, domain, context, priority, state 중 하나일 수 있습니다(열거 순서와 무관).

  ```
  asa(config)# prompt hostname context priority state
  ```

- 상황 내에 있을 경우, 프롬프트는 호스트 이름으로 시작하고 그 다음 상황 이름이 옵니다.

  ```
  ciscoasa/context
  ```

프롬프트는 액세스 모드에 따라 변경됩니다.

- 사용자 EXEC 모드

  사용자 EXEC 모드에서는 최소 ASA 설정을 볼 수 있습니다. 먼저 ASA에 액세스한 경우 사용자 EXEC 모드 프롬프트는 다음과 같이 표시됩니다.

  ```
  ciscoasa>

  ciscoasa/context>
  ```

- 특권 EXEC 모드

  특권 EXEC 모드에서는 특권 수준까지의 모든 현재 설정을 볼 수 있습니다. 모든 사용자 EXEC 명령이 특권 EXEC 모드에서 작동합니다. 사용자 EXEC 모드에서 **enable** 명령을 입력하면(비밀번호가 필요함) 특권 EXEC 모드가 시작됩니다. 프롬프트에는 번호 기호(#)가 포함되어 있습니다.

  ```
  ciscoasa#

  ciscoasa/context#
  ```

- 전역 구성 모드

  전역 구성 모드에서 ASA 구성을 변경할 수 있습니다. 모든 사용자 EXEC, 특권 EXEC 및 전역 구성 명령을 이 모드에서 사용할 수 있습니다. 특권 EXEC 모드에서 **configure terminal** 명령을 입력하면 전역 구성 모드가 시작됩니다. 프롬프트가 다음으로 변경됩니다.

  ```
  ciscoasa(config)#

  ciscoasa/context(config)#
  ```

- 명령별 구성 모드

  전역 구성 모드에서 일부 명령은 명령별 구성 모드를 시작합니다. 모든 사용자 EXEC, 특권 EXEC, 전역 구성 및 명령별 구성 명령을 이 모드에서 사용할 수 있습니다. 예를 들어 **interface** 명령은 인터페이스 구성 모드를 시작합니다. 프롬프트가 다음으로 변경됩니다.

  ```
  ciscoasa(config-if)#

  ciscoasa/context(config-if)#
  ```

구문 형식 지정

명령 구문 설명에서는 표 7-1에 나열된 규칙을 사용합니다.

표 7-1 구문 규칙

표기 규칙	설명
굵은 글꼴	굵은 텍스트는 표시된 대로 입력할 명령 및 키워드를 나타냅니다.
기울임꼴	기울임꼴 텍스트는 값을 제공할 인수를 나타냅니다.
[x]	선택적 요소(키워드 또는 인수)를 대괄호로 묶습니다.
|	세로 막대는 선택적 또는 필수 키워드 또는 인수 집합 내에서 선택할 수 있음을 나타냅니다.
[x | y]	대괄호 안의 세로 막대로 구분된 키워드 또는 인수는 선택사항을 나타냅니다.
{x | y}	중괄호 안의 세로 막대로 구분된 키워드 또는 인수는 필수 선택 항목을 나타냅니다.
[x {y | z}]	중첩된 대괄호 또는 중괄호 집합은 선택 요소 또는 필수 요소 내의 선택사항 또는 필수 선택 항목을 나타냅니다. 대괄호 안의 중괄호 및 세로 막대는 선택 요소 내의 필수 선택 항목을 나타냅니다.

명령 약어 지정

대부분의 명령을 최소한의 고유한 명령 문자로 축약할 수 있습니다. 예를 들어 **wr t** 를 전체 명령 **write terminal**을 입력하는 대신 입력하여 구성을 보거나, **en**을 입력하여 특권 모드를 시작하고 **conf t** 를 입력하여 구성 모드를 시작할 수 있습니다. 또한 **0**을 입력하여 **0.0.0.0**을 나타낼 수 있습니다.

