Cisco ASA Series Firewall CLI 컨피그레이션 가이드

소프트웨어 버전 9.3

릴리스 날짜: 2014년 7월 24일
업데이트 날짜: 2014년 9월 16일

Cisco Systems, Inc.
www.cisco.com

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

텍스트 파트 번호: 해당 없음, 온라인 전용

Cisco ASA Series Firewall CLI 컨피그레이션 가이드

목 차

설명서 정보

문서의 용도

이 설명서의 목적은 사용자가 명령줄 인터페이스인을 사용하여 Cisco ASA Series용 방화벽 기능을 구성하도록 도와주는 것입니다. 여기서는 모든 기능을 다루기보다는 가장 대표적인 컨피그레이션 시나리오에 대해서만 설명합니다.

웹 기반 GUI 애플리케이션인 ASDM(Adaptive Security Device Manager)을 사용하여 ASA를 구성하고 모니터링할 수도 있습니다. ASDM에서는 일반적인 컨피그레이션 시나리오를 안내하는 컨피그레이션 마법사 및 상대적으로 일반적이지 않은 시나리오를 위한 온라인 도움말을 제공합니다.

이 설명서에서 "ASA"는 달리 명시되지 않는 한 지원되는 모델을 총칭합니다.

관련 설명서

자세한 내용은 Cisco ASA Series 설명서(*Navigating the Cisco ASA Series Documentation*, http://www.cisco.com/go/asadocs)를 참조하십시오.

표기 규칙

이 설명서는 다음과 같은 표기 규칙을 사용합니다.

표기 규칙	표시
굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은** 글꼴로 표시합니다.
기울임꼴	설명서 제목, 신규 용어 또는 강조된 용어, 사용자가 값을 지정해야 하는 인수는 *기울임꼴*로 표시합니다.
[ ]	대괄호로 묶인 요소는 선택 사항입니다.

{x | y | z }	필수 대체 키워드는 중괄호로 묶어 세로 선으로 구분합니다.
[x | y | z]	선택적 대체 키워드는 대괄호로 묶어 세로 선으로 구분합니다.
문자열	따옴표 없는 문자의 집합입니다. 문자열 주변에 따옴표를 사용하지 마십시오. 그러지 않으면 따옴표도 문자열에 포함됩니다.
`courier` 글꼴	시스템에 표시되는 터미널 세션 및 정보는 `courier` 글꼴로 표시됩니다.
`courier` 굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은 `courier`** 글꼴로 표시됩니다.
`courier` 기울임꼴	사용자가 값을 지정하는 인수는 *`courier` 기울임꼴*로 표시됩니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 우물 정자(#)는 코멘트 라인을 나타냅니다.

참고 *독자가 주목해야 하는 내용*을 의미합니다.

팁 *다음 정보가 문제를 해결하는 데 도움이 된다는 것*을 의미합니다.

주의 *독자가 유의해야 하는 내용*을 의미합니다. 이 경우, 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 합니다.

설명서 받기 및 서비스 요청 제출

설명서 다운로드, Cisco BST(Bug Search Tool) 사용, 서비스 요청 제출, 추가 정보 수집에 대한 자세한 내용은 *Cisco 제품 설명서의 새로운 소식* (http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html)을 참조하십시오.

Cisco의 새로운 기술 문서 및 개정된 기술 문서를 모두 소개하는 *Cisco 제품 설명서의 새로운 소식*을 RSS 피드로 구독하면 콘텐츠가 데스크톱으로 곧바로 배달되어 리더 애플리케이션으로 읽어볼 수 있습니다. RSS 피드는 무료로 제공되는 서비스입니다.

파 트 1

서비스 정책 및 액세스 제어

Modular Policy Framework를 사용하는 서비스 정책

릴리스 날짜: 2014년 7월 24일
업데이트 날짜: 2014년 9월 16일

Modular Policy Framework를 사용하는 서비스 정책은 ASA 기능을 구성하기 위한 일관되고 유연한 방법을 제공합니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 컨피그레이션을 만드는 서비스 정책을 사용할 수 있습니다. 서비스 정책은 인터페이스에 적용되거나 전체적으로 적용되는 여러 작업 또는 규칙으로 구성됩니다.

서비스 정책 정보

다음 항목에서는 서비스 정책의 작동 방식에 대해 설명합니다.

서비스 정책의 구성 요소

서비스 정책의 요점은 허용 트래픽에 고급 서비스를 적용하는 것입니다. 액세스 규칙에서 허용하는 트래픽에는 서비스 정책을 적용할 수 있습니다. 이에 따라 이러한 트래픽은 서비스 모듈로 리디렉션되거나 애플리케이션 검사를 받는 등 특수한 프로세싱을 거치게 됩니다.

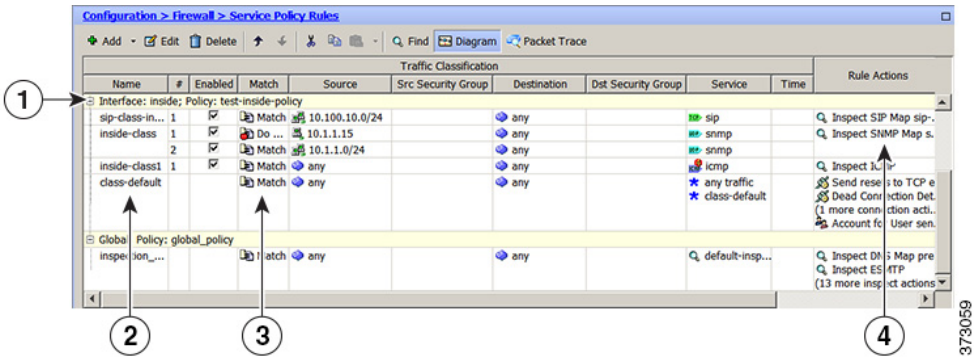
다음 유형의 서비스 정책을 사용할 수 있습니다.

- 모든 인터페이스에 적용되는 하나의 글로벌 정책.
- 인터페이스당 적용되는 하나의 서비스 정책. 이 정책에서는 디바이스를 통과한 트래픽 및 ASA 인터페이스에서 전달된(통과되기보다는) 관리 트래픽에 대한 클래스를 혼합할 수 있습니다.

각 서비스 정책은 다음 요소로 구성됩니다.

1. 서비스 정책 맵 - 순서가 지정된 규칙의 집합으로, **service-policy** 명령을 통해 이름을 지정합니다. ASDM에서는 정책 맵이 Service Policy Rules 페이지에 폴더로서 표시됩니다.
2. 규칙 - 각 규칙은 서비스 정책 맵 내의 **class** 명령이거나 **class** 명령과 연결된 명령입니다. ASDM에서 각 규칙은 별도의 행에 표시되며, 규칙의 이름은 클래스 이름입니다.
   a. **class** 명령은 규칙의 트래픽 매칭 기준을 정의합니다.
   b. **inspect**, **set connection timeout** 등의 클래스와 연결된 명령은 일치하는 트래픽에 적용되는 서비스 및 제약 조건을 정의합니다. inspect 명령은 검사된 트래픽에 적용할 작업을 정의하는 검사 정책 맵을 가리킬 수 있습니다. 검사 정책 맵과 서비스 정책 맵은 서로 다르다는 점에 유의해야 합니다.

다음의 예는 ASDM에 나타나는 서비스 정책과 CLI에 나타나는 서비스 정책을 비교하여 보여줍니다. 그림의 콜아웃과 CLI의 줄이 1대1로 매핑되지는 않습니다.



위의 그림에서 보여주는 규칙에 의해 다음 CLI가 생성됩니다.

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all by v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
```

```
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

서비스 정책으로 구성된 기능

다음 표에는 서비스 정책을 사용하여 구성하는 기능이 나열되어 있습니다.

표 1-1 서비스 정책으로 구성된 기능

기능	통과 트래픽?	관리 트래픽?	참조:
애플리케이션 검사(여러 유형)	RADIUS 어카운팅을 제외한 **전부**	**RADIUS 어카운팅** 전용	• 7 장, “애플리케이션 계층 프로토콜 검사 시작”. • 8 장, “기본 인터넷 프로토콜 검사”. • 9 장, “음성 및 비디오 프로토콜에 대한 검사”. • 10 장, “데이터베이스 및 디렉토리 프로토콜 검사”. • 11 장, “관리 애플리케이션 프로토콜에 대한 검사”. • 15 장, “ASA 및 Cisco Cloud Web Security”.
ASA IPS	**예**	아니요	19 장, “ASA IPS 모듈”.
ASA CX	**예**	아니요	18 장, “ASA CX 모듈”.
ASA FirePOWER(ASA SFR)	**예**	아니요	17 장, “ASA FirePOWER(SFR) 모듈”.
NetFlow Secure Event Logging 필터링	**예**	**예**	일반 운영 컨피그레이션 가이드 섹션을 참조하십시오.
QoS 입력 및 출력 폴리싱	**예**	아니요	13 장, “Quality of Service”.
QoS 표준 우선 순위 큐	**예**	아니요	13 장, “Quality of Service”.
TCP 및 UDP 연결 제한과 시간 제한, TCP 시퀀스 번호 임의 지정	**예**	**예**	12 장, “연결 설정”.
TCP 정규화	**예**	아니요	12 장, “연결 설정”.
TCP 상태 바이패스	**예**	아니요	12 장, “연결 설정”.
아이덴티티 방화벽용 사용자 통계	**예**	**예**	명령 참조의 **user-statistics** 명령을 참조하십시오.

기능 방향성

기능에 따라 작업이 트래픽에 양방향 또는 단방향으로 적용됩니다. 양방향으로 적용되는 기능의 경우, 트래픽이 양쪽 방향에서 클래스 맵과 일치하면 정책 맵을 적용하는 인터페이스로 드나드는 모든 트래픽이 영향을 받습니다.

참고 글로벌 정책을 사용하면 모든 기능은 단방향입니다. 단일 인터페이스에 적용될 때 정상적으로 양방향인 기능을 전체적으로 적용하면 인그레스(ingress)에만 적용됩니다. 정책은 모든 인터페이스에 적용되므로 양쪽 방향에 적용되어서, 이 경우 양방향이 중복됩니다.

단방향으로 적용되는 기능의 경우(예: QoS 우선 순위 큐), 정책 맵을 적용하는 인터페이스로 들어가는 트래픽(또는 나가는 트래픽, 기능에 따라 다름)만 영향을 받습니다. 각 기능의 방향성은 다음 표를 참조하십시오.

표 1-2 기능 방향성

기능	단일 인터페이스 방향	글로벌 방향
애플리케이션 검사(여러 유형)	양방향	인그레스
ASA CSC	양방향	인그레스
ASA CX	양방향	인그레스
ASA CX 인증 프록시	인그레스	인그레스
ASA FirePOWER(ASA SFR)	양방향	인그레스
ASA IPS	양방향	인그레스
NetFlow Secure Event Logging 필터링	N/A	인그레스
QoS 입력 폴리싱	인그레스	인그레스
QoS 출력 폴리싱	이그레스	이그레스
QoS 표준 우선 순위 큐	이그레스	이그레스
TCP 및 UDP 연결 제한과 시간 제한, TCP 시퀀스 번호 임의 지정	양방향	인그레스
TCP 정규화	양방향	인그레스
TCP 상태 바이패스	양방향	인그레스
아이덴티티 방화벽용 사용자 통계	양방향	인그레스

서비스 정책 내에서의 기능 일치

패킷은 다음 규칙에 따라 지정된 인터페이스의 정책 맵에서 클래스 맵과의 일치가 확인됩니다.

1. 패킷은 각 기능 유형에 대해 인터페이스의 정책 맵 규칙에서맵에서만 일치가 확인됩니다.
2. 패킷이 특정 기능 유형에 대해 하나의 클래스 맵과 일치하면 ASA에서는 해당 기능에 대해 이후의 다른 클래스 맵과 일치를 확인하려고 시도하지 않습니다.
3. 그러나 패킷이 다른 기능 유형에 대해 이후의 클래스 맵과 일치하면 ASA에서는 이후의 클래스 맵에 대한 작업도 적용합니다(지원되는 경우). 지원되지 않는 조합에 대한 자세한 내용은 1-6 페이지의 특정 기능 작업의 비호환성을 참조하십시오.

참고 애플리케이션 검사에는 여러 검사 유형이 포함되며 대부분 상호 배타적입니다. 결합할 수 있는 검사의 경우 각 검사는 별도의 기능으로 고려됩니다.

패킷 일치의 예

예:

- 패킷이 연결 제한에 대한 클래스 맵과 일치하고 애플리케이션 검사에 대한 클래스 맵과도 일치하면 두 작업이 모두 적용됩니다.
- 패킷이 HTTP 검사에 대한 클래스 맵과 일치하고 HTTP 검사를 포함하는 또 다른 클래스 맵과도 일치하면 두 번째 클래스 맵 작업은 적용되지 않습니다.

- 패킷이 HTTP 검사에 대한 클래스 맵과 일치하고 FTP 검사를 포함하는 또 다른 클래스 맵과도 일치하면 두 번째 클래스 맵 작업은 적용되지 않습니다. HTTP와 FTP 검사는 결합할 수 없기 때문입니다.
- 패킷이 HTTP 검사에 대한 클래스 맵과 일치하고 IPv6 검사를 포함하는 또 다른 클래스 맵과도 일치하면 두 작업이 모두 적용됩니다. IPv6 검사는 다른 모든 유형의 검사와 결합할 수 있기 때문입니다.

여러 기능 작업이 적용되는 순서

정책 맵의 서로 다른 작업 유형이 수행되는 순서는 정책 맵에 작업이 나타나는 순서와 상관이 없습니다.

작업은 다음 순서로 수행됩니다.

1. QoS 입력 폴리싱
2. TCP 정규화, TCP 및 UDP 연결 제한과 시간 제한, TCP 시퀀스 번호 임의 지정, TCP 상태 바이패스.

   참고 ASA가 프록시 서비스(예: AAA 또는 CSC)를 수행하거나 TCP 페이로드(예: FTP 검사)를 수정하면, TCP 노멀라이저가 이중 모드에서 작동하여 프록시 또는 페이로드 수정 서비스 전후에 적용됩니다.

3. ASA CSC
4. 다른 검사와 결합할 수 있는 애플리케이션 검사:
   a. IPv6
   b. IP 옵션
   c. WAAS
5. 다른 검사와 결합할 수 없는 애플리케이션 검사. 자세한 내용은 1-6 페이지의 특정 기능 작업의 비호환성 섹션을 참조하십시오.
6. ASA IPS
7. ASA CX
8. ASA FirePOWER(ASA SFR)
9. QoS 출력 폴리싱
10. QoS 표준 우선 순위 큐

참고 NetFlow Secure Event Logging 필터링 및 아이덴티티 방화벽용 사용자 통계는 순서와 관련이 없습니다.

특정 기능 작업의 비호환성

일부 기능은 동일한 트래픽에 대해 서로 호환되지 않습니다. 비호환성을 보여주는 다음 리스트에는 누락된 내용이 있을 수 있습니다. 각 기능의 호환성에 대한 정보는 해당 기능의 장 또는 섹션을 참조하십시오.

- 동일한 트래픽 집합에 대해서는 QoS 우선 순위 큐잉과 QoS 폴리싱을 구성할 수 없습니다.

- 대부분의 검사는 다른 검사와 결합할 수 없습니다. 따라서 사용자가 동일한 트래픽에 대해 여러 검사를 구성한 경우 ASA는 하나의 검사만 적용합니다. HTTP 검사는 클라우드 Cloud Web Security와 결합할 수 없습니다. 기타 예외는 1-6 페이지의 여러 기능 작업이 적용되는 순서에 나열되어 있습니다.
- 트래픽을 여러 모듈(예: ASA CX 및 ASA IPS)로 전송하도록 구성할 수 없습니다.
- HTTP 검사는 ASA CX 또는 ASA FirePOWER와 호환되지 않습니다.
- Cloud Web Security는 ASA CX 또는 ASA FirePOWER와 호환되지 않습니다.

참고 기본 글로벌 정책에서 사용되는 **match default-inspection-traffic** 명령는 모든 검사용 기본 포트를 확인하기 위한 특수 CLI 바로 가기입니다. 이 클래스 맵을 정책 맵에서 사용하면 트래픽의 목적지 포트를 기반으로 올바른 검사가 각 패킷에 적용됩니다. 예를 들어 포트 69용 UDP 트래픽이 ASA에 도달하면 ASA는 TFTP 검사를 적용합니다. 포트 21용 TCP 트래픽이 도착하면 ASA는 FTP 검사를 적용합니다. 따라서 이 경우에만 동일한 클래스 맵에 대해 여러 검사를 구성할 수 있습니다. 일반적으로 ASA는 적용할 검사를 결정하는 데 포트 번호를 사용하지 않으므로, 사용자는 예를 들어 비표준 포트에도 유연하게 검사를 적용할 수 있습니다.

이 트래픽 클래스에는 Cloud Web Security 검사용 기본 포트(80 및 443)가 포함되어 있지 않습니다.

잘못된 컨피그레이션의 예는 동일한 정책 맵에 여러 검사를 구성하고 default-inspection-traffic 바로 가기를 사용하지 않는 것입니다. 예 1-1에서는 포트 21로 이동하는 트래픽이 FTP 및 HTTP 검사 모두에 대해 잘못 구성되었습니다. 예 1-2에서는 포트 80으로 이동하는 트래픽이 FTP 및 HTTP 검사 모두에 대해 잘못 구성되었습니다. 잘못된 컨피그레이션의 이 두 가지 예에서는 FTP 검사만 적용됩니다. 적용되는 검사의 순서에서 FTP가 HTTP 앞에 오기 때문입니다.

예 1-1 FTP 패킷의 잘못된 컨피그레이션: HTTP 검사도 구성됨

```
class-map ftp
   match port tcp eq 21
class-map http
   match port tcp eq 21 [it should be 80]
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

예 1-2 HTTP 패킷의 잘못된 컨피그레이션: FTP 검사도 구성됨

```
class-map ftp
   match port tcp eq 80 [it should be 21]
class-map http
   match port tcp eq 80
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

여러 서비스 정책의 기능 일치

TCP 및 UDP(상태 기반 ICMP 검사를 활성화한 경우 ICMP) 트래픽의 경우 개별 패킷만이 아니라 트래픽 흐름에서도 서비스 정책이 작동합니다. 트래픽이 한 인터페이스에서 정책의 기능과 일치하는 기존 연결의 일부인 경우, 또 다른 인터페이스에서 정책의 동일한 기능으로 해당 트래픽 흐름을 확인할 수 없습니다. 첫 번째 정책만 사용됩니다.