명령줄 편집

ASA에서는 Cisco IOS 소프트웨어와 동일한 명령줄 편집 표기 규칙을 사용합니다. **show history** 명령을 사용하여 이전에 입력한 모든 명령을 보거나 위쪽 화살표 또는 **^p** 명령을 사용하여 개별적으로 볼 수 있습니다. 이전에 입력한 명령을 검토한 후에는 아래쪽 화살표 **^n** 명령을 사용하여 목록에서 앞으로 이동할 수 있습니다. 재사용할 명령에 도달하면 해당 명령을 편집하거나 **Enter** 키를 눌러 명령을 시작할 수 있습니다. 또한 **^w**를 사용하여 커서 왼쪽에 있는 단어를 삭제하거나 **^u**를 사용하여 행을 지울 수 있습니다.

ASA에서는 명령에 최대 512자를 입력할 수 있으며, 추가 문자는 무시됩니다.

명령 완성

부분 문자열을 입력한 후 명령 또는 키워드를 완성하려면 **Tab** 키를 누릅니다. ASA에서는 부분 문자열이 하나의 명령 또는 키워드와 일치하는 경우에만 명령 또는 키워드를 완성합니다. 예를 들어 **s**를 입력하고 **Tab** 키를 누른 경우 이는 둘 이상의 명령과 일치하므로 ASA에서 명령을 완성하지 않습니다. 그러나 **dis**를 입력하고 **Tab** 키를 누르면 **disable** 명령이 완성됩니다.

명령 도움말

다음 명령을 입력하여 커맨드 라인에서 도움말 정보를 사용할 수 있습니다.

- **help** *command_name*

  특정 명령에 대한 도움말을 표시합니다.

- *command_name* **?**

  사용 가능한 인수 목록을 표시합니다.

- *string***?** (공백 없음)

  이 문자열로 시작할 수 있는 명령을 나열합니다.

- **?** 및 **+?**

  사용 가능한 모든 명령을 나열합니다. **?**를 입력한 경우 ASA에서는 현재 모드에 사용 가능한 명령만 표시합니다. 하위 모드의 명령을 포함하여 사용 가능한 모든 명령을 표시하려면 **+?**를 입력합니다.

참고 명령 문자열에 물음표(?)를 포함하려면 물음표를 입력하기 전에 **Ctrl-V**를 눌러서 CLI 도움말이 실수로 호출되지 않도록 해야 합니다.

실행 중인 구성 보기

실행 중인 구성을 보려면 다음 명령 중 하나를 사용합니다.

명령 출력을 필터링하려면 "show 및 more 명령 출력 필터링" 섹션, 7-5페이지을 참고하십시오.

명령어	목적
show running-config [**all**] [*command*]	실행 중인 구성을 표시합니다. **all**을 지정하면 모든 기본 설정도 표시됩니다. *command*를 지정하면 출력에 관련 명령만 포함됩니다. **참고** 대다수의 비밀번호는 *****로 표시됩니다. 비밀번호를 일반 텍스트로 보거나 마스터 패스프레이즈가 활성화된 경우 암호화된 형식으로 보려면 아래의 **more** 명령을 사용합니다.
more system:running-config	실행 중인 구성을 표시합니다. 비밀번호는 일반 텍스트 또는 암호화된 형식(마스터 암호가 활성화된 경우)으로 표시됩니다.

show 및 more 명령 출력 필터링

show 명령에서 세로 막대(|)를 사용하여 필터 옵션 및 필터링 식을 포함할 수 있습니다. 필터링은 Cisco IOS 소프트웨어와 마찬가지로 각 출력 행을 정규식과 일치하여 수행합니다. 다른 필터 옵션을 선택하여 식과 일치하는 모든 출력을 포함하거나 제외할 수 있습니다. 또한 해당 식과 일치하는 행으로 시작되는 모든 출력도 표시할 수 있습니다.

show 명령에서 필터링 옵션을 사용하는 구문은 다음과 같습니다.

```
ciscoasa# show command | {include | exclude | begin | grep [-v]} regexp
```

또는

```
ciscoasa# more system:running-config | {include | exclude | begin | grep [-v]} regexp
```

참고 **more** 명령은 실행 중인 구성뿐만 아니라 모든 파일의 내용을 표시할 수 있습니다. 자세한 내용은 명령 참조를 참고하십시오.

이 명령 문자열에서 첫 번째 세로 막대(|)는 연산자이며 명령에 꼭 포함되어야 합니다. 이 연산자는 **show** 명령의 출력을 필터링하도록 지시합니다. 구문 다이어그램에서 다른 세로 막대 (|)는 대체 옵션을 나타내며, 명령의 일부가 아닙니다.

include 옵션은 정규식과 일치하는 모든 출력 행을 포함합니다. **-v**가 포함되지 않은 **grep** 옵션도 동일한 효과를 가집니다. **exclude** 옵션은 정규식과 일치하는 모든 출력 행을 제외합니다. **-v**가 포함된 **grep** 옵션도 동일한 효과를 가집니다. **begin** 옵션은 정규식과 일치하는 행으로 시작하는 모든 출력 행을 표시합니다.

*regexp*를 원하는 Cisco IOS 정규식으로 대체합니다. 정규식은 따옴표나 큰따옴표로 묶이지 않으므로 공백이 뒤에 오지 않도록 주의해야 합니다. 이러한 공백은 정규식에 포함되는 것으로 간주됩니다.

정규식을 만들 때 일치시킬 문자나 숫자를 사용할 수 있습니다. 또한 *metacharacters*라는 특정 키워드 문자는 정규식에서 사용될 때 특별한 의미를 가집니다.

CLI에서 물음표(?) 또는 탭 같은 모든 특수 문자를 이스케이프하려면 **Ctrl+V**를 사용합니다. 예를 들어 **d[Ctrl+V]?g**를 입력하여 구성에서 **d?g**를 입력할 수 있습니다.

show 명령 출력 리디렉션 및 추가

화면에 **show** 명령의 출력을 표시하는 대신 디바이스 또는 원격 위치에 있는 파일로 리디렉션할 수 있습니다. 디바이스에 있는 파일로 리디렉션하는 경우, 파일에 명령 출력을 추가할 수도 있습니다.

show *command* | {**append** | **redirect**} *url*

- **append** *url*은 출력을 기존 파일에 추가합니다. 다음 중 하나를 사용하여 파일을 지정합니다.
  - **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*] - **flash**와 **disk0** 둘 다 내부 플래시 메모리를 가리킵니다. 옵션 중 하나를 사용할 수 있습니다.
  - **disk1:/**[[*path*/]*filename*] - 외부 메모리를 가리킵니다.
- **redirect** *url*은 지정된 파일을 생성하거나 파일이 이미 있는 경우 이를 덮어씁니다.
  - **disk0:/**[[*path*/]*filename*] or **flash:/**[[*path*/]*filename*] - **flash**와 **disk0** 둘 다 내부 플래시 메모리를 가리킵니다. 옵션 중 하나를 사용할 수 있습니다.
  - **disk1:/**[[*path*/]*filename*] - 외부 메모리를 가리킵니다.

- **smb:**/[[*path*/]*filename*] - 서버 메시지 블록, UNIX 서버 로컬 파일 시스템을 나타냅니다.
- **ftp://**[[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]] - FTP 서버를 나타냅니다. **type**은 **ap**(ASCII 패시브 모드), **an**(ASCII 일반 모드), **ip**(기본값 - 이진 패시브 모드), **in**(이진 일반 모드) 키워드 중 하나일 수 있습니다.
- **scp://**[[*user*[**:***password*]**@**]*server*[/*path*]/*filename*[**;int=***interface_name*]] - SCP 서버를 나타냅니다. **;int=***interface* 옵션은 경로 조회를 우회하고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다.
- **tftp://**[[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*[**;int=***interface_name*]] - TFTP 서버를 나타냅니다.

show 명령 출력에 대한 라인 수 가져오기

show 명령 출력을 실제로 확인하는 대신 출력에서 행 수 또는 표현식과 일치하는 행 수를 간단하게 확인할 수 있습니다. 그런 다음 명령을 입력한 이전 횟수와 행 수를 쉽게 비교할 수 있습니다. 이렇게 하면 신속하게 구성하는 것처럼 빨리 확인할 수 있습니다. **count** 키워드를 사용하거나 **-c**를 **grep** 키워드에 추가할 수 있습니다.