예를 들어, HTTP 트래픽이 HTTP 트래픽을 검사하는 내부 인터페이스의 정책과 일치하며 HTTP 검사에 대한 별도의 정책이 외부 인터페이스에 있으면, 해당 트래픽은 외부 인터페이스의 이그레스에서는 다시 검사되지 않습니다. 마찬가지로, 외부 인터페이스의 인그레스 정책과 내부 인터페이스의 이그레스 정책에서 모두 해당 연결의 반환 트래픽을 검사하지 않습니다.

흐름으로 취급되지 않는 트래픽(예: 상태 기반 ICMP 검사를 활성화하지 않은 경우의 ICMP)의 경우, 반환 트래픽은 반환 인터페이스의 다른 정책 맵으로 확인할 수 있습니다. 예를 들어 내부 및 외부 인터페이스에서 IPS를 구성하지만 내부 정책에서는 가상 센서 1을 사용하고 외부 정책에서는 가상 센서 2를 사용하는 경우, 비 상태 기반 Ping은 아웃바운드에서 가상 센서 1을 확인하고 인바운드에서 가상 센서 2를 확인합니다.

서비스 정책 지침

IPv6 지침

다음 기능에 대해 IPv6을 지원합니다.

- DNS, FTP, HTTP, ICMP, ScanSafe, SIP, SMTP, IPsec-pass-thru 및 IPv6에 대한 애플리케이션 검사.
- ASA IPS
- ASA CX
- ASA FirePOWER
- NetFlow Secure Event Logging 필터링
- TCP 및 UDP 연결 제한과 시간 제한, TCP 시퀀스 번호 임의 지정
- TCP 정규화
- TCP 상태 바이패스
- 아이덴티티 방화벽용 사용자 통계

클래스 맵(트래픽 클래스) 지침

모든 클래스 맵(트래픽 클래스) 유형의 최대 수는 단일 모드에서 또는 다중 모드의 컨텍스트당 255개입니다. 클래스 맵에는 다음 유형이 포함됩니다.

- Layer 3/4 클래스 맵(통과 트래픽 및 관리 트래픽의 경우)
- 검사 클래스 맵
- 정규식 클래스 맵
- **match** 명령(검사 정책 맵 바로 아래에서 사용됨)

또한 이 제한은 모든 유형의 기본 클래스 맵을 포함하며 사용자 구성 클래스 맵을 약 235개로 제한합니다. 1-10 페이지의 기본 클래스 맵(트래픽 클래스) 섹션을 참조하십시오.

정책 맵 지침

정책 맵 사용에 대한 다음 지침을 참조하십시오.

- 인터페이스당 정책 맵을 하나만 할당할 수 있습니다. 그러나 컨피그레이션에서 최대 64개의 정책 맵을 만들 수 있습니다.
- 동일한 정책 맵을 여러 인터페이스에 적용할 수 있습니다.
- Layer 3/4 정책 맵 하나에서 최대 63개의 Layer 3/4 클래스 맵을 식별할 수 있습니다.
- 각 클래스 맵에 대해 하나 이상의 기능 유형에서 여러 작업을 할당할 수 있습니다(지원되는 경우). 1-6 페이지의 특정 기능 작업의 비호환성 섹션을 참조하십시오.

서비스 정책 지침

- 특정 기능에 대해 인터페이스 서비스 정책이 글로벌 서비스 정책보다 우선 적용됩니다. 예를 들어 FTP 검사가 포함된 글로벌 정책 및 TCP 정규화가 포함된 인터페이스 정책을 가지고 있으면 인터페이스에는 FTP 검사와 TCP 정규화가 모두 적용됩니다. 그러나 FTP 검사가 포함된 글로벌 정책 및 FTP 검사가 포함된 인터페이스 정책을 가지고 있으면 해당 인터페이스에는 인터페이스 정책 FTP 검사만 적용됩니다.
- 글로벌 정책은 하나만 적용할 수 있습니다. 예를 들어, 기능 집합 1이 포함된 글로벌 정책 및 기능 집합 2가 포함된 별도의 글로벌 정책을 만들 수 없습니다. 모든 기능은 단일 정책에 포함해야 합니다.
- 컨피그레이션에서 서비스 정책을 변경하면 모든 *새* 연결에 새 서비스 정책이 사용됩니다. 기존 연결에는 연결 설정 시 구성된 정책이 계속해서 사용됩니다. **show** 명령의 출력에는 이전 연결에 대한 데이터가 포함되지 않습니다.

  예를 들어, 인터페이스에서 QoS 서비스 정책을 제거하고 수정된 버전을 추가하면 **show service-policy** 명령은 새 서비스 정책과 일치하는 새 연결과 관련된 QoS 카운터만 표시합니다. 이전 정책의 기존 연결은 명령 출력에 더 이상 표시되지 않습니다.

  모든 연결에서 새 정책이 사용되도록 하려면, 새 정책을 사용하여 다시 연결할 수 있도록 현재 연결을 모두 끊어야 합니다. **clear conn** 또는 **clear local-host** 명령을 사용하십시오.

서비스 정책 기본값

다음 항목에서는 서비스 정책 및 Modular Policy Framework의 기본 설정에 대해 설명합니다.

- 1-9 페이지의 기본 서비스 정책 컨피그레이션
- 1-10 페이지의 기본 클래스 맵(트래픽 클래스)

기본 서비스 정책 컨피그레이션

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며, 모든 인터페이스의 트래픽에 특정 검사가 적용됩니다(글로벌 정책). 모든 검사가 기본적으로 사용되는 것은 아닙니다. 글로벌 정책은 하나만 적용할 수 있으므로, 글로벌 정책을 변경하려면 기본 정책을 편집하거나 비활성화한 후 새 정책을 적용해야 합니다. 인터페이스 정책은 특정 기능에 대해 글로벌 정책을 재지정합니다.

기본 정책에는 다음 애플리케이션 검사가 포함됩니다.

- DNS
- FTP
- H323(H225)

- H323(RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny(SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

기본 정책 컨피그레이션에는 다음 명령이 포함됩니다.

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
service-policy global_policy global
```

참고 기본 클래스 맵에 사용되는 특수 **match default-inspection-traffic** 명령에 대한 자세한 내용은 1-6 페이지의 특정 기능 작업의 비호환성을 참조하십시오.

기본 클래스 맵(트래픽 클래스)

컨피그레이션에는 ASA가 default-inspection-traffic이라는 기본 글로벌 정책에서 사용하며 기본 검사 트래픽을 확인하는 기본 Layer 3/4 클래스 맵(트래픽 클래스)이 포함됩니다. 기본 글로벌 정책에서 사용되는 이 클래스는 모든 검사에 대해 기본 포트를 확인하는 특수 바로 가기입니다.

이 클래스를 정책에서 사용하면 트래픽의 목적지 포트를 기반으로 각 패킷에 올바른 검사가 적용됩니다. 예를 들어 포트 69용 UDP 트래픽이 ASA에 도달하면 ASA는 TFTP 검사를 적용합니다. 포트 21용 TCP 트래픽이 도착하면 ASA는 FTP 검사를 적용합니다. 따라서 이 경우에만 동일한 클래스 맵에 대해 여러 검사를 구성할 수 있습니다. 일반적으로 ASA는 적용할 검사를 결정하는 데 포트 번호를 사용하지 않으므로, 사용자는 예를 들어 비표준 포트에도 유연하게 검사를 적용할 수 있습니다.

```
class-map inspection_default
 match default-inspection-traffic
```

기본 컨피그레이션에 존재하는 또 다른 클래스 맵은 모든 트래픽을 확인하는 class-default입니다. 이 클래스 맵은 모든 Layer 3/4 정책 맵의 끝에 나타나며, 모든 기타 트래픽에 대해서는 어떤 작업도 수행하지 않도록 ASA에 특별히 지시합니다. 원하는 경우 Any 트래픽 클래스를 사용하는 자체 **match any** 클래스 맵을 대신 class-default 클래스를 사용할 수 있습니다. 실제로 일부 기능은 class-default에 대해서만 이용 가능합니다.

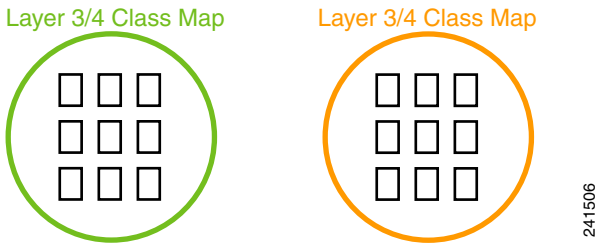
```
class-map class-default
 match any
```

서비스 정책 구성

Modular Policy Framework를 사용하여 서비스 정책을 구성하려면 다음 단계를 수행하십시오.

1단계 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)에서 설명한 대로 Layer 3/4 클래스 맵을 만들어서 작업을 수행할 트래픽을 식별합니다.

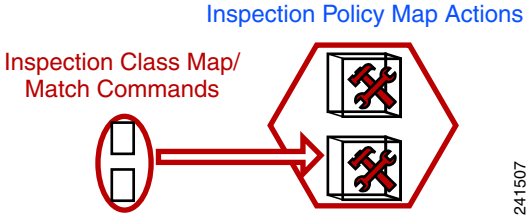
예를 들면, ASA를 통과하는 모든 트래픽에 대해 작업을 수행할 수도 있고, 10.1.1.0/24에서 모든 수신 주소로 이동하는 트래픽에 대해서만 특정 작업을 수행할 수도 있습니다.



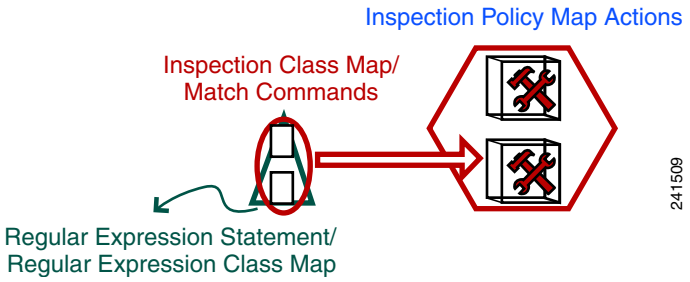
2단계 선택적으로, 일부 검사 트래픽에 대해 추가 작업을 수행합니다.

수행할 작업 중 하나가 애플리케이션 검사이며 일부 검사 트래픽에 대해 추가 작업을 수행하려는 경우 검사 정책 맵을 만드십시오. 검사 정책 맵은 트래픽을 식별하고 어떤 작업을 수행할지를 지정합니다.

예를 들면, 본문 길이가 1000바이트보다 큰 모든 HTTP 요청을 삭제할 수 있습니다.

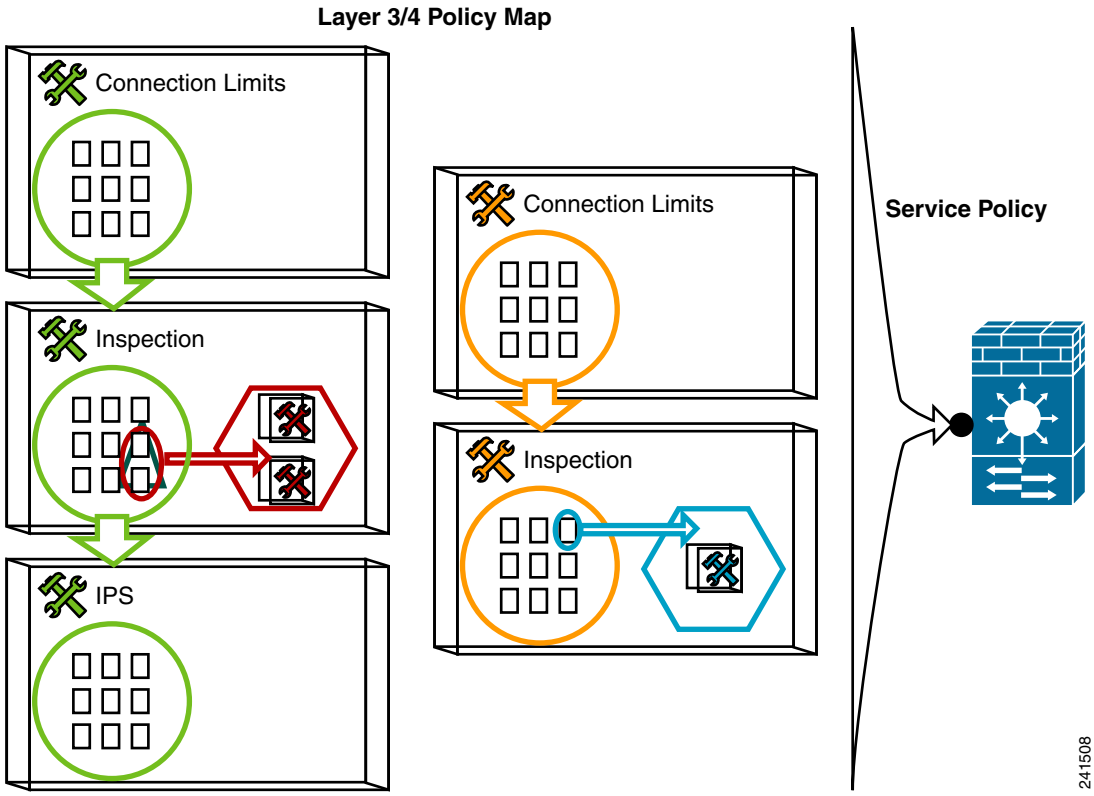


match 명령으로 트래픽을 직접 식별하는 자체 포함 검사 정책 맵을 만들거나, 재사용을 위한 또는 좀 더 복잡한 일치를 위한 검사 클래스 맵을 만들 수도 있습니다. 예를 들어, 정규식 또는 정규식 그룹(정규식 클래스 맵)을 사용하여 검사된 패킷 내부의 텍스트를 확인하고 좀 더 기준을 좁혀 작업 대상을 지정할 수 있습니다. 예를 들면, "example.com" 텍스트가 포함된 URL의 모든 HTTP 요청을 삭제할 수 있습니다.



2-4 페이지의 검사 정책 맵에서 작업 정의 및 2-5 페이지의 검사 클래스 맵의 트래픽 식별 섹션을 참조하십시오.

3단계 1-16 페이지의 작업 정의(Layer 3/4 정책 맵)에서 설명한 대로 Layer 3/4 정책 맵을 만들어 각 Layer 3/4 클래스 맵에서 수행할 작업을 정의합니다.



4단계 1-17 페이지의 인터페이스에 작업 적용(서비스 정책)에서 설명한 대로 정책 맵을 적용할 인터페이스를 결정하거나, 전체적으로 적용합니다.

트래픽 식별(Layer 3/4 클래스 맵)

Layer 3/4 클래스 맵은 작업을 적용할 Layer 3 및 4 트래픽을 식별합니다. 각 Layer 3/4 정책 맵에 대해 여러 Layer 3/4 클래스 맵을 만들 수 있습니다.

- 1-13 페이지의 통과 트래픽용 Layer 3/4 클래스 맵 만들기
- 1-15 페이지의 관리 트래픽용 Layer 3/4 클래스 맵 만들기

통과 트래픽용 Layer 3/4 클래스 맵 만들기

Layer 3/4 클래스 맵은 프로토콜, 포트, IP 주소 및 기타 Layer 3 또는 4 특성을 기반으로 트래픽을 확인합니다.

팁 애플리케이션 트래픽이 예상되는 포트에 대해서만 트래픽을 검사하는 것이 좋습니다. 예를 들어 **match any**를 사용하여 모든 트래픽을 검사하는 경우 ASA 성능이 저하될 수 있습니다.

절차

1단계 Layer 3/4 클래스 맵을 만듭니다. 여기서 *class_map_name*은 길이 최대 40자의 문자열입니다.

class-map *class_map_name*

"class-default"는 예약된 이름입니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다. CLI가 클래스 맵 컨피그레이션 모드로 들어갑니다.

예:

```
hostname(config)# class-map all_udp
```

2단계 (선택 사항) 클래스 맵에 설명을 추가합니다.

description *string*

예:

```
hostname(config-cmap)# description All UDP traffic
```

3단계 다음 명령 중 하나를 사용하여 트래픽을 확인합니다. 달리 지정되지 않는 한 클래스 맵에 **match** 명령을 하나만 포함할 수 있습니다.

- **match any** - 모든 트래픽을 확인합니다.

  ```
  hostname(config-cmap)# match any
  ```

- **match access-list** *access_list_name* - 확장 ACL에서 지정한 트래픽을 확인합니다. ASA가 투명 방화벽 모드에서 운영되는 경우 EtherType ACL을 사용할 수 있습니다.

  ```
  hostname(config-cmap)# match access-list udp
  ```

- **match port** {**tcp** | **udp**} {**eq** *port_num* | **range** *port_num port_num*} - TCP 또는 UDP 목적지 포트(단일 포트 또는 연속된 포트의 범위)를 확인합니다. 비연속 다중 포트를 사용하는 애플리케이션의 경우 **match access-list** 명령을 사용하고 각 포트를 확인할 ACE를 정의하십시오.

  ```
  hostname(config-cmap)# match tcp eq 80
  ```

- **match default-inspection-traffic** - 검사할 기본 트래픽을 확인합니다. 기본 TCP 및 UDP 포트는 ASA에서 검사할 수 있는 모든 애플리케이션에서 사용됩니다.

  ```
  hostname(config-cmap)# match default-inspection-traffic
  ```

  기본 글로벌 정책에서 사용되는 이 명령은 특수 CLI 바로 가기입니다. 이 명령을 정책 맵에서 사용하면 트래픽의 목적지 포트를 기반으로 각 패킷에 올바른 검사가 적용됩니다. 예를 들어 포트 69용 UDP 트래픽이 ASA에 도달하면 ASA는 TFTP 검사를 적용합니다. 포트 21용 TCP 트래픽이 도착하면 ASA는 FTP 검사를 적용합니다. 따라서 이 경우에만 동일한 클래스 맵에 대해 여러 검사를 구성할 수 있습니다. 다른 검사와 함께 구성할 수 있는 WAAS 검사는 예외입니다. 작업 결합에 대한 자세한 내용은 1-6 페이지의 특정 기능 작업의 비호환성을 참조하십시오. 일반적으로 ASA는 적용할 검사를 결정하는 데 포트 번호를 사용하지 않으므로, 사용자는 예를 들어 비표준 포트에도 유연하게 검사를 적용할 수 있습니다.

  기본 포트 리스트는 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오. **match default-inspection-traffic** 명령에 해당 포트가 포함된 애플리케이션이 모두 정책 맵에서 기본적으로 활성화되는 것은 아닙니다.

  일치하는 트래픽을 좁히려면 **match access-list** 명령과 **match default-inspection-traffic** 명령을 함께 지정할 수 있습니다. **match default-inspection-traffic** 명령은 확인할 포트 및 프로토콜을 지정하므로 ACL의 포트 및 프로토콜은 모두 무시됩니다.

- **match dscp** *value1* [*value2*] [...] [*value8*] - IP 헤더에서 DSCP 값을 확인합니다(DSCP 값 최대 8개).

  ```
  hostname(config-cmap)# match dscp af43 cs1 ef
  ```

- **match precedence** *value1* [*value2*] [*value3*] [*value4*] - IP 헤더에서 TOS 바이트로 표시되는 최대 4개의 우선 적용 값을 확인합니다. 여기서 *value1~value4*는 가능한 우선 적용에 따라 0~7일 수 있습니다.

  ```
  hostname(config-cmap)# match precedence 1 4
  ```

- **match rtp** *starting_port range* - RTP 트래픽을 확인합니다. 여기서 *starting_port*는 2000~65534의 짝수 UDP 목적지 포트입니다. *range*는 추가 UDP 포트(*starting_port* 위, 0~16383)의 번호를 지정합니다.

  ```
  hostname(config-cmap)# match rtp 4004 100
  ```

- **match tunnel-group** *name* - QoS를 적용할 VPN 터널 그룹 트래픽을 확인합니다.

  트래픽 일치를 조정하기 위해 또 다른 **match** 명령을 지정할 수도 있습니다. 이전 명령 중 하나를 지정할 수 있지만 **match any**, **match access-list** 또는 **match default-inspection-traffic** 명령은 예외입니다. 또는 각 IP 주소로 이동하는 터널 그룹에서 흐름을 확인하기 위해 **match flow ip destination-address** 명령을 입력할 수도 있습니다.

  ```
  hostname(config-cmap)# match tunnel-group group1
  hostname(config-cmap)# match flow ip destination-address
  ```

예

다음은 **class-map** 명령의 예입니다.

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp
```

```
hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

관리 트래픽용 Layer 3/4 클래스 맵 만들기

ASA로 이동하는 관리 트래픽에 대해서는 이 종류의 트래픽에만 해당하는 작업을 수행할 수 있습니다. ACL, TCP 또는 UDP 포트를 확인할 관리 클래스 맵을 지정할 수 있습니다. 정책 맵의 관리 클래스 맵에 사용할 수 있는 작업의 유형은 관리 트래픽에 맞게 특화되어 있습니다. 1-4 페이지의 서비스 정책으로 구성된 기능 섹션을 참조하십시오.

절차

1단계 관리 클래스 맵을 만듭니다. 여기서 *class_map_name*은 길이 최대 40자의 문자열입니다.

class-map type management *class_map_name*

"class-default"는 예약된 이름입니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다. CLI가 클래스 맵 컨피그레이션 모드로 들어갑니다.

예:

```
hostname(config)# class-map all_udp
```

2단계 (선택 사항) 클래스 맵에 설명을 추가합니다.

description *string*

예:

```
hostname(config-cmap)# description All UDP traffic
```

3단계 다음 명령 중 하나를 사용하여 트래픽을 확인합니다.

- **match access-list** *access_list_name* - 확장 ACL에서 지정한 트래픽을 확인합니다. ASA가 투명 방화벽 모드에서 운영되는 경우 EtherType ACL을 사용할 수 있습니다.

  ```
  hostname(config-cmap)# match access-list udp
  ```

- **match port** {**tcp** | **udp**} {**eq** *port_num* | **range** *port_num port_num*} - TCP 또는 UDP 목적지 포트(단일 포트 또는 연속된 포트의 범위)를 확인합니다. 비연속 다중 포트를 사용하는 애플리케이션의 경우 **match access-list** 명령을 사용하고 각 포트를 확인할 ACE를 정의하십시오.

  ```
  hostname(config-cmap)# match tcp eq 80
  ```

작업 정의(Layer 3/4 정책 맵)

트래픽을 식별할 Layer 3/4 클래스 맵을 구성한 후에는 Layer 3/4 정책 맵을 사용하여 작업을 해당 클래스에 연결합니다.

팁 최대 정책 맵 수는 64이지만 인터페이스당 정책 맵을 하나만 적용할 수 있습니다.

절차

1단계 정책 맵을 추가합니다.

policy-map *policy_map_name*

policy_map_name 인수는 길이 최대 40자의 정책 맵 이름입니다. 모든 유형의 정책 맵은 동일한 네임스페이스를 사용하므로, 다른 정책 맵 유형에서 사용된 이름을 재사용할 수 없습니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

예:

```
hostname(config)# policy-map global_policy
```

2단계 전에 구성한 Layer 3/4 클래스 맵을 지정합니다. 여기서 *class_map_name*은 클래스 맵의 이름입니다.

class *class_map_name*

클래스 맵을 추가하려면 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

참고 클래스 맵에 **match default-inspection-traffic** 명령이 없으면 하나의 **inspect** 명령만 클래스 아래에서 구성할 수 있습니다.

class *class_map_name*

예:

```
hostname(config-pmap)# description global policy map
```

3단계 이 클래스 맵에 대해 하나 이상의 작업을 지정합니다.

1-4 페이지의 서비스 정책으로 구성된 기능 섹션을 참조하십시오.

4단계 이 정책 맵에 포함할 각 클래스 맵에 대해 이 프로세스를 반복합니다.

예

다음은 연결 정책용 **policy-map** 명령의 예로, 웹 서버 10.1.1.1에 대해 허용된 연결 수를 제한합니다.

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

다음 예는 정책 맵에서 multi-match의 작동 방식을 보여줍니다.

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout idle 0:10:0
```

다음 예는 첫 번째 사용 가능한 클래스 맵으로 트래픽을 확인하고, 동일한 기능 도메인에서 작업을 지정하는 이후의 클래스 맵으로는 확인하지 않는 방법을 보여줍니다.

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout idle 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout idle 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout idle 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

텔넷 연결이 시작되면 **class telnet_traffic**을 확인합니다. 마찬가지로 FTP 연결이 시작되면 **class ftp_traffic**을 확인합니다. 텔넷 및 FTP 이외의 TCP 연결에서는 **class tcp_traffic**을 확인합니다. 텔넷 또는 FTP 연결에서 **class tcp_traffic**을 확인할 수 있더라도, 전에 다른 클래스에서 일치를 확인했으므로 ASA는 이 일치를 수행하지 않습니다.

인터페이스에 작업 적용(서비스 정책)

Layer 3/4 정책 맵을 활성화하려면 이 맵을 하나 이상의 인터페이스에 적용하거나 모든 인터페이스에 전체적으로 적용하는 서비스 정책을 만드십시오. 다음 명령을 사용합니다.

service-policy *policy_map_name* {**global** | **interface** *interface_name*} [**fail-close**]

여기서 각 항목은 다음을 나타냅니다.

- *policy_map_name*은 정책 맵의 이름입니다.
- **global**은 특정 정책을 가지지 않은 모든 인터페이스에 적용되는 서비스 정책을 만듭니다.

  글로벌 정책은 하나만 적용할 수 있으므로, 글로벌 정책을 변경하려면 기본 정책을 편집하거나 비활성화한 후 새 정책을 적용해야 합니다. 기본적으로 이 컨피그레이션은 모든 기본 애플리케이션 검사 트래픽과 일치하는 글로벌 정책을 포함하며 전체적으로 트래픽에 검사를 적용합니다. 기본 서비스 정책은 **service-policy global_policy global** 명령을 포함합니다.
- **interface** *interface_name*은 정책 맵을 인터페이스와 연결하여 서비스 정책을 만듭니다.

- **fail-close**는 IPv6 트래픽을 지원하지 않는 애플리케이션 검사에 의해 삭제되는 IPv6 트래픽에 대해 syslog(767001)를 생성합니다. 기본적으로 syslog는 생성되지 않습니다. IPv6을 지원하는 검사 리스트는 1-8 페이지의 IPv6 지침을 참조하십시오.

예

예를 들어 다음 명령은 외부 인터페이스에서 inbound_policy 정책 맵을 활성화합니다.

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

다음 명령은 기본 글로벌 정책을 비활성화하고, 다른 모든 ASA 인터페이스에서 new_global_policy라는 새로운 정책을 활성화합니다.

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

서비스 정책 모니터링

서비스 정책을 모니터링하려면 다음 명령을 입력합니다.

- **show service-policy**

  서비스 정책 통계를 표시합니다.

서비스 정책의 예(Modular Policy Framework)

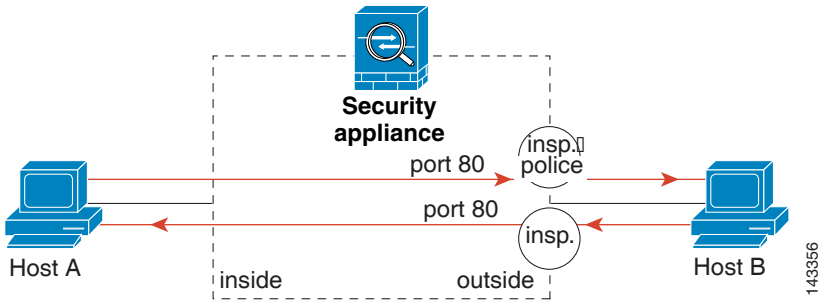
이 섹션에는 몇 가지 Modular Policy Framework 예가 포함되어 있습니다.

- 1-18 페이지의 검사 및 QoS 폴리싱을 HTTP 트래픽에 적용
- 1-19 페이지의 HTTP 트래픽에 전체적으로 검사 적용
- 1-19 페이지의 HTTP 트래픽에 대한 검사 및 연결 제한을 특정 서버에 적용
- 1-20 페이지의 NAT로 HTTP 트래픽에 검사 적용

검사 및 QoS 폴리싱을 HTTP 트래픽에 적용

이 예에서는 외부 인터페이스를 통해 ASA로 드나드는 HTTP 연결(포트 80의 TCP 트래픽)이 HTTP 검사를 위해 분류됩니다. 외부 인터페이스에서 빠져나오는 HTTP 트래픽은 폴리싱을 위해 분류됩니다.

그림 1-1 HTTP 검사 및 QoS 폴리싱



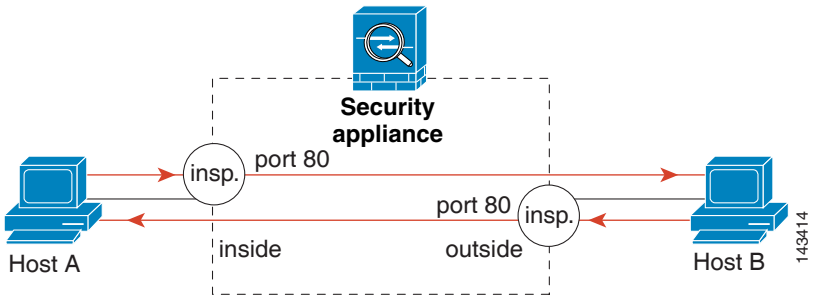
이 예의 다음 명령을 참조하십시오.

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

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside
```

HTTP 트래픽에 전체적으로 검사 적용

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

그림 1-2 글로벌 HTTP 검사



이 예의 다음 명령을 참조하십시오.

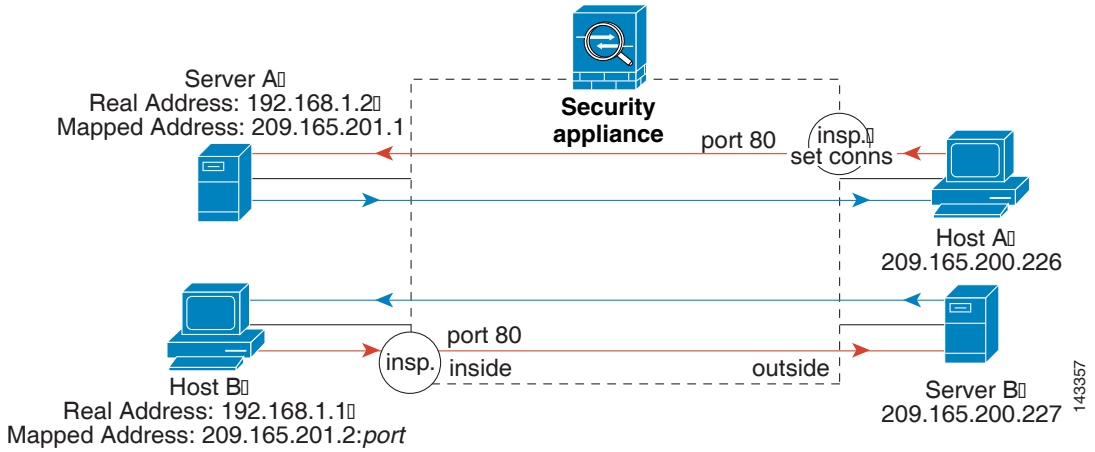
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

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

HTTP 트래픽에 대한 검사 및 연결 제한을 특정 서버에 적용

이 예에서는 외부 인터페이스를 통해 ASA로 들어오는 Server A에 대한 HTTP 연결(포트 80의 TCP 트래픽)이 HTTP 검사 및 최대 연결 제한을 위해 분류됩니다. Server A에서 Host A로의 연결은 클래스 맵의 ACL에서 확인하지 않으므로 영향을 받지 않습니다.

내부 인터페이스를 통해 ASA로 들어가는 Server B에 대한 모든 HTTP 연결은 HTTP 검사를 위해 분류됩니다. Server B에서 Host B로의 연결은 클래스 맵의 ACL에서 확인하지 않으므로 영향을 받지 않습니다.

그림 1-3 특정 서버에 대한 HTTP 검사 및 연결 제한



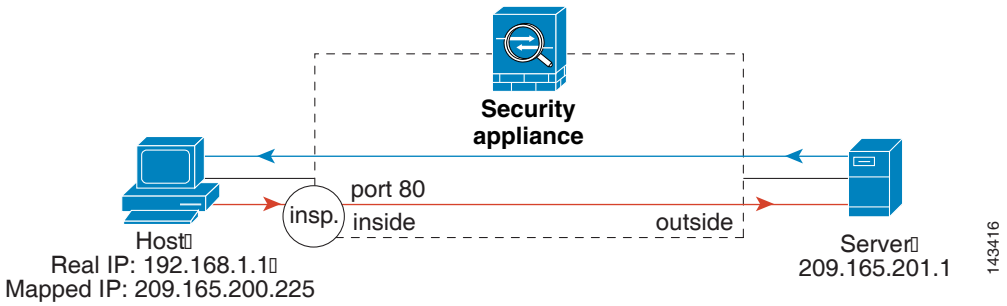
이 예의 다음 명령을 참조하십시오.

```
hostname(config)# object network obj-192.168.1.2
hostname(config-network-object)# host 192.168.1.2
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1
hostname(config)# object network obj-192.168.1.0
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 eq 80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

NAT로 HTTP 트래픽에 검사 적용

이 예에서 내부 네트워크의 Host에는 두 개의 주소가 있습니다. 하나는 실제 IP 주소 192.168.1.1이고 다른 하나는 외부 네트워크에서 사용되는 매핑된 IP 주소 209.165.200.225입니다. 클래스 맵의 ACL에서는 실제 IP 주소를 사용해야 합니다. 이를 외부 인터페이스에 적용한 경우에도 실제 주소를 사용하게 됩니다.

그림 1-4 NAT를 이용한 HTTP 검사



이 예의 다음 명령을 참조하십시오.

```
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1,outside) static 209.165.200.225

hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 any eq 80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client

hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```

서비스 정책의 기록

기능 이름	릴리스	설명
Modular Policy Framework	7.0(1)	Modular Policy Framework가 추가되었습니다.
RADIUS 어카운팅 트래픽과 사용할 관리 클래스 맵	7.2(1)	RADIUS 어카운팅 트래픽과 함께 사용할 수 있도록 관리 클래스 맵이 추가되었습니다. 추가된 명령: **class-map type management**, and **inspect radius-accounting**.
검사 정책 맵	7.2(1)	검사 정책 맵이 추가되었습니다. 추가된 명령: **class-map type inspect**.
정규식 및 정책 맵	7.2(1)	검사 정책 맵에서 사용할 수 있도록 정규식과 정책 맵이 추가되었습니다. 추가된 명령: **class-map type regex**, **regex**, **match regex**.
검사 정책 맵을 위한 Match any	8.0(2)	검사 정책 맵과 사용할 수 있도록 **match any** 키워드가 추가되었습니다. 트래픽이 하나 이상의 기준을 충족하면 클래스 맵과 일치합니다. 전에는 **match all**만 사용 가능했습니다.

2 장

애플리케이션 검사를 위한 특별 작업 (검사 정책 맵)

Modular Policy Framework를 사용하면 많은 애플리케이션 검사에 대한 특별 작업을 구성할 수 있습니다. Layer 3/4 정책 맵에서 검사 엔진을 활성화할 때 *검사 정책 맵*에서 정의한 대로 선택적으로 작업을 활성화할 수도 있습니다. 검사 정책 맵이 검사 작업을 정의한 Layer 3/4 클래스 맵 내의 트래픽과 일치하면, 해당 트래픽 하위 집합은 지정된 대로 작동합니다(예: 삭제됨 또는 속도가 제한됨).

검사 정책 맵에 대한 정보

검사 정책 맵을 지원하는 애플리케이션 리스트는 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

검사 정책 맵은 다음과 같은 요소 중 하나 이상으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 옵션은 애플리케이션에 따라 다릅니다.

- Traffic matching command - 애플리케이션 트래픽을 애플리케이션에 해당하는 기준(예: URL 문자열)과 맞춰본 다음 작업을 활성화할 수 있도록, 검사 정책 맵에서 트래픽 매칭 명령을 직접 정의할 수 있습니다.
  - 일부 트래픽 매칭 명령은 패킷 내부의 텍스트를 확인하기 위해 정규식을 사용할 수 있습니다. 정책 맵을 구성하기 전에, 단독으로 또는 정규식 클래스 맵에서 그룹으로 정규식을 만들고 테스트해야 합니다.
- Inspection class map - 검사 클래스 맵 하나에 여러 트래픽 매칭 명령을 포함할 수 있습니다. 그러면 정책 맵에서 클래스 맵을 식별하고 해당 클래스 맵에 대해 전체적으로 작업을 활성화할 수 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다. 그러나 서로 다른 일치에 대해 서로 다른 작업을 설정할 수는 없습니다. **참고:** 모든 검사가 검사 클래스 맵을 지원하는 것은 아닙니다.
- Parameters - 검사 엔진의 동작에 영향을 미칩니다.

지침 및 제한

- HTTP 검사 정책 맵 - 사용 중인 HTTP 검사 정책 맵을 수정하려는 경우(**policy-map type inspect http**), 변경 사항을 적용하려면 **inspect http** *map* 작업을 제거한 후 다시 적용해야 합니다. 예를 들어, "http-map" 검사 정책 맵을 수정하려면 해당 맵을 제거하고, , 검사 정책 맵을 서비스 Layer 3/4 정책의 **inspect http http-map** 명령

```
hostname(config)# policy-map test
hostname(config-pmap)# class http
hostname(config-pmap-c)# no inspect http http-map
hostname(config-pmap-c)# inspect http http-map
```

- 모든 검사 정책 맵 - 사용 중인 검사 정책 맵을 다른 맵 이름으로 교체하려면 해당 맵을 제거하고, **inspect** *protocol map* 명령을 이용해 새 맵으로 다시 추가합니다. 예:

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

- 여러 검사 클래스 검사 정책 맵에서 **class** 또는 **match** 명령을 직접 맞춰볼 수도 있습니다.

  패킷이 서로 다른여러 **match** 또는 **class** 명령과 일치하는 경우 ASA에서 작업을 적용하는 순서는 내부 ASA 규칙에 의해 결정되며, 검사 정책 맵에 추가된 순서에 의해 결정되지 않습니다. 내부 규칙은 애플리케이션 유형 및 패킷 분석의 논리적 진행에 의해 결정되며, 사용자가 구성할 수 없습니다. 예를 들어 HTTP 트래픽의 경우, Request Method 필드 분석이 Header Host Length 필드 분석을 선행합니다. Header Host Length 필드에 대한 작업이 수행되기 전에 Request Method 필드에 대한 작업이 수행됩니다. 예를 들어 다음의 일치 명령을 임의의 순서로 입력할 수 있지만 **match request method get** 명령이 가장 먼저 적용됩니다.