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

*regular_expression*을 원하는 Cisco IOS 정규식으로 대체합니다. 정규식은 따옴표나 큰따옴표로 묶이지 않으므로 공백이 뒤에 오지 않도록 주의해야 합니다. 이러한 공백은 정규식에 포함되는 것으로 간주됩니다. 정규식은 선택 사항입니다. 포함하지 않을 경우 카운트가 필터링되지 않은 출력의 총 행 수를 반환합니다.

정규식을 만들 때 일치시킬 문자나 숫자를 사용할 수 있습니다. 또한 metacharacters라는 특정 키워드 문자는 정규식에서 사용될 때 특별한 의미를 가집니다. CLI에서 물음표(?) 또는 탭 같은 모든 특수 문자를 이스케이프하려면 **Ctrl+V**를 사용합니다. 예를 들어 **d[Ctrl+V]?g**를 입력하여 구성에서 **d?g**를 입력할 수 있습니다.

예를 들어, **show running-config** 출력에서 모든 행의 총 수를 표시합니다.

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

다음 예에서는 가동 중인 인터페이스 수가 얼마나 많은지 신속하게 확인하는 방법을 보여줍니다. 첫 번째 예에서는 가동 상태로 표시되는 행에서만 필터링하도록 정규식이 있는 **grep** 키워드를 사용하는 방법을 보여 줍니다. 다음 예에서는 출력의 실제 행 대신 카운트를 간단히 표시하기 위해 **-c** 옵션을 추가합니다.

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
Number of lines which match regexp = 2
```

명령 출력 페이징

help 또는 **?**, **show**, **show xlate** 또는 그 밖에 긴 목록을 제공하는 명령의 경우 정보가 화면에 표시되고 일시 중지되는지 또는 명령을 완성하도록 해주는지 확인할 수 있습니다. **pager** 명령을 사용하면 More 프롬프트가 나타나기 전에 표시할 행의 개수를 선택할 수 있습니다.

페이징이 활성화된 경우 다음 프롬프트가 나타납니다.

```
<--- More --->
```

More 프롬프트에서는 UNIX **more** 명령과 유사한 구문을 사용합니다.

- 다른 화면을 보려면 **스페이스바**를 누릅니다.
- 다음 행을 보려면 **Enter** 키를 누릅니다.
- 명령줄로 돌아가려면 **q** 키를 누릅니다.

주석 추가

행 앞에 콜론(:)을 넣어 주석을 생성할 수 있습니다. 그러나 주석은 명령 기록 버퍼에만 표시되고 구성에는 표시되지 않습니다. 따라서 **show history** 명령을 사용하거나, 화살표 키를 눌러 이전 명령을 검색하여 주석을 볼 수는 있지만, 주석은 구성에 없으므로 **write terminal** 명령은 주석을 표시하지 않습니다.

텍스트 구성 파일

이 섹션에서는 ASA에 다운로드할 수 있는 텍스트 구성 파일의 형식을 지정하는 방법을 설명하며, 다음 항목을 포함합니다.

명령이 텍스트 파일의 행과 일치하는 방식

텍스트 구성 파일에는 이 가이드에 설명된 명령과 대응하는 행이 포함되어 있습니다.

예를 들어, 명령은 CLI 프롬프트 앞에 옵니다. 다음 예의 프롬프트는 "ciscoasa(config)#" 입니다.

```
ciscoasa(config)# context a
```

텍스트 구성 파일에서는 명령을 입력하라는 프롬프트가 나타나지 않으므로 프롬프트가 생략됩니다.