```
match request header host length gt 100
  reset
match request method get
  log
```

  작업에서 패킷을 삭제하는 경우 검사 정책 맵에서 추가 작업이 수행되지 않습니다. 예를 들어, 첫 번째 작업에서 연결을 재설정하면 추가 **class** 또는 **match** 명령이 적용되지 않습니다. 첫 번째 작업에서 패킷을 기록하면, 두 번째 작업(예: 연결 재설정)이 발생할 수 있습니다.

  패킷에 동일한 여러 **match** 또는 **class** 명령이 있는 경우 논리 맵에 나타나는 순서대로 적용됩니다. 예를 들어, 헤더 길이가 1001인 패킷의 경우 아래의 첫 번째 명령이 적용되고, 기록되고, 두 번째 명령이 적용된 후 재설정됩니다. 두 **match** 명령의 순서를 바꾸면, 두 번째 **match** 명령이 적용되기 전에 패킷이 삭제되고 연결이 재설정됩니다. 따라서 기록이 진행되지 않습니다.

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

  클래스 맵은 클래스 맵 내 최저 우선 순위 **match** 명령을 기준으로 다른 클래스 맵 또는 **match** 명령과 동일한 유형으로 확인됩니다(우선 순위는 내부 규칙을 기반으로 함). 한 클래스 맵에 다른 클래스 맵과 동일한 유형의 최저 우선 순위 **match** 명령이 있으면, 정책 맵에 추가된 순서대로 클래스 맵이 적용됩니다. 각 클래스 맵의 최저 우선 순위 일치가 다른 경우, 더 높은 우선 순위 **match** 명령의 클래스 맵이 먼저 적용됩니다. 예를 들어 다음 3개의 클래스 맵에는 두 가지 유형의 **match** 명령, 즉 **match request-cmd**(더 높은 우선 순위) 및 **match filename**(더 낮은 우선 순위)이 포함되어 있습니다. ftp3 클래스 맵에는 두 명령이 모두 포함되어 있지만, 우선 순위가 가장 낮은 명령인 **match filename**으로 순위가 지정됩니다. ftp1 클래스 맵에는 우선 순위가 가장 높은 명령이 포함되어 있으므로, 정책 맵에서의 순서와 상관없이 가장 먼저 적용됩니다. ftp3 클래스 맵은 역시 **match filename** 명령이 포함된 ftp2 클래스 맵과 동일한 우선 순위가 지정됩니다. 이 둘은 정책 맵의 순서에 따라 적용됩니다(ftp3 -> ftp2).

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

기본 검사 정책 맵

DNS 검사는 preset_dns_map 검사 클래스 맵을 사용하여 기본적으로 활성화됩니다.

- 최대 DNS 메시지 길이는 512바이트입니다.
- 최대 클라이언트 DNS 메시지 길이는 자동으로 리소스 레코드에 맞게 설정됩니다.
- DNS Guard가 사용되므로 ASA에 의해 DNS 회신이 전달되자마자 ASA에서 DNS 쿼리와 관련된 DNS 세션을 해제합니다. ASA는 또한 DNS 회신의 ID가 DNS 쿼리의 ID와 일치하는지 확인하기 위해 메시지 교환을 모니터링합니다.
- NAT 컨피그레이션으로 기반으로 하는 DNS 레코드의 변환이 활성화됩니다.
- 프로토콜 적용이 활성화되고, 이에 따라 DNS 메시지 형식 확인이 활성화됩니다. 여기에는 도메인 이름 길이 최대 255자, 레이블 길이 63자, 압축 및 반복되는 포인터 확인 등이 포함됩니다.

다음의 기본 명령을 참조하십시오.

```
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
```

참고 다른 기본 검사 정책 맵(예: **_default_esmtp_map**)도 있습니다. 예를 들어, **inspect esmtp**는 정책 맵 "_default_esmtp_map"을 암시적으로 사용합니다. **show running-config all policy-map** 명령을 사용하면 모든 기본 정책 맵을 표시할 수 있습니다.

검사 정책 맵에서 작업 정의

Layer 3/4 정책 맵에서 검사 엔진을 활성화할 때 검사 정책 맵에서 정의한 대로 선택적으로 작업을 활성화할 수도 있습니다.

자세한 단계

	명령	목적
1단계	(선택 사항) 검사 클래스 맵을 만듭니다.	2-5 페이지의 검사 클래스 맵의 트래픽 식별 섹션을 참조하십시오. 또는 정책 맵 내에서 직접 트래픽을 식별할 수도 있습니다.
2단계	(선택 사항) 정규식을 만듭니다.	정규식을 지원하는 정책 맵 유형은 일반 운영 컨피그레이션 가이드를 참조하십시오.
3단계	**policy-map type inspect** *application policy_map_name* **예:** `hostname(config)# policy-map type inspect http http_policy`	검사 정책 맵을 만듭니다. 검사 정책 맵을 지원하는 애플리케이션 리스트는 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오. *policy_map_name* 인수는 정책 맵의 이름입니다(길이 최대 40자). 모든 유형의 정책 맵은 동일한 네임스페이스를 사용하므로, 다른 정책 맵 유형에서 사용된 이름을 재사용할 수 없습니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.
4단계	다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.	

	class *class_map_name*
	
	예:
	`hostname(config-pmap)# class http_traffic`
	`hostname(config-pmap-c)#`
		2-5 페이지의 검사 클래스 맵의 트래픽 식별에서 만든 검사 클래스 맵을 지정합니다.
		모든 애플리케이션이 검사 클래스 맵을 지원하는 것은 아닙니다.

	검사 장의 각 애플리케이션에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다.
	
	예:
	`hostname(config-pmap)# match req-resp content-type mismatch`
	`hostname(config-pmap-c)#`
		match not 명령을 사용하는 경우 **match not** 명령의 기준과 일치하는 트래픽에 작업이 적용되지 않습니다.
		정규식을 지원하는 정책 맵 유형은 일반 운영 컨피그레이션 가이드를 참조하십시오.

5단계	*action* **예:** `hostname(config-pmap-c)# drop-connection log`	일치하는 트래픽에 대해 수행할 작업을 지정합니다. 작업은 검사 및 일치 유형에 따라 다릅니다. 일반적인 작업에는 **drop**, **log** 및 **drop-connection**이 있습니다. 각 일치에 대해 사용 가능한 작업은 해당 검사 장을 참조하십시오.

6단계	**parameters**
	
	예:
	`hostname(config-pmap)# parameters`
	`hostname(config-pmap-p)#`
		검사 엔진에 영향을 미치는 매개변수를 구성합니다. CLI가 매개변수 컨피그레이션 모드로 들어갑니다. 각 애플리케이션에 대해 사용 가능한 매개변수는 해당 검사 장을 참조하십시오.

예

다음은 HTTP 검사 정책 맵 및 관련 클래스 맵의 예입니다. 이 정책 맵은 서비스 정책에 의해 활성화되는 Layer 3/4 정책 맵에 의해 활성화됩니다.

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test (a Layer 3/4 class map not shown)
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy test interface outside
```

검사 클래스 맵의 트래픽 식별

이 클래스 맵 유형을 사용하면 애플리케이션에 해당하는 기준을 맞춰볼 수 있습니다. 예를 들어 DNS 트래픽의 경우 DNS 쿼리에서 도메인 이름을 맞춰볼 수 있습니다.

하나의 클래스 맵에서 여러 트래픽 일치를 그룹화하거나(match-all 클래스 맵), 일치 리스트 중 하나를 확인할 수 있습니다(match-any 클래스 맵). 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 여러 일치 명령을 그룹화하고 클래스 맵을 재사용할 수 있다는 점입니다. 이 클래스 맵에서 식별하는 트래픽에 대해, 검사 정책 맵에서 연결의 삭제, 재설정 및/또는 기록 등의 작업을 지정할 수 있습니다. 서로 다른 트래픽 유형에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

제한

모든 애플리케이션이 검사 클래스 맵을 지원하는 것은 아닙니다. 지원되는 애플리케이션 리스트는 **class-map type inspect**에 대한 CLI 도움말을 참조하십시오.

자세한 단계

	명령	목적
1단계	(선택 사항) 정규식을 만듭니다.	일반 운영 컨피그레이션 가이드 섹션을 참조하십시오.

2단계	**class-map type inspect** *application* [**match-all** | **match-any**] *class_map_name*
	
	예:
	`hostname(config)# class-map type inspect http http_traffic`
	`hostname(config-cmap)#`
		검사 클래스 맵을 만듭니다. 여기서 *application*은 검사할 애플리케이션입니다. 지원되는 애플리케이션을 알아보려면 지원되는 애플리케이션에 대한 CLI 도움말 또는 7 장, "애플리케이션 계층 프로토콜 검사 시작"을 참조하십시오.
		class_map_name 인수는 클래스 맵의 이름입니다(길이 최대 40자).
		match-all 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다.
		match-any 키워드는 트래픽이 하나 이상의 기준과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다.
		CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

3단계	(선택 사항) **description** *string* 예: `hostname(config-cmap)# description All UDP traffic`	클래스 맵에 설명을 추가합니다.
4단계	애플리케이션에 대해 사용할 수 있는 하나 이상의 **match** 명령을 입력하여 클래스에 포함할 트래픽을 정의합니다.	클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다. 각 애플리케이션에 대해 사용 가능한 **match** 명령은 해당 검사 장을 참조하십시오.

예

다음 예는 모든 기준과 일치해야 하는 HTTP 클래스 맵을 만듭니다.

```
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs
```

다음 예는 기준 중 하나와 일치하면 되는 HTTP 클래스 맵을 만듭니다.

```
hostname(config-cmap)# class-map type inspect http match-any monitor-http
hostname(config-cmap)# match request method get
hostname(config-cmap)# match request method put
hostname(config-cmap)# match request method post
```

다음 학습 내용

검사 정책을 사용하려면 1 장, “Modular Policy Framework를 사용하는 서비스 정책”을 참조하십시오.

검사 정책 맵의 기능 기록

표 2-1에는 이 기능의 릴리스 기록이 나열되어 있습니다.

표 2-1 서비스 정책의 기능 기록

기능 이름	릴리스	기능 정보
검사 정책 맵	7.2(1)	검사 정책 맵이 추가되었습니다. 추가된 명령: **class-map type inspect**.
정규식 및 정책 맵	7.2(1)	검사 정책 맵에서 사용할 수 있도록 정규식과 정책 맵이 추가되었습니다. 추가된 명령: **class-map type regex**, **regex**, **match regex**.
검사 정책 맵을 위한 Match any	8.0(2)	검사 정책 맵과 사용할 수 있도록 **match any** 키워드가 추가되었습니다. 트래픽이 하나 이상의 기준을 충족하면 클래스 맵과 일치합니다. 전에는 **match all**만 사용 가능했습니다.

3 장

액세스 규칙

이 장에서는 액세스 규칙을 사용하여 ASA를 통과하거나 이곳으로 이동하는 네트워크 액세스를 제어하는 방법에 대해 설명합니다. 투명 및 라우팅된 방화벽 모드에서 모두 액세스 규칙을 사용하여 네트워크 액세스를 제어할 수 있습니다. 투명 모드에서는 액세스 규칙(Layer 3 트래픽용) 및 EtherType 규칙(Layer 2 트래픽용)을 모두 사용할 수 있습니다.

참고 또한 관리를 위해 ASA 인터페이스에 액세스하려는 경우 호스트 IP 주소를 허용하는 액세스 규칙이 필요하지 않습니다. 일반 운영 컨피그레이션 가이드에 따라 관리 액세스를 구성하기만 하면 됩니다.

네트워크 액세스 제어

액세스 규칙은 ASA 통과를 허용할 트래픽을 결정합니다. 액세스 제어 정책을 구현하기 위해 함께 작동하는 서로 다른 몇 가지 규칙 레이어가 있습니다.

- 인터페이스에 할당되는 확장 액세스 규칙(Layer 3+ 트래픽) - 인바운드 방향과 아웃바운드 방향에 각기 다른 규칙 집합(ACL)을 적용할 수 있습니다. 확장 액세스 규칙은 소스 및 대상 트래픽 기준을 기반으로 트래픽을 승인하거나 거부합니다.
- 전체적으로 할당되는 확장 액세스 규칙 - 단일 글로벌 규칙 집합을 작성하여 기본 액세스 제어로 사용할 수 있습니다. 글로벌 규칙은 인터페이스 규칙 이후에 적용됩니다.
- 관리 액세스 규칙(Layer 3+ traffic) - 인터페이스에서 전달되는 트래픽(일반적으로 관리 트래픽)을 처리하기 위해 단일 규칙 집합을 적용할 수 있습니다. CLI에서 이러한 규칙은 "제어 평면" 액세스 그룹입니다. 디바이스에서 전달되는 ICMP 트래픽의 경우 ICMP 규칙을 대신 구성할 수 있습니다.
- 인터페이스에 할당되는 EtherType 규칙(Layer 2 트래픽)(투명 방화벽 모드 전용) - 인바운드 방향과 아웃바운드 방향에 각기 다른 규칙 집합을 적용할 수 있습니다. EtherType 규칙은 비 IP 트래픽에 대한 네트워크 액세스를 제어합니다. EtherType 규칙은 EtherType을 기반으로 트래픽을 허용하거나 거부합니다.

투명 방화벽 모드에서는 확장 액세스 규칙, 관리 액세스 규칙, EtherType 규칙을 동일한 인터페이스에서 결합할 수 있습니다.

규칙에 대한 일반 정보

이 섹션의 다음 항목에서는 액세스 규칙 및 EtherType 규칙에 대한 정보를 설명합니다.

인터페이스 액세스 규칙 및 글로벌 액세스 규칙

액세스 규칙을 특정 인터페이스에 적용할 수도 있고 모든 인터페이스에 전체적으로 적용할 수도 있습니다. 글로벌 액세스 규칙을 인터페이스 액세스 규칙과 함께 구성할 수 있습니다. 이 경우 특정 인바운드 인터페이스 액세스 규칙이 항상 일반 글로벌 액세스 규칙보다 먼저 처리됩니다. 글로벌 액세스 규칙은 인바운드 트래픽에만 적용됩니다.

인바운드 및 아웃바운드 규칙

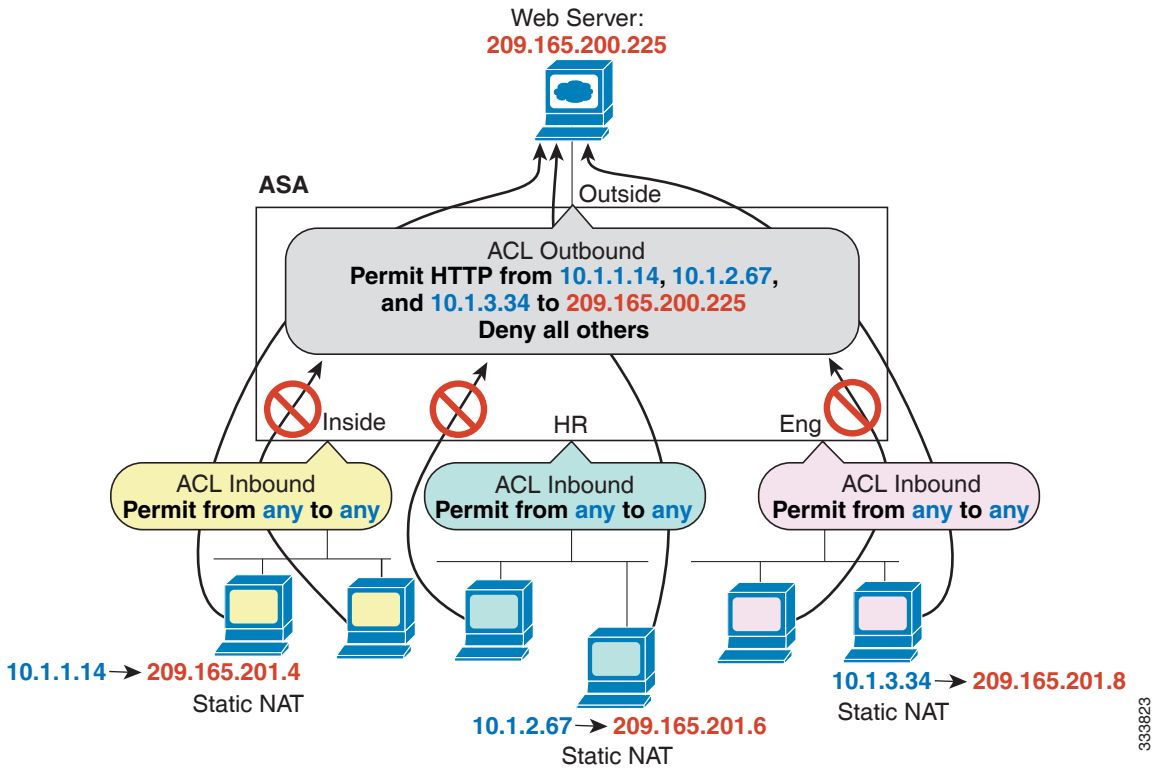
트래픽의 방향을 기반으로 액세스 규칙을 구성할 수 있습니다.

- 인바운드 - 인바운드 액세스 규칙은 인터페이스에 들어가는 트래픽에 적용됩니다. 글로벌 및 관리 액세스 규칙은 항상 인바운드입니다.
- 아웃바운드 - 아웃바운드 규칙은 인터페이스에서 나가는 트래픽에 적용됩니다.

참고 "인바운드" 및 "아웃바운드"는 인터페이스에서 ACL의 적용 방식을 가리킵니다(인터페이스에서 트래픽이 ASA에 들어갈 때 또는 트래픽이 ASA에서 나갈 때). 이러한 용어는 트래픽의 이동, 즉 보안이 더 낮은 인터페이스에서 더 높은 인터페이스로의 이동(일반적으로 인바운드라고 알려짐) 또는 그 반대의 이동(일반적으로 아웃바운드라고 알려짐)을 가리키지 않습니다.

아웃바운드 ACL은 예를 들어 내부 네트워크의 특정 호스트만 외부 네트워크의 웹 서버에 액세스하도록 허용하려는 경우 유용합니다. 액세스 제한을 위해 여러 인바운드 ACL을 만드는 대신 지정된 호스트만 허용하는 단일 아웃바운드 ACL을 만들 수 있습니다. (다음 그림 참조.) 이 아웃바운드 ACL은 다른 호스트가 외부 네트워크에 도달하는 것을 차단합니다.

그림 3-1 아웃바운드 ACL



이 예의 다음 명령을 참조하십시오.

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

규칙 순서

규칙의 순서는 중요합니다. ASA에서 패킷을 전달할지 삭제할지를 결정해야 할 때 ASA는 적용되는 ACL에 나열된 규칙의 순서에 따라 각 규칙을 기준으로 패킷을 테스트합니다. 일치가 발견되면 규칙이 더 이상 점검되지 않습니다. 예를 들어, 시작할 때 인터페이스에 대한 모든 트래픽을 명시적으로 허용하는 액세스 규칙을 만들면 더 이상 다른 규칙이 점검되지 않습니다.

암시적 허용

라우팅된 모드에서는 다음의 트래픽 유형이 기본적으로 허용됩니다.

- 보안이 더 높은 인터페이스에서 더 낮은 인터페이스로의 유니캐스트 IPv4 및 IPv6 트래픽.

투명 모드에서는 다음의 트래픽 유형이 기본적으로 허용됩니다.

- 보안이 더 높은 인터페이스에서 더 낮은 인터페이스로의 유니캐스트 IPv4 및 IPv6 트래픽.

- 양방향의 ARP. (ARP 검사를 사용해 ARP 트래픽을 제어할 수 있지만 액세스 규칙으로는 제어할 수 없습니다.)
- 양방향의 BPDU.

기타 트래픽에는 확장 액세스 규칙(IPv4 및 IPv6) 또는 EtherType 규칙(비 IP)을 사용해야 합니다.

암시적 거부

ACL의 리스트 끝에는 암시적 거부가 있으므로 명시적으로 허용하지 않는 한 트래픽이 통과하지 못합니다. 예를 들어, 특정 주소를 제외하고 모든 사용자가 ASA를 통해 네트워크에 액세스하도록 허용하려면 특정 주소를 거부한 다음 다른 모든 주소를 허용해야 합니다.

EtherType ACL의 경우 ACL 끝의 암시적 거부는 IP 또는 ARP에 영향을 미치지 않습니다. 예를 들어 EtherType 8037을 허용하는 경우 ACL 끝의 암시적 거부는 전에 확장 ACL로 허용한(또는 높은 보안 인터페이스에서 낮은 보안 인터페이스로 암시적으로 허용한) IP 트래픽을 차단하지 않습니다. 그러나 EtherType 규칙으로 모든 트래픽을 명시적으로 거부하면 IP 및 ARP 트래픽은 거부되고, 자동 협상과 같은 물리적 프로토콜 트래픽만 계속 허용됩니다.

글로벌 액세스 규칙을 구성하는 경우 글로벌 규칙이 처리된 *이후* 암시적 거부가 옵니다. 다음의 작동 순서를 참조하십시오.

1. 인터페이스 액세스 규칙.
2. 글로벌 액세스 규칙.
3. 암시적 거부.

NAT 및 액세스 규칙

NAT를 구성한 경우라도, 액세스 규칙은 액세스 규칙 일치를 확인할 때 항상 실제 IP 주소를 사용합니다. 예를 들어 외부에 공개적으로 라우팅 가능한 IP 주소(209.165.201.5)를 가질 수 있도록 내부 서버(10.1.1.5)에 대해 NAT를 구성한 경우, 외부 트래픽이 내부 서버에 액세스하도록 허용하는 액세스 규칙은 매핑된 주소(209.165.201.5)가 아닌 서버의 실제 IP 주소(10.1.1.5)를 참조해야 합니다.

확장 액세스 규칙

이 섹션에서는 확장 액세스 규칙에 대한 정보를 설명합니다.

- 3-4 페이지의 반환 트래픽에 대한 확장 액세스 규칙
- 3-5 페이지의 액세스 규칙을 사용하여 브로드캐스트 및 멀티캐스트 트래픽이 투명 방화벽을 통과하도록 허용
- 3-5 페이지의 관리 액세스 규칙

반환 트래픽에 대한 확장 액세스 규칙

라우팅된 모드 및 투명 모드에 대한 TCP 및 UDP 연결의 경우 반환 트래픽을 허용하기 위한 액세스 규칙이 필요하지 않습니다. ASA는 기존의 양방향 연결에 대한 모든 반환 트래픽을 허용하기 때문입니다.

그러나 ICMP처럼 연결 없는 프로토콜의 경우 ASA는 단방향 세션을 설정하므로, 액세스 규칙에서 ICMP를 양방향으로 허용하거나(소스 및 대상 인터페이스에 ACL을 적용하여) ICMP 검사 엔진을 활성화해야 합니다. ICMP 검사 엔진은 ICMP 세션을 양방향 연결로 취급합니다. Ping을 제어하려면 **echo-reply** (**0**)(ASA에서 호스트로) 또는 **echo** (**8**)(호스트에서 ASA로)을 지정합니다.

액세스 규칙을 사용하여 브로드캐스트 및 멀티캐스트 트래픽이 투명 방화벽을 통과하도록 허용

라우팅된 방화벽 모드에서는 액세스 규칙에서 허용하더라도 브로드캐스트 및 멀티캐스트 트래픽이 차단됩니다. 지원되지 않는 동적 라우팅 프로토콜과 DHCP도 마찬가지입니다(DHCP 릴레이를 구성하지 않는 한). 투명 방화벽 모드에서는 모든 IP 트래픽을 허용할 수 있습니다.

참고 이러한 특수 유형의 트래픽은 연결이 없기 때문에 반환 트래픽이 허용되도록 두 인터페이스에 모두 액세스 규칙을 적용해야 합니다.

다음 표에는 투명 방화벽의 통과를 허용할 수 있는 일반적인 트래픽 유형이 나열되어 있습니다.

표 3-1 투명 방화벽 특별 트래픽

트래픽 유형	프로토콜 또는 포트	참고
DHCP	UDP 포트 67 및 68	사용자가 DHCP 서버를 활성화하면 ASA는 DHCP 패킷을 전달하지 않습니다.
EIGRP	프로토콜 88	—
OSPF	프로토콜 89	—
멀티캐스트 스트림	UDP 포트는 애플리케이션에 따라 달라집니다.	멀티캐스트 스트림은 항상 Class D 주소(224.0.0.0~239.x.x.x)로 이동합니다.
RIP(v1 또는 v2)	UDP 포트 520	—

관리 액세스 규칙

ASA로 이동할 관리 트래픽을 제어하는 액세스 규칙을 구성할 수 있습니다. To-the-box 관리 트래픽(**http**, **ssh**, **telnet** 등의 명령으로 정의)에 대한 액세스 제어 규칙은 **control-plane** 옵션으로 적용한 관리 액세스 규칙보다 우선 순위가 높습니다. 따라서 이렇게 허용된 관리 트래픽은 to-the-box ACL에서 명시적으로 거부하더라도 통과가 허용됩니다.

또는 ICMP 규칙을 사용하여 디바이스에 대한 ICMP 트래픽을 제어할 수 있습니다. ICMP 트래픽의 디바이스 통과를 제어하려면 일반 확장 액세스 규칙을 사용하십시오.

EtherType 규칙

이 섹션에서는 EtherType 규칙에 대해 설명합니다.

- 3-5 페이지의 지원되는 EtherType 및 기타 트래픽
- 3-6 페이지의 반환 트래픽에 대한 EtherType 규칙
- 3-6 페이지의 MPLS 허용

지원되는 EtherType 및 기타 트래픽

EtherType 규칙은 다음을 제어합니다.

- 공통 유형 IPX 및 MPLS 유니캐스트 또는 멀티캐스트를 포함하여 16비트 16진수로 식별되는 EtherType.
- 이더넷 V2 프레임.

- 기본적으로 허용되는 BPDU. BPDU는 SNAP로 캡슐화되며, ASA는 특별히 BPDU를 처리하도록 설계되었습니다.
- 트렁크 포트(Cisco 독점) BPDU. 트렁크 BPDU는 페이로드 내부에 VLAN 정보를 가지고 있으므로, 사용자가 BPDU를 허용하면 ASA는 나가는 VLAN으로 페이로드를 수정합니다.
- IS-IS(Intermediate System to Intermediate System).

다음의 트래픽 유형은 지원되지 않습니다.

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

반환 트래픽에 대한 EtherType 규칙

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

MPLS 허용

MPLS를 허용하는 경우 ASA를 통해 Label Distribution Protocol 및 Tag Distribution Protocol TCP 연결이 설정되도록 해야 합니다. ASA에 연결된 두 MPLS 라우터가 ASA 인터페이스의 IP 주소를 LDP 또는 TDP 세션에 대한 router-id로 사용하도록 구성하면 됩니다. (LDP 및 TDP에서는 MPLS 라우터가 패킷 전달에 사용되는 레이블(주소)을 협상할 수 있습니다.)

Cisco IOS 라우터에서 프로토콜 LDP 또는 TDP에 맞는 적절한 명령을 입력하십시오. *interface*는 ASA에 연결된 인터페이스입니다.

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

또는

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

액세스 제어를 위한 지침

IPv6 지침

IPv6을 지원합니다. 소스 및 수신 주소는 IPv4와 IPv6 주소를 혼합하여 포함할 수 있습니다.

Per-User ACL 지침

- Per-user ACL은 **timeout uauth** 명령의 값을 사용하지만, AAA per-user 세션 시간 제한 값에 의해 재지정될 수 있습니다.
- Per-user ACL 때문에 트래픽이 거부되면 syslog 메시지 109025가 기록됩니다. 트래픽이 허용되면 syslog 메시지가 생성되지 않습니다. Per-user ACL의 **log** 옵션은 효과가 없습니다.

추가 지침 및 제한

- 객체 그룹 검색을 활성화하여 액세스 규칙을 검색하는 데 필요한 메모리를 줄일 수 있지만, 이 경우 조회 성능이 저하됩니다. 객체 그룹 검색을 활성화할 경우 검색이 네트워크 객체로 확장되지 않습니다. 대신 해당 그룹 정의를 기반으로 일치하는 액세스 규칙을 검색합니다. **object-group-search access-control** 명령을 사용하여 이 옵션을 설정할 수 있습니다.

- 액세스 그룹용 트랜잭션 커밋 모델을 사용하여 시스템 성능과 신뢰성을 높일 수 있습니다. 자세한 내용은 일반 운영 컨피그레이션 가이드의 기본 설정 장을 참조하십시오. **asp rule-engine transactional-commit access-group** 명령을 사용하십시오.
- ASDM에서 규칙 설명은 ACL의 규칙 앞에 오는 액세스 목록 리마크(remark)를 기반으로 합니다. ASDM에서 만드는 새로운 규칙의 경우 설명 역시 관련 규칙 앞에서 리마크로 구성됩니다. 그러나 ASDM의 패킷 추적기는 CLI의 일치 규칙 뒤에 구성되는 리마크를 확인합니다.

액세스 제어 구성

다음 항목은 액세스 제어를 구성하는 방법에 대해 설명합니다.

- 3-7 페이지의 액세스 그룹 구성
- 3-8 페이지의 ICMP 액세스 규칙 구성

액세스 그룹 구성

액세스 그룹을 만들려면 먼저 ACL을 만들어야 합니다. 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

ACL을 인터페이스에 바인딩하거나 전체적으로 적용하려면 다음 명령을 사용합니다.

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

예:

```
hostname(config)# access-group outside_access in interface outside
```

인터페이스 전용 액세스 그룹의 경우:

- 확장 또는 EtherType ACL 이름을 지정합니다. ACL당, 인터페이스당, 방향당, 그리고 하나의 제어 평면 ACL당 하나의 **access-group** 명령을 구성할 수 있습니다. 제어 평면 ACL은 확장 ACL이어야 합니다.
- **in** 키워드는 ACL을 인바운드 트래픽에 적용합니다. **out** 키워드는 ACL을 아웃바운드 트래픽에 적용합니다.
- **interface** 이름을 지정합니다.
- **per-user-override** 키워드(인바운드 ACL 전용)는 사용자 권한을 위해 다운로드된 동적 사용자 ACL이 인터페이스에 할당된 ACL을 재지정하도록 허용합니다. 예를 들어, 인터페이스 ACL은 10.0.0.0의 모든 트래픽을 거부하지만 동적 ACL은 10.0.0.0의 모든 트래픽을 허용하는 경우 해당 사용자에 대해 동적 ACL이 인터페이스 ACL을 재지정합니다.

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

  - No **per-user-override**, no **vpn-filter** - 인터페이스 ACL을 기준으로 트래픽을 확인합니다.
  - No **per-user-override**, **vpn-filter** - 처음에는 인터페이스 ACL을 기준으로 트래픽을 확인한 후 VPN 필터를 기준으로 확인합니다.
  - **per-user-override**, **vpn-filter** - VPN 필터만을 기준으로 트래픽을 확인합니다.
- **control-plane** 키워드는 규칙이 to-the-box 트래픽에 대한 것인지를 지정합니다.

글로벌 액세스 그룹의 경우 모든 인터페이스의 인바운드 방향에 확장 ACL을 적용하려면 **global** 키워드를 지정합니다.

예

다음 예는 **access-group** 명령 사용 방법을 보여줍니다.

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access interface outside
```

access-list 명령은 호스트가 포트 80을 사용하여 호스트 주소에 액세스하도록 허용합니다. **access-group** 명령은 **access-list** 명령이 외부 인터페이스에 들어가는 트래픽에 적용되도록 지정합니다.

ICMP 액세스 규칙 구성

기본적으로 IPv4 또는 IPv6을 사용하여 ICMP 패킷을 모든 ASA 인터페이스로 전송할 수 있습니다.

- ASA는 브로드캐스트 주소로 전달되는 ICMP 에코 요청에 응답하지 않습니다.
- ASA는 트래픽이 들어오는 인터페이스로 전송되는 ICMP 트래픽에만 응답합니다. 인터페이스를 통해 먼 인터페이스로 ICMP 트래픽을 전송할 수 없습니다.

디바이스를 공격으로부터 보호하려면 ICMP 규칙을 사용하여 ASA 인터페이스에 대한 ICMP 액세스를 특정 호스트, 네트워크 또는 ICMP 유형으로 제한할 수 있습니다. ICMP 규칙은 액세스 규칙과 같은 방식으로 작동합니다. 규칙의 순서가 정해지고, 패킷과 일치하는 첫 번째 규칙이 작업을 정의합니다.

인터페이스에 대해 ICMP 규칙을 구성하면 ICMP 규칙 리스트의 끝에 암시적 거부 ICMP 규칙이 추가되어 기본 동작이 변경됩니다. 따라서 단지 몇 가지 메시지 유형만 거부하려면 ICMP 규칙 리스트의 끝에 나머지 메시지 유형을 허용하는 허용 규칙을 포함해야 합니다.

ICMP Unreachable 메시지 유형(type 3)은 항상 허용하는 것이 좋습니다. ICMP Unreachable 메시지를 거부하면 ICMP 경로 MTU 검색이 비활성화되고, 그 결과 IPsec 및 PPTP 트래픽이 정지할 수 있습니다. 또한 IPv6 네이버 검색 프로세스에서 IPv6의 ICMP 패킷이 사용됩니다. 경로 MTU 검색에 대한 자세한 내용은 RFC 1195 및 RFC 1435를 참조하십시오.

절차

1단계 ICMP 트래픽에 대한 규칙을 만듭니다.

```
icmp {permit | deny} {host ip_address | ip_address mask | any}
[icmp_type] interface_name
```

*icmp_type*을 지정하지 않으면 규칙이 모든 유형에 적용됩니다. 번호 또는 이름을 입력할 수 있습니다. Ping을 제어하려면 echo-reply (0)(ASA에서 호스트로) 또는 echo (8)(호스트에서 ASA로)을 지정합니다.

주소의 경우 규칙을 **any** 주소, 단일 **host** 또는 네트워크(*ip_address mask*)에 적용할 수 있습니다.

2단계 ICMPv6(IPv6) 트래픽에 대한 규칙을 만듭니다.

```
ipv6 icmp {permit | deny} {host ipv6_address | ipv6-network/prefix-length | any}
[icmp_type] interface_name
```

*icmp_type*을 지정하지 않으면 규칙이 모든 유형에 적용됩니다.

주소의 경우 규칙을 **any** 주소, 단일 **host** 또는 네트워크(*ipv6-network/prefix-length*)에 적용할 수 있습니다.

3단계 (선택 사항) ASA가 traceroute 출력에 나타나도록 ICMP Unreachable 메시지에 대한 속도 제한을 설정합니다.

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

예

```
hostname(config)# icmp unreachable rate-limit 50 burst-size 1
```

속도 제한의 범위는 1~100이며 기본값은 1입니다. Burst size는 의미가 없지만 범위는 1~10이어야 합니다.

ASA를 홉(hop) 중 하나로 표시하는 traceroute를 ASA 전체에서 허용하려면 서비스 정책에서 **set connection decrement-ttl** 명령을 활성화하여 속도 제한을 높여야 합니다. 예를 들어 다음 정책은 ASA 전체에서 모든 트래픽에 대한 TTL(Time-To-Live) 값을 줄입니다.