```
context a
```

명령별 구성 모드 명령

명령별 구성 모드 명령은 명령줄에 입력할 경우 기본 명령 아래에 들여 쓴 형태로 표시됩니다. 텍스트 파일 행의 경우 명령이 기본 명령 다음에 바로 표시되기만 하면 들여 쓰지 않아도 됩니다. 예를 들어 다음 들여쓰기되지 않은 텍스트는 들여쓰기된 텍스트와 동일하게 해석됩니다.

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
  nameif outside
```

자동 텍스트 항목

구성을 ASA에 다운로드할 경우, 일부 행이 자동으로 삽입됩니다. 예를 들어, ASA에서는 기본 설정 또는 구성이 수정된 시간에 대한 행을 삽입합니다. 텍스트 파일을 만들 때 이러한 자동 항목을 입력할 필요가 없습니다.

행 순서

대부분의 경우 명령은 파일에서 정해진 순서가 없습니다. 그러나 ACE 같은 일부 행의 경우 표시되는 순서대로 처리되며, 이러한 순서는 액세스 목록의 기능에 영향을 미칠 수 있습니다. 다른 명령에도 순서 요건이 있을 수 있습니다. 예를 들어 많은 후속 명령에서 인터페이스 이름을 사용하는 경우 먼저 인터페이스에 대한 **nameif** 명령을 입력해야 합니다. 또한 명령별 구성 모드의 명령은 기본 명령 바로 다음에 와야 합니다.

텍스트 구성에 포함되지 않은 명령

일부 명령의 경우 구성에 행을 삽입하지 않습니다. 예를 들어, **show running-config** 같은 런타임 명령의 경우 텍스트 파일에 해당 행이 없습니다.

비밀번호

로그인, 활성화 및 사용자 비밀번호는 구성에 저장되기 전에 자동으로 암호화됩니다. 예를 들어 비밀번호 "cisco"의 암호화된 형식은 jMorNbK0514fadBh처럼 나타날 수 있습니다. 구성 비밀번호를 암호화된 형식으로 다른 ASA에 복사할 수 있지만 비밀번호의 암호를 직접 해독할 수는 없습니다.

텍스트 파일에 암호화되지 않은 비밀번호를 입력한 경우 ASA는 구성을 ASA에 복사할 때 비밀번호를 자동으로 암호화하지 않습니다. ASA에서는 **copy running-config startup-config** 또는 **write memory** 명령을 사용하여 명령줄에서 실행 중인 구성을 저장할 경우에만 비밀번호를 암호화합니다.

다중 보안 상황 파일

다중 보안 상황의 경우, 전체 구성이 다음과 같은 여러 부분으로 구성됩니다.

- 보안 상황 구성
- 시스템 구성 - ASA의 기본 설정(상황 목록 포함) 식별
- 관리자 상황 - 시스템 구성에 대한 네트워크 인터페이스 제공

  시스템 구성에는 시스템 자체에 대한 인터페이스 또는 네트워크 설정이 포함되지 않습니다. 그 대신 시스템에서 네트워크 리소스에 액세스해야 할 경우(예: 서버에서 상황을 다운로드할 경우), 관리자 상황으로 지정된 상황을 사용합니다.

각 상황은 단일 상황 모드 구성과 유사합니다. 시스템 구성은 시스템 전용 명령(예: 모든 상황의 목록)을 포함하지만 기타 일반적인 명령(예: 대다수의 인터페이스 파라미터)은 없다는 점에서 상황 구성과 다릅니다.

지원되는 문자 집합

ASA CLI는 현재 UTF-8 인코딩만 지원합니다. UTF-8은 유니코드 기호에 대한 특정 인코딩 체계이며, ASCII 기호 하위 집합과 호환되도록 설계되었습니다. ASCII 문자는 1바이트 문자로 UTF-8에 표시됩니다. 나머지 모든 문자는 다중 바이트 기호로 UTF-8에 표시됩니다.

인쇄 가능한 ASCII 문자(0x20~0x7e)는 완전히 지원됩니다. 인쇄 가능한 ASCII 문자는 ISO 8859-1과 동일합니다. UTF-8은 ISO 8859-1의 상위 집합이므로 첫 번째 256자(0-255)는 ISO 8859-1과 동일합니다. ASA CLI는 ISO 8859-1의 최대 255자(다중 바이트 문자)를 지원합니다.