```
class-map global-class
  match any
policy-map global_policy
  class global-class
  set connection decrement-ttl
```

예

다음 예는 10.1.1.15의 호스트를 제외한 모든 호스트가 내부 인터페이스에 대해 ICMP를 사용하도록 허용하는 방법을 보여줍니다.

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

다음 예는 10.1.1.15의 호스트가 내부 인터페이스에 대해 ping만 사용하도록 허용하는 방법을 보여줍니다.

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

다음 예는 외부 인터페이스에서 모든 ping 요청을 거부하고 모든 packet-too-big 메시지를 허용하는(경로 MTU 검색을 지원하기 위해) 방법을 보여줍니다.

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

다음 예는 호스트 2000:0:0:4::2 또는 접두사 2001::/64의 호스트가 외부 인터페이스에 대해 ping하도록 허용하는 방법을 보여줍니다.

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

액세스 규칙 모니터링

네트워크 액세스를 모니터링하려면 다음 명령을 입력합니다.

- **clear access-list** *id* **counters**

  액세스 리스트에 대한 적중 횟수를 지웁니다.

- **show access-list** [*name*]

  각 ACE의 줄 번호 및 적중 횟수를 비롯한 액세스 리스트를 표시합니다. ACL 이름을 포함하지 않으면 모든 액세스 리스트가 표시됩니다.

- **show running-config access-group**

  인터페이스에 바인딩된 현재 ACL을 표시합니다.

액세스 규칙에 대한 **Syslog** 메시지 평가

액세스 규칙과 관련된 메시지를 보려면 syslog 이벤트 뷰어(예: ASDM에 있는 뷰어)를 사용하십시오.

기본 기록을 사용하면 명시적으로 거부된 흐름에 대해서만 syslog 메시지 106023이 표시됩니다. 규칙 리스트를 종료하는 "implicit deny" 항목과 일치하는 트래픽은 기록되지 않습니다.

ASA가 공격을 받는 경우 거부된 패킷에 대한 syslog 메시지 수가 매우 커질 수 있습니다. 따라서 각 규칙(허용 규칙 포함)에 대한 통계를 제공하며 생성되는 syslog 메시지 수를 제한할 수 있는 syslog 메시지 106100을 사용하는 기록을 대신 활성화하는 것이 좋습니다. 또는 특정 규칙에 대한 모든 기록을 비활성화할 수도 있습니다.

메시지 106100에 대한 기록을 활성화한 경우 패킷이 ACE와 일치하면 ASA는 특정 간격 내에 수신된 패킷 수를 추적하기 위해 흐름 항목을 만듭니다. ASA는 첫 번째 적중 시 및 각 간격의 끝에 syslog 메시지를 생성하여, 간격 중 총 적중 수 및 마지막 적중의 타임스탬프를 표시합니다. 각 간격의 끝에서 ASA는 적중 횟수를 0으로 재설정합니다. 간격 중 ACE와 일치하는 패킷이 없으면 ASA는 흐름 항목을 삭제합니다. 규칙에 대한 기록을 구성할 때 간격은 물론 심지어 규칙당 로그 메시지의 심각도 수준도 제어할 수 있습니다.

흐름은 소스/수신 IP 주소, 프로토콜 및 포트에 의해 정의됩니다. 소스 포트는 동일한 두 호스트 간에도 새 연결에 대해 다를 수 있으므로, 연결에 대해 새 흐름이 생성된 경우 흐름이 동일하게 증가하지 않을 수도 있습니다.

기존 연결에 속하는 허용된 패킷은 ACL에 대해 다시 점검할 필요가 없습니다. 초기 패킷만 기록되고 적중 횟수에 포함됩니다. 연결이 없는 프로토콜(예: ICMP)의 경우 모든 패킷이 기록되며(허용된 패킷이라도), 모든 거부된 패킷도 기록됩니다.

이러한 메시지에 대한 자세한 내용은 *syslog 메시지 가이드*를 참조하십시오.

팁 메시지 106100에 대한 기록을 활성화한 경우 패킷이 ACE와 일치하면 ASA는 특정 간격 내에 수신된 패킷 수를 추적하기 위해 흐름 항목을 만듭니다. ASA는 ACE에 대해 최대 32K 기록 흐름을 가지고 있습니다. 큰 흐름 수가 언제든지 동시에 존재할 수 있습니다. 메모리 및 CPU 리소스의 무제한 소비를 방지하기 위해 ASA에서는 동시 *거부(deny)* 흐름의 수를 제한합니다. 거부 흐름은 공격을 나타낼 수 있기 때문에 거부 흐름에만 제한이 적용됩니다(허가 흐름에는 적용되지 않음). 제한에 도달하면 ASA는 기존 흐름이 만료될 때까지 기록을 위한 새 거부 흐름을 만들지 않고, 메시지 106101을 제공합니다. **access-list alert-interval** *secs* 명령을 사용하여 이 메시지의 빈도를 제어하고, **access-list deny-flow-max** *number* 명령을 사용하여 캐시되는 최대 거부 흐름 수를 제어할 수 있습니다.

네트워크 액세스 허용 또는 거부의 컨피그레이션 예

이 섹션에서는 네트워크 액세스 허용 또는 거부의 일반적인 컨피그레이션 예를 보여줍니다.

다음 예는 inside server 1에 대한 네트워크 객체를 추가하고, 서버에 대해 고정 NAT를 수행하고, 외부에서 inside server 1에 액세스하도록 설정합니다.

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12
```

```
hostname(config)# access-list outside_access extended permit tcp any object inside-server1
eq www
hostname(config)# access-group outside_access in interface outside
```

다음 예는 모든 호스트가 **inside** 및 **hr** 네트워크 간에 통신하되, 특정 호스트만 외부 네트워크에 액세스하도록 허용합니다.

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

예를 들어 다음의 샘플 ACL은 내부 인터페이스에서 시작되는 공통 EtherType을 허용합니다.

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

다음 예는 EtherType ASA를 통한 일부 EtherType만 허용하고 나머지는 모두 거부합니다.

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

다음 예는 EtherType 0x1256의 트래픽을 거부하고 두 인터페이스의 나머지 트래픽은 모두 허용합니다.

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

다음 예는 객체 그룹을 사용하여 내부 인터페이스의 특정 트래픽을 허용합니다.

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

액세스 규칙의 기록

기능 이름	플랫폼 릴리스	설명
인터페이스 액세스 규칙	7.0(1)	ACL을 사용하여 ASA를 통과하는 네트워크 액세스를 제어합니다. 추가된 명령: **access-group**.
글로벌 액세스 규칙	8.3(1)	글로벌 액세스 규칙이 추가되었습니다. 수정된 명령: **access-group.**
아이덴티티 방화벽 지원	8.4(2)	이제 소스 및 대상에 대해 아이덴티티 방화벽 사용자 및 그룹을 사용할 수 있습니다. 액세스 규칙 및 AAA 규칙과 함께, 그리고 VPN 인증에 대해 아이덴티티 방화벽 ACL을 사용할 수 있습니다. 수정된 명령: **access-list extended**.
IS-IS 트래픽에 대해 EtherType ACL 지원	8.4(5), 9.1(2)	투명 방화벽 모드에서 ASA는 이제 EtherType ACL을 사용하여 IS-IS 트래픽을 전달합니다. 수정된 명령: **access-list ethertype {permit | deny} isis**.
TrustSec 지원	9.0(1)	이제 소스 및 대상에 대해 TrustSec 보안 그룹을 사용할 수 있습니다. 액세스 규칙과 함께 아이덴티티 방화벽 ACL을 사용할 수 있습니다. 수정된 명령: **access-list extended**.
IPv4 및 IPv6에 대한 통합 ACL	9.0(1)	ACL이 이제 IPv4 및 IPv6 주소를 지원합니다. 소스 및 대상에 대해 IPv4와 IPv6 주소를 혼합하여 지정할 수도 있습니다. **any** 키워드가 IPv4 및 IPv6 트래픽을 나타내도록 변경되었습니다. IPv4 전용 및 IPv6 전용 트래픽을 나타내도록 **any4** 및 **any6** 키워드가 추가되었습니다. IPv6 전용 ACL은 사용되지 않습니다. 기존의 IPv6 ACL은 확장 ACL로 마이그레이션됩니다. 마이그레이션에 대한 자세한 내용은 릴리스 정보를 참조하십시오. 수정된 명령: **access-list extended**, **access-list webtype**. 제거된 명령: **ipv6 access-list**, **ipv6 access-list webtype**, **ipv6-vpn-filter**

기능 이름	플랫폼 릴리스	설명
확장 ACL 및 객체 향상을 통해 ICMP 코드로 ICMP 트래픽 필터링	9.0(1)	이제 ICMP 코드를 기반으로 ICMP 트래픽을 허용/거부할 수 있습니다. 추가 또는 수정된 명령: **access-list extended, service-object, service**.
액세스 그룹 규칙 엔진에 대한 트랜잭션 커밋 모델	9.1(5)	활성화할 경우 규칙 편집이 완료된 후 규칙 업데이트가 적용되며, 규칙 일치 성능에 영향을 미치지 않습니다. 추가된 명령: **asp rule-engine transactional-commit**, **show running-config asp rule-engine transactional-commit**, **clear configure asp rule-engine transactional-commit**.

파 트 2

네트워크 주소 변환

4 장

NAT(Network Address Translation)

이 장에서는 ASA에서 NAT(Network Address Translation)가 작동하는 방식에 대한 개요를 제공합니다.

참고 NAT 구성을 시작하려면 5 장, “네트워크 객체 NAT”, 또는 6 장, “Twice NAT”를 참조하십시오.

NAT를 사용해야 하는 이유

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지 않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.
- IP 라우팅 솔루션 - NAT를 사용할 때에는 IP 주소 겹치기가 문제가 되지 않습니다.
- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

참고 NAT는 필수 항목이 아닙니다. 특정 트래픽에 대해 NAT를 구성하지 않으면 해당 트래픽은 변환되지 않지만, 모든 보안 정책은 정상적으로 적용됩니다.

NAT 용어

이 설명서는 다음과 같은 용어를 사용합니다.

- 실제 주소/호스트/네트워크/인터페이스 - 실제 주소는 변환되기 전 호스트에서 정의된 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 내부 네트워크가 "실제" 네트워크일 수 있습니다. 내부 네트워크만이 아니라 ASA에 연결된 모든 네트워크를 변환할 수 있습니다. 따라서 외부 주소를 변환하도록 NAT를 구성하면 "실제"는 외부 네트워크(내부 네트워크에 액세스할 때)를 가리킬 수 있습니다.
- 매핑된 주소/호스트/네트워크/인터페이스 - 매핑된 주소는 실제 주소가 변환되는 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 외부 네트워크가 "매핑된" 네트워크일 수 있습니다.

참고 주소 변환 중에, ASA 인터페이스에 상주하는 IP 주소는 변환되지 않습니다.

- 양방향 시작 - 고정 NAT에서는 연결이 *양방향으로* 시작될 수 있습니다(호스트에서 나가기도 하고 호스트로 들어오기도 함).
- 소스(source) 및 수신(destination) NAT - 모든 패킷에 대해 소스 및 수신 IP 주소를 NAT 규칙과 비교하며, 하나 또는 둘 모두를 변환하거나 변환하지 않을 수 있습니다. 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "소스(source)"와 "수신(destination)"이 사용됩니다. 특정 연결이 "수신" 주소에서 시작되는 경우에도 마찬가지입니다.

NAT 형식

다음 항목에서는 다양한 NAT 유형에 대해 설명합니다.

- 4-3 페이지의 NAT 유형 개요
- 4-3 페이지의 고정 NAT
- 4-8 페이지의 동적 NAT
- 4-10 페이지의 동적 PAT
- 4-12 페이지의 아이덴티티 NAT

NAT 유형 개요

다음 방법을 사용하여 NAT를 구현할 수 있습니다.

- 고정(Static) NAT - 실제 IP 주소와 매핑된 IP 주소 간의 일관된 매핑입니다. 양방향 트래픽 시작이 허용됩니다. 4-3 페이지의 고정 NAT 섹션을 참조하십시오.
- 동적(Dynamic) NAT - 실제 IP 주소의 그룹이 매핑된 IP 주소의 그룹(대개 더 작음)에 선착순으로 매핑됩니다. 실제 호스트만 트래픽을 시작할 수 있습니다. 4-8 페이지의 동적 NAT 섹션을 참조하십시오.
- 동적 PAT(Dynamic Port Address Translation) - 실제 IP 주소의 그룹이 해당 IP 주소의 고유한 소스 포트를 사용하여 단일 IP 주소로 매핑됩니다. 4-10 페이지의 동적 PAT 섹션을 참조하십시오.
- 아이덴티티(Identity) NAT - 실제 주소가 기본적으로 NAT를 우회하여 자신에게 고정으로 변환됩니다. 대규모 주소 그룹을 변환하되 좀 더 작은 규모의 주소 하위 집합을 제외하고자 할 경우 이 방법으로 NAT를 구성할 수 있습니다. 4-12 페이지의 아이덴티티 NAT 섹션을 참조하십시오.

고정 NAT

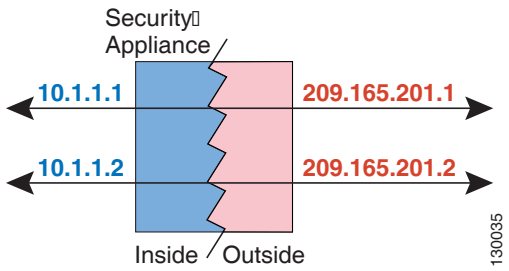
다음 항목에서는 고정 NAT에 대해 설명합니다.

고정 NAT 정보

고정 NAT는 실제 주소에서 매핑된 주소로의 고정된 변환을 생성합니다. 매핑된 주소는 각각의 연속 연결에 대해 동일하므로 NAT는 양방향 연결 시작을 허용합니다. 이를 허용하는 액세스 규칙이 있는 경우 호스트에서 나가기도 하고 호스트로 들어오기도 합니다. 반면 동적 NAT 및 PAT의 경우, 각 호스트는 각 후속 변환에 대해 서로 다른 주소 또는 포트를 사용하므로 양방향 시작이 지원되지 않습니다.

다음 그림은 일반적인 고정 NAT 시나리오를 보여줍니다. 변환이 항상 활성 상태이므로 실제 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 4-1 고정 NAT



참고 원하는 경우 양방향을 비활성화할 수 있습니다.

Static NAT with Port Translation

Static NAT with port translation을 사용하면 실제 및 매핑된 프로토콜(TCP 또는 UDP)과 포트를 지정할 수 있습니다.

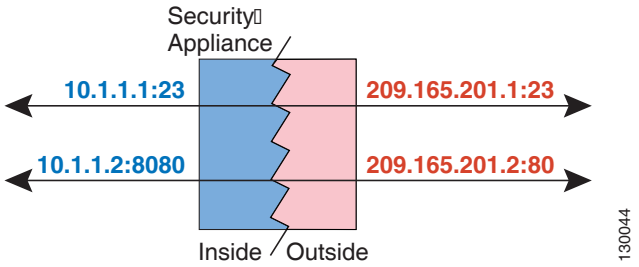
- 4-4 페이지의 Static NAT with PAT(Port Address Translation) 정보
- 4-5 페이지의 Static NAT with Identity Port Translation
- 4-5 페이지의 비표준 포트에 대한 Static NAT with Port Translation
- 4-5 페이지의 Static Interface NAT with Port Translation

Static NAT with PAT(Port Address Translation) 정보

고정 NAT로 포트를 지정하는 경우 포트 및/또는 IP 주소를 동일한 값으로 매핑할지 아니면 다른 값으로 매핑할지를 선택할 수 있습니다.

다음 그림은 자신에게 매핑되는 포트와 다른 값으로 매핑되는 포트 모두를 보여주는 포트 변환 시나리오의 일반적인 고정 NAT를 보여줍니다. 두 경우 모두 IP 주소는 다른 값으로 매핑됩니다. 변환이 항상 활성 상태이므로 변환된 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 4-2 일반적인 Static NAT with Port Translation 시나리오

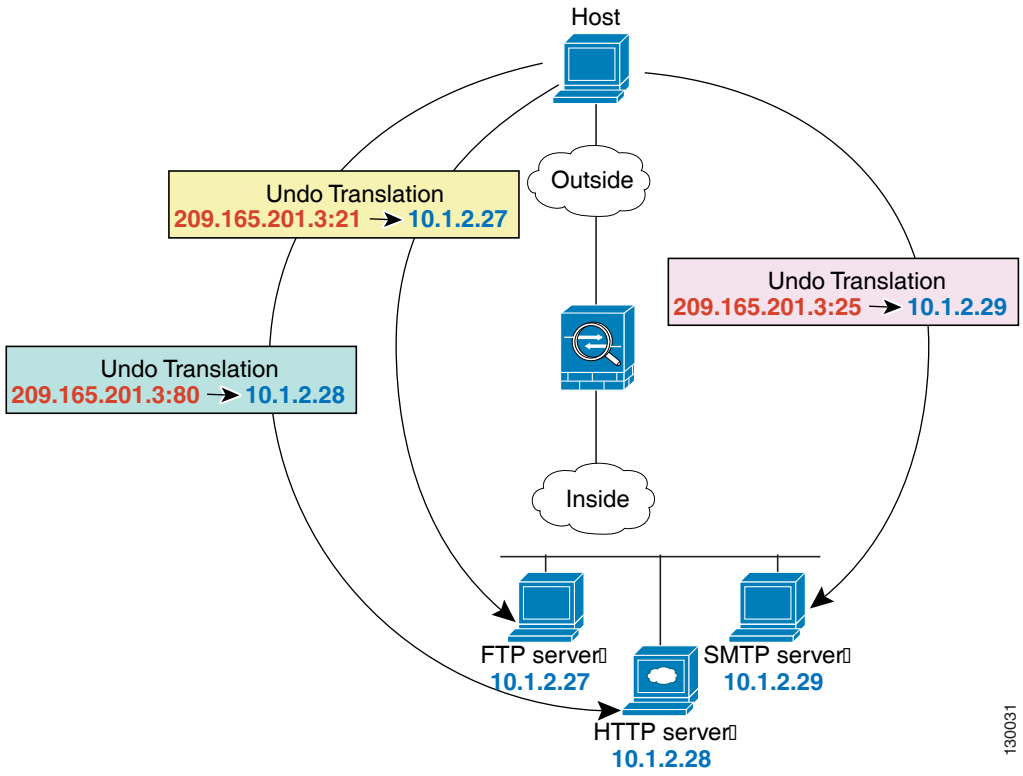


참고 보조 채널(예: FTP 및 VoIP)에 대해 애플리케이션 검사를 요구하는 애플리케이션의 경우 ASA에서는 자동으로 보조 포트를 변환합니다.

Static NAT with Identity Port Translation

다음의 static NAT with port translation 예는 원격 사용자가 FTP, HTTP 및 SMTP에 액세스하기 위해 사용할 단일 주소를 제공합니다. 이러한 서버는 실제 네트워크에서 실제로 서로 다른 디바이스이지만, 각 서버에 대해 동일한 매핑된 IP 주소를 사용하되 포트는 서로 다른 static NAT with port translation 규칙을 지정할 수 있습니다. 이 예의 구성에 대한 자세한 내용은 5-21 페이지의 FTP, HTTP 및 SMTP용 단일 주소(Static NAT-with-Port-Translation) 섹션을 참조하십시오.

그림 4-3 Static NAT with Port Translation



비표준 포트에 대한 Static NAT with Port Translation

잘 알려진 포트를 비표준 포트로 또는 그 반대로 변환하려는 경우에도 static NAT with port translation을 사용할 수 있습니다. 예를 들어 내부 웹 서버가 포트 8080을 사용하는 경우 외부 사용자가 포트 80에 연결하도록 허용한 다음 원래 포트 8080으로의 변환을 취소할 수 있습니다. 마찬가지로, 보안을 강화하려면 웹 사용자에게 비표준 포트 6785로 연결하도록 안내한 다음 포트 80으로의 변환을 취소할 수 있습니다.

Static Interface NAT with Port Translation

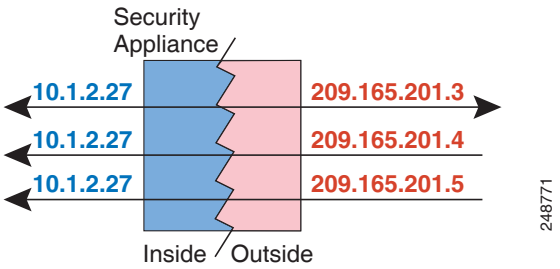
실제 주소를 인터페이스 주소/포트 조합으로 매핑하도록 고정 NAT를 구성할 수 있습니다. 예를 들어 ASA 외부 인터페이스에 대한 텔넷 액세스를 내부 호스트로 리디렉션하려면, 내부 호스트 IP 주소/포트 23을 ASA 인터페이스 주소/포트 23으로 매핑할 수 있습니다. 보안 수준이 가장 낮은 인터페이스에 대해서는 ASA에 대한 텔넷이 허용되지 않지만 static interface NAT with port translation은 텔넷 세션을 거부하는 대신 리디렉션합니다.

일대다 고정 NAT

일반적으로 NAT는 일대일 매핑으로 구성합니다. 그러나 경우에 따라 여러 매핑된 주소에 대해 단일 실제 주소를 구성해야 할 수도 있습니다(일대다). 일대다 고정 NAT를 구성할 경우, 실제 호스트가 트래픽을 시작하면 항상 첫 번째 매핑된 주소를 사용합니다. 그러나 호스트에 대해 시작된 트래픽의 경우, 매핑된 주소 중 하나에 대해 트래픽을 시작할 수 있습니다. 이러한 주소는 단일 실제 주소로 변환되지 않습니다.

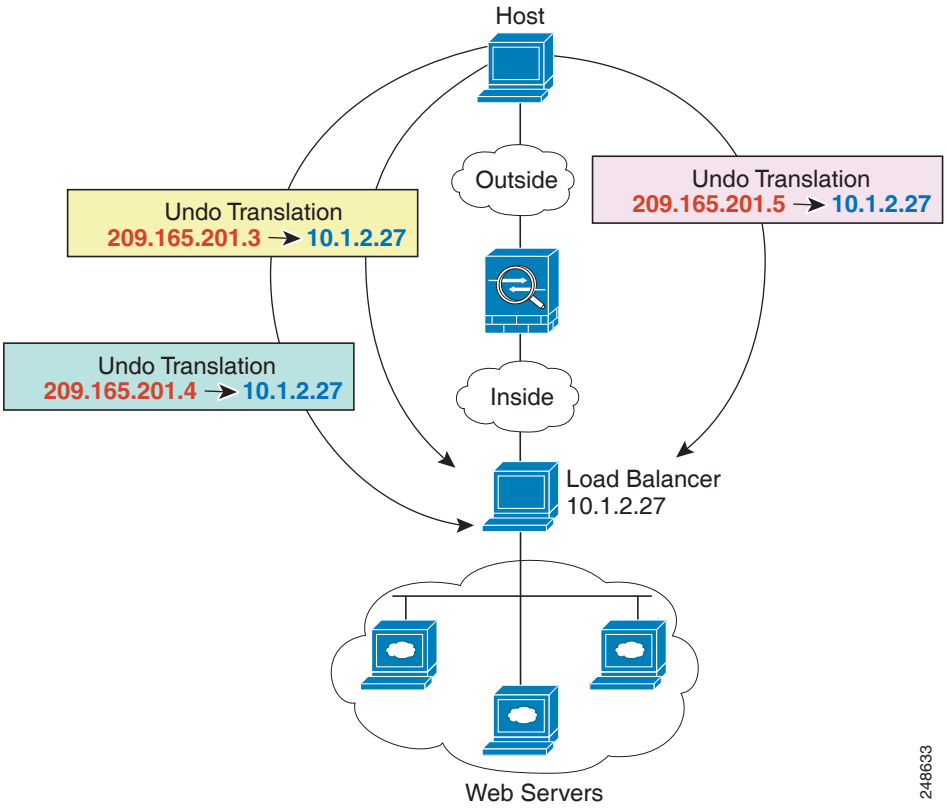
그림 4-4는 일대다 고정 NAT 시나리오를 보여줍니다. 실제 호스트에 의한 시작은 항상 첫 번째 매핑된 주소를 사용하므로, 실제 호스트 IP/첫 번째 매핑된 IP의 변환이 기술적으로 유일한 양방향 변환입니다.

그림 4-4 일대다 고정 NAT



예를 들어 10.1.2.27에 로드 밸런서가 있으면, 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다. 이 예의 구성에 대한 자세한 내용은 5-20 페이지의 여러 매핑된 주소가 있는 내부 로드 밸런서(Static NAT, 일대다) 섹션을 참조하십시오.

그림 4-5 일대다 고정 NAT 예



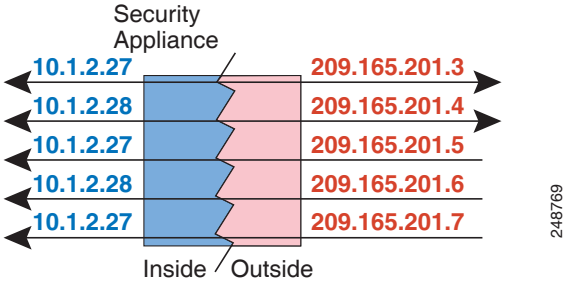
기타 매핑 시나리오(권장되지 않음)

ASA에서는 일대일(one-to-one), 일대다(one-to-many), 소수대다수(few-to-many), 다수대소수(many-to-few), 다대일(many-to-one) 등 모든 종류의 고정 매핑 시나리오를 유연하게 허용합니다. 그러나 일대일 또는 일대다 매핑만 사용하는 것이 좋습니다. 다른 매핑 옵션을 사용할 경우 예기치 않은 결과가 발생할 수 있습니다.

소수대다수(few-to-many)는 기능상 일대다(one-to-many)와 같지만, 컨피그레이션이 좀 더 복잡하고 실제 매핑이 한눈에 명확히 파악되지 않을 수 있으므로 필요한 경우 각 실제 주소에 대해 일대다 컨피그레이션을 만드는 것이 좋습니다. 소수대다수 시나리오에서는 소수의 실제 주소가 다수의 매핑된 주소로 순서대로 매핑됩니다(A-1, B-2, C-3). 모든 실제 주소가 매핑되면 다음의 매핑된 주소는 첫 번째 실제 주소로 매핑되며, 모든 매핑된 주소가 매핑될 때까지 같은 방식이 반복됩니다(A-4, B-5, C-6). 그 결과 각 실제 주소에 다수의 매핑된 주소가 연결됩니다. 일대다 컨피그레이션의 경우와 마찬가지로 첫 번째 매핑만 양방향이고 이후 매핑에서는 실제 호스트*로만* 트래픽이 시작되고, 실제 호스트*로부터의* 모든 트래픽은 소스에 대해 첫 번째 매핑된 주소만 사용합니다.

다음 그림은 일반적인 소수대다수 고정 NAT 시나리오를 보여줍니다.

그림 4-6 소수대다수(Few-to-Many) 고정 NAT

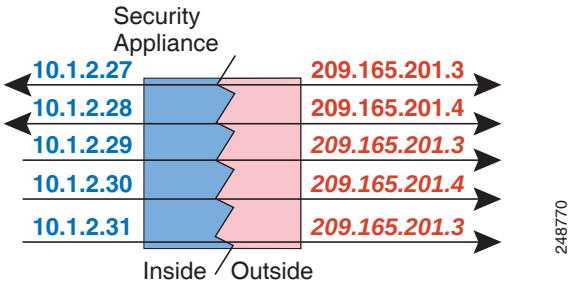


매핑된 주소보다 실제 주소가 더 많은 다수대소수(many-to-few) 또는 다대일 컨피그레이션의 경우, 실제 주소가 소진되기 전에 매핑된 주소가 소진됩니다. 가장 낮은 실제 IP 주소와 매핑된 풀 간의 매핑만 양방향 시작이 가능합니다. 나머지 더 높은 실제 주소는 트래픽을 시작할 수 있지만 이러한 주소로 트래픽이 시작될 수는 없습니다. 연결에 대한 고유한 5개 튜플(source/destination IP address, source/destination port 및 protocol) 때문에 연결에 대한 반환 트래픽은 정확한 실제 주소로 전달됩니다.

참고 다수대소수 또는 다대일 NAT는 PAT가 아닙니다. 두 개의 실제 호스트가 동일한 소스 포트 번호를 사용하고 동일한 외부 서버 및 동일한 TCP 목적지 포트로 이동하며 두 호스트가 동일한 IP 주소로 변환되면, 주소 충돌 때문에(5개 튜플이 고유하지 않음) 두 연결이 재설정됩니다.

다음 그림은 일반적인 다수대소수 고정 NAT 시나리오를 보여줍니다.

그림 4-7 다수대소수(Many-to-Few) 고정 NAT



고정 규칙을 이 방식으로 사용하는 대신, 양방향 시작이 필요한 트래픽에 대해 일대일 규칙을 만든 다음 나머지 주소에 대해 동적 규칙을 만드는 방식을 권장합니다.

동적 NAT

다음 항목에서는 동적 NAT에 대해 설명합니다.

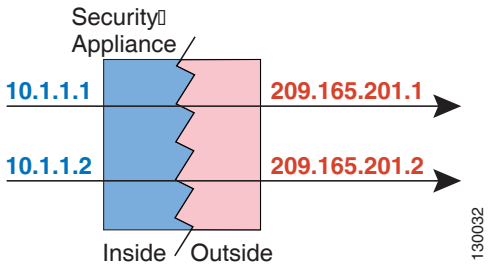
- 4-9 페이지의 동적 NAT 정보
- 4-10 페이지의 동적 NAT 단점 및 장점

동적 NAT 정보

동적 NAT는 실제 주소의 그룹을 수신 네트워크에서 라우팅 가능한 매핑된 주소의 풀로 변환합니다. 매핑된 풀에는 일반적으로 실제 그룹보다 더 적은 수의 주소가 포함되어 있습니다. 변환하려는 호스트가 수신 네트워크에 액세스하면 ASA에서는 매핑된 풀의 IP 주소를 호스트에 할당합니다. 실제 호스트가 연결을 시작하는 경우에만 변환이 생성됩니다. 변환은 연결되어 있는 동안에만 이루어지며, 변환 시간이 초과된 후에는 사용자의 IP 주소가 동일하게 유지되지 않습니다. 따라서 액세스 규칙에서 연결을 허용하더라도, 수신 네트워크의 사용자는 동적 NAT를 사용하는 호스트에 대해 안정적인 연결을 시작할 수 없습니다.

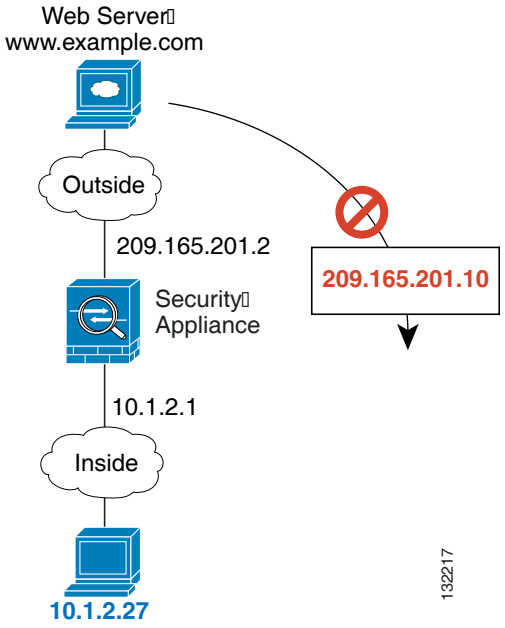
다음 그림은 일반적인 동적 NAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다.

그림 4-8 동적 NAT



다음 그림은 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트를 보여줍니다. 이 주소는 현재 변환 테이블에 있지 않으므로 ASA에서는 패킷을 삭제합니다.

그림 4-9 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트



참고 액세스 규칙에서 허용하는 경우, 변환 기간 동안 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 주소는 예측할 수 없으므로 호스트로의 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

동적 NAT 단점 및 장점

동적 NAT의 단점은 다음과 같습니다.

- 매핑된 풀의 주소 수가 실제 그룹의 주소 수보다 적은 경우, 트래픽의 양이 예상보다 많아지면 주소가 부족해질 수 있습니다.

  PAT는 단일 주소의 포트를 사용하여 64,000이 넘는 변환을 제공하므로, 이러한 상황이 발생하면 PAT 또는 PAT 대안을 사용하십시오.
- 매핑된 풀에서 대량의 라우팅 가능한 주소를 사용해야 하는데, 라우팅 가능한 주소는 대량으로 사용 가능하지 않을 수 있습니다.

동적 NAT의 장점은 일부 프로토콜이 PAT를 사용할 수 없다는 것입니다. PAT는 다음과 작동하지 않습니다.

- GRE 버전 0과 같이 오버로드할 포트가 없는 IP 프로토콜.
- 한 포트에 데이터 스트림이 있고 다른 포트에 제어 경로가 있으며 개방형 표준이 아닌 일부 멀티미디어 애플리케이션.

NAT 및 PAT 지원에 대한 자세한 내용은 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오.

동적 PAT

다음 항목에서는 동적 PAT에 대해 설명합니다.

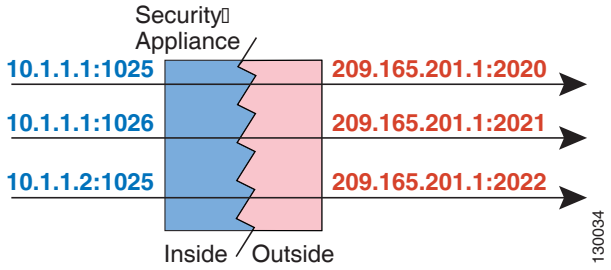
동적 PAT 정보

동적 PAT는 실제 주소 및 소스 포트를 매핑된 주소 및 고유한 포트로 변환함으로써 여러 실제 주소를 단일 매핑된 IP 주소로 변환합니다. 사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 *없*는 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다. 낮은 포트 범위를 사용하는 트래픽이 많은 경우 크기가 서로 다른 세 가지 계층 대신 균일한 포트 범위를 사용하도록 지정할 수 있습니다.

소스 포트는 각 연결에 대해 다르므로 연결마다 별도의 변환 세션이 필요합니다. 예를 들어 10.1.1.1:1025를 사용하려면 10.1.1.1:1026에서 별도로 변환해야 합니다.

다음 그림은 일반적인 동적 PAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다. 매핑된 주소는 각 변환에 대해 동일하지만 포트는 동적으로 할당됩니다.

그림 4-10 동적 PAT



연결이 만료되면 포트 변환도 만료됩니다. Multi-Session PAT의 경우 PAT 시간 제한이 사용됩니다(기본값 30초). Per-Session PAT의 경우 xlate가 즉시 제거됩니다. 액세스 규칙에서 연결을 허용하더라도, 수신 네트워크의 사용자는 PAT를 사용하는 호스트에 대해 안정적으로 연결을 시작할 수 없습니다.

참고 액세스 규칙에서 허용하는 경우, 변환 기간 동안 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 포트 주소(실제 및 매핑된 주소 모두)는 예측할 수 없으므로 호스트에 대한 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

Per-Session PAT 대 Multi-Session PAT

Per-Session PAT는 PAT의 확장성을 개선하며, 클러스터링의 경우 각 멤버 유닛이 PAT 연결을 소유하도록 허용합니다. Multi-Session PAT 연결은 마스터 유닛에서 전달 및 소유해야 합니다. Per-Session PAT 세션이 끝날 무렵 ASA는 재설정을 전송하고 xlate를 즉시 제거합니다. 재설정을 통해 종료 노드에서 연결을 즉시 해제하므로 TIME_WAIT 상태를 피할 수 있습니다. 반면 다중 세션 PAT는 PAT 시간 제한을 사용합니다(기본값 30초).

"hit-and-run" 트래픽(예: HTTP 또는 HTTPS)의 경우 Per-Session PAT는 한 주소에 의해 지원되는 연결 속도를 극적으로 높일 수 있습니다. Per-Session PAT를 사용하지 않으면 IP 프로토콜에 대한 한 주소의 최대 연결 속도는 초당 약 2000입니다. Per-Session PAT를 사용하면 IP 프로토콜에 대한 한 주소의 연결 속도는 65535/*average-lifetime*입니다.

기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽은 Per-Session PAT xlate를 사용합니다. Multi-Session PAT의 혜택을 받을 수 있는 트래픽(예: H.323, SIP 또는 Skinny)의 경우 Per-Session 거부 규칙을 만들어 Per-Session PAT를 비활성화할 수 있습니다. 5-15 페이지의 Per-Session PAT 규칙 구성 섹션을 참조하십시오.

동적 PAT 단점 및 장점

동적 PAT에서는 단일 매핑된 주소를 사용하여 라우팅 가능한 주소를 아낄 수 있습니다. ASA 인터페이스 IP 주소를 PAT 주소로서 사용할 수도 있습니다.

데이터 스트림이 제어 경로와 다른 일부 멀티미디어 애플리케이션에서는 동적 PAT가 작동하지 않습니다. NAT 및 PAT 지원에 대한 자세한 내용은 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오.

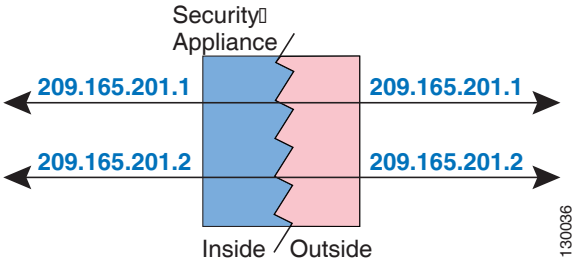
동적 PAT는 단일 IP 주소에서 오는 것처럼 보이는 대량의 연결을 생성할 수 있으며, 서버는 이 트래픽을 DoS 공격으로 해석할 수 있습니다. 주소의 PAT 풀을 구성하고 PAT 주소를 라운드 로빈 방식으로 할당하여 이 상황을 완화할 수 있습니다.

아이덴티티 NAT

IP 주소를 자신으로 변환해야 하는 NAT 컨피그레이션이 있을 수 있습니다. 예를 들어 NAT를 모든 네트워크에 적용하는 광범위한 규칙을 만들되 NAT에서 하나의 네트워크만 제외하고 싶은 경우, 주소를 자신으로 변환하는 고정 NAT 규칙을 만들 수 있습니다. 아이덴티티 NAT는 NAT에서 클라이언트 트래픽을 제외해야 하는 원격 액세스 VPN에 필요합니다.

다음 그림은 일반적인 아이덴티티 NAT 시나리오를 보여줍니다.

그림 4-11 아이덴티티 NAT



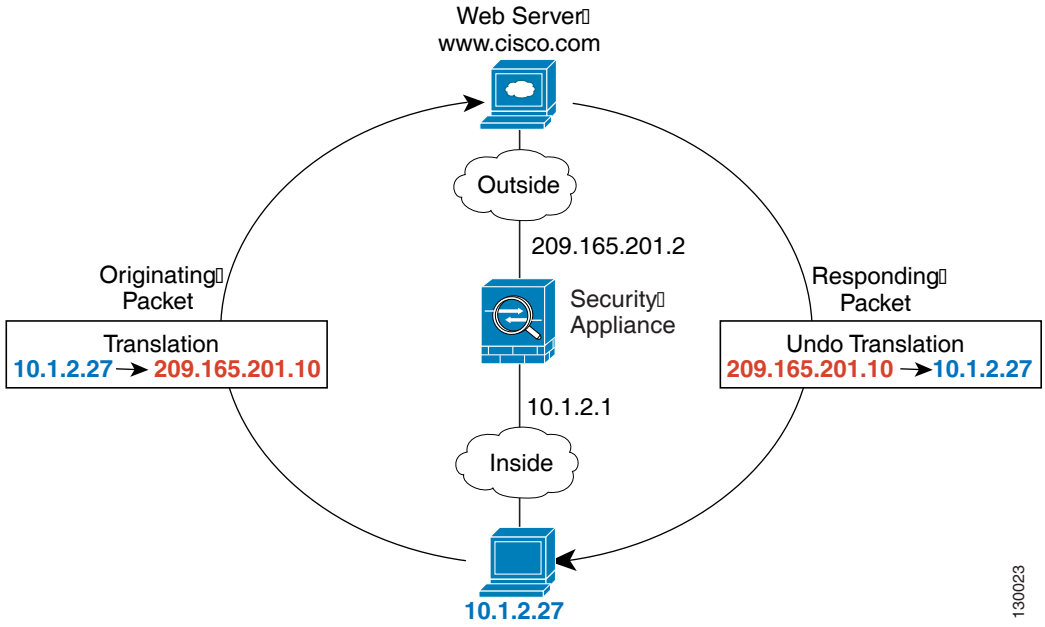
라우팅된 모드 및 투명 모드의 NAT

라우팅된 방화벽 모드와 투명 방화벽 모드에서 모두 NAT를 구성할 수 있습니다. 이 섹션에서는 각 방화벽 모드의 일반적인 사용법에 대해 설명합니다.

라우팅된 모드의 NAT

다음 그림은 내부에 사설 네트워크가 있는 라우팅된 모드의 일반적인 NAT 예를 보여줍니다.

그림 4-12 NAT 예: 라우팅된 모드



1. 10.1.2.27의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.2.27이 매핑된 주소 209.165.201.10으로 변경됩니다.
2. 서버가 응답하면 해당 호스트는 응답을 매핑된 주소 209.165.201.10으로 전송하며 ASA에서 패킷을 수신합니다. ASA에서는 프록시 ARP를 수행하여 패킷을 클레임하기 때문입니다.
3. 그런 다음 ASA에서는 호스트로 전송하기 전에, 매핑된 주소 209.165.201.10에서 다시 실제 주소 10.1.2.27로의 변환을 변경합니다.

투명 모드의 NAT

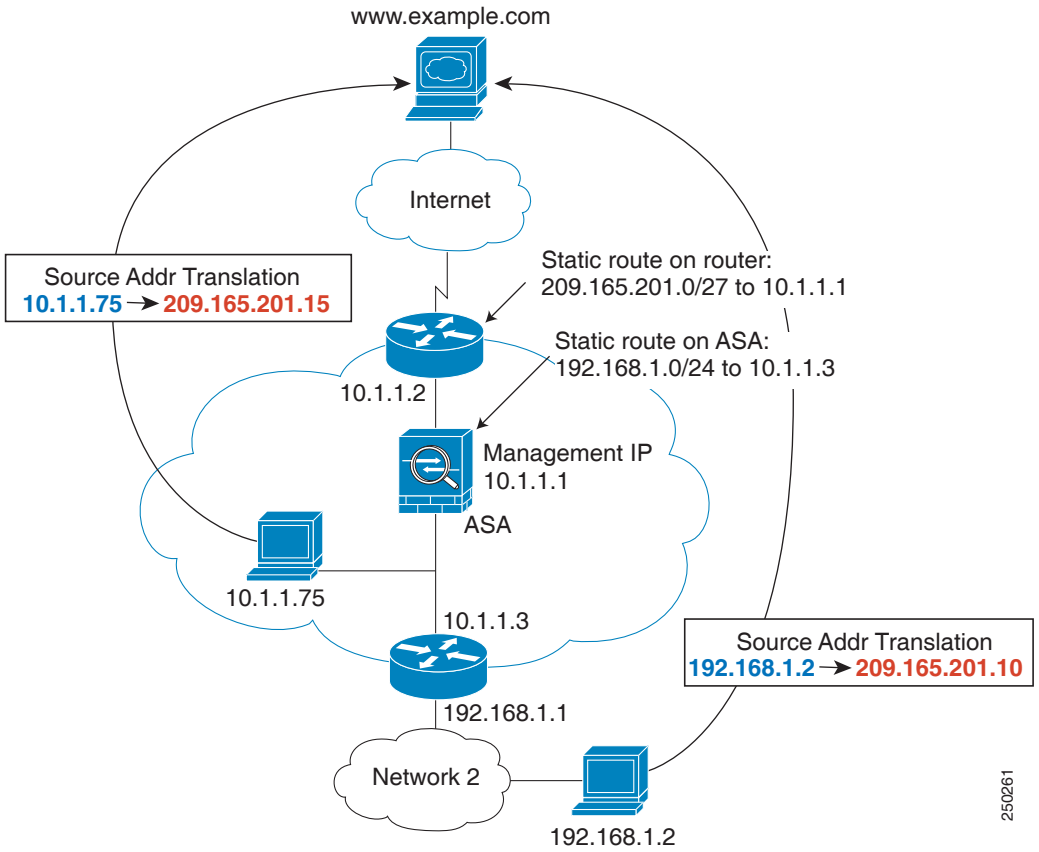
투명 모드에서 NAT를 사용하면 업스트림 또는 다운스트림 라우터가 네트워크에 대해 NAT를 수행할 필요가 없습니다.

투명 모드의 NAT에는 다음과 같은 요구 사항과 제한이 있습니다.

- 투명 방화벽에는 인터페이스 IP 주소가 없으므로 인터페이스 PAT를 사용할 수 없습니다.
- ARP 검사는 지원되지 않습니다. 또한 ASA의 한 쪽에 있는 호스트가 어떤 이유로든 ASA의 다른 쪽에 있는 호스트로 ARP 요청을 전송하고, 시작한 호스트의 실제 주소가 동일한 서브넷의 다른 주소로 매핑되면, ARP 요청에 실제 주소가 가시적으로 남게 됩니다.
- IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 두 IPv6 네트워크 간 변환 또는 두 IPv4 네트워크 간 변환은 지원됩니다.

다음 그림은 내부 인터페이스와 외부 인터페이스의 네트워크가 동일한 투명 모드의 일반적인 NAT 시나리오를 보여줍니다. 이 시나리오의 투명 방화벽은 NAT 서비스를 수행하므로 업스트림 라우터가 NAT를 수행할 필요가 없습니다.

그림 4-13 NAT 예: 투명 모드



1. 10.1.1.75의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.1.75가 매핑된 주소 209.165.201.15로 변경됩니다.
2. 서버가 응답하며 매핑된 주소 209.165.201.15로 응답을 전송하면, ASA에서 패킷을 수신합니다. 업스트림 라우터는 ASA 관리 IP 주소로 연결되는 고정 경로에 이 매핑된 주소를 포함하기 때문입니다. 필수 경로에 대한 자세한 내용은 4-22 페이지의 매핑된 주소 및 라우팅을 참조하십시오.
3. 그런 다음 ASA에서는 매핑된 주소 209.165.201.15에서 다시 실제 주소 10.1.1.1.75로의 변환을 취소합니다. 실제 주소는 직접 연결되어 있으므로 ASA는 호스트로 주소를 직접 전송합니다.
4. 호스트 192.168.1.2에서도 반환 트래픽을 제외하고는 동일한 프로세스가 발생합니다. ASA는 라우팅 테이블에서 경로를 조회하고, 192.168.1.0/24에 대한 ASA 고정 경로를 기반으로 10.1.1.3의 다운스트림 라우터로 패킷을 전송합니다. 필수 경로에 대한 자세한 내용은 4-24 페이지의 원격 네트워크에 대한 투명 모드 라우팅 요구 사항을 참조하십시오.

NAT 및 IPv6

IPv6 네트워크 간 변환 및 IPv4와 IPv6 네트워크 간 변환(라우팅된 모드 전용)을 위해 NAT를 사용할 수 있습니다. 다음의 모범 사례를 권장합니다.

- NAT66(IPv6-to-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(Twice NAT 전용).
- NAT46(IPv4-to-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. IPv6 주소 공간이 IPv4 주소 공간보다 훨씬 크기 때문에 고정 변환을 손쉽게 수용할 수 있습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(Twice NAT 전용). IPv6 서브넷(/96 이하)으로 변환하면 결과로 나타나는 매핑된 주소는 기본적으로 IPv4-embedded IPv6 주소입니다. 이 경우 IPv6 접두사 뒤에 IPv4 주소의 32비트가 포함됩니다. 예를 들어 IPv6 접두사가 /96 접두사이면, 주소의 마지막 32비트에 IPv4 주소가 첨부됩니다. 예를 들어 192.168.1.0/24를 201b::0/96에 매핑하면 192.168.1.4는 201b::0.192.168.1.4(혼합된 표기로 표시됨)에 매핑됩니다. 접두사가 더 작으면(예: /64) IPv4 주소가 접두사 뒤에 첨부되고, 접미사 0이 IPv4 주소 뒤에 첨부됩니다. 선택적으로 주소를 net-to-net으로 변환할 수도 있습니다. 이 경우 첫 번째 IPv4 주소가 첫 번째 IPv6 주소로, 두 번째가 두 번째로 등과 같이 매핑됩니다.
- NAT64(IPv6-to-IPv4) - IPv6 주소의 수를 수용할 만큼 IPv4 주소가 충분하지 않을 수 있습니다. 대량의 IPv4 변환을 제공하려면 동적 PAT 풀을 사용하는 것이 좋습니다.

구현과 관련된 특정 지침 및 제한을 보려면 컨피그레이션 장을 참조하십시오.

NAT 구현 방법

ASA에서는 주소 변환을 두 가지 방법, 즉 *네트워크 객체(Network Object) NAT* 및 *Twice NAT*로 구현할 수 있습니다.

- 4-15 페이지의 네트워크 객체 NAT와 Twice NAT의 주요 차이점
- 4-16 페이지의 네트워크 객체 NAT
- 4-16 페이지의 Twice NAT

네트워크 객체 NAT와 Twice NAT의 주요 차이점

이 두 NAT 유형의 주요 차이점은 다음과 같습니다.

- 실제 주소를 정의하는 방법
  - 네트워크 객체 NAT - NAT를 네트워크 객체의 매개변수로서 정의합니다. 네트워크 객체가 IP 호스트, 범위 또는 서브넷을 명명하므로 NAT 컨피그레이션에서 실제 IP 주소 대신 객체를 사용할 수 있습니다. 네트워크 객체 IP 주소는 실제 주소 역할을 합니다. 이 방법을 사용하면 컨피그레이션의 다른 부분에서 이미 사용 중일 수 있는 네트워크 객체에 NAT를 손쉽게 추가할 수 있습니다.
  - Twice NAT - 실제 주소와 매핑된 주소 모두에서 네트워크 객체 또는 네트워크 객체 그룹을 식별합니다. 이 경우 NAT는 네트워크 객체의 매개변수가 아닙니다. 네트워크 객체 또는 그룹은 NAT 컨피그레이션의 매개변수입니다. 실제 주소에 네트워크 객체 *그룹*을 사용할 수 있으므로 Twice NAT의 확장성이 더 뛰어납니다.

- 소스 및 수신 NAT의 구현 방법.
  - 네트워크 객체 NAT - 각 규칙을 패킷의 소스 주소 또는 수신 주소에 적용할 수 있습니다. 따라서 소스 IP 주소와 수신 IP 주소에 각각 하나씩 두 개의 규칙이 사용될 수 있습니다. source/destination 조합에 특정 변환을 적용하기 위해 이러한 두 규칙을 결합할 수 없습니다.
  - Twice NAT - 단일 규칙이 소스 주소와 수신 주소를 모두 변환합니다. 일치하는 패킷은 하나의 규칙에서만 일치하며, 더 이상 규칙이 점검되지 않습니다. Twice NAT에 대해 선택적인 수신 주소를 구성하지 않더라도 일치하는 패킷이 여전히 하나의 Twice NAT 규칙에서만 일치합니다. 소스와 수신이 결합되어 있으므로, source/destination 조합에 따라 서로 다른 변환을 적용할 수 있습니다. 예를 들어 sourceA/destinationA의 변환은 sourceA/destinationB의 변환과 다를 수 있습니다.
- NAT 규칙의 순서.
  - 네트워크 객체 NAT - NAT 테이블에서 순서가 자동으로 지정됩니다.
  - Twice NAT - NAT 테이블에서 순서를 수동으로 지정합니다(네트워크 객체 NAT 규칙 앞 또는 뒤).

  자세한 내용은 4-20 페이지의 NAT 규칙 순서 섹션을 참조하십시오.

Twice NAT가 제공하는 추가적인 기능이 필요한 경우가 아니면 네트워크 객체 NAT를 사용하는 것이 좋습니다. 네트워크 객체 NAT가 구성이 더 쉽고, VoIP(Voice over IP) 등의 애플리케이션에서 좀 더 안정적입니다. (Twice NAT는 두 객체 간에만 적용되므로 VoIP의 경우 두 객체 중 하나에 속하지 않는 간접 주소를 변환할 때 오류가 발생할 수 있습니다.)

네트워크 객체 NAT

네트워크 객체의 매개변수로서 구성되는 모든 NAT 규칙은 *네트워크 객체 NAT* 규칙으로 간주됩니다. 네트워크 객체 NAT는 단일 IP 주소, 주소 범위 또는 서브넷 등의 네트워크 객체에 대해 NAT를 구성하기 위한 빠르고 쉬운 방법입니다.

네트워크 객체를 구성한 후에는 해당 객체의 매핑된 주소를 인라인 주소로서 식별하거나, 또 다른 네트워크 객체 또는 네트워크 객체 그룹으로서 식별할 수 있습니다.

패킷이 ASA로 들어가면 소스 및 수신 IP 주소 모두에서 네트워크 객체 NAT 규칙의 점검이 수행됩니다. 별도의 일치를 만든 경우 별도의 규칙을 통해 패킷의 소스 및 수신 주소를 변환할 수 있습니다. 이러한 규칙은 서로 연결되어 있지 않습니다. 트래픽에 따라 규칙의 서로 다른 조합을 사용할 수 있습니다.

규칙은 쌍을 이루지 않으므로 sourceA/destinationA가 sourceA/destinationB 이외의 다른 변환을 갖도록 지정할 수 없습니다. 그런 종류의 기능이 필요한 경우 Twice NAT를 사용하십시오. Twice NAT를 사용하면 단일 규칙으로 소스 및 수신 주소를 식별할 수 있습니다.

네트워크 객체 NAT 구성을 시작하려면 5 장, “네트워크 객체 NAT”를 참조하십시오.

Twice NAT

Twice NAT에서는 소스 주소와 수신 주소를 단일 규칙에서 식별할 수 있습니다. 소스 주소와 수신 주소를 모두 지정하면 sourceA/destinationA가 sourceA/destinationB 이외의 다른 변환을 갖도록 지정할 수 있습니다.

수신 주소는 선택 사항입니다. 수신 주소를 지정하는 경우 이를 수신 주소 자신에게 매핑할 수도 있고(아이덴티티 NAT) 다른 주소에 매핑할 수도 있습니다. 수신 주소 매핑은 항상 고정 매핑입니다.

또한 Twice NAT를 사용하는 경우 static NAT with port translation에 대해 서비스 객체를 사용할 수 있습니다. 네트워크 객체 NAT는 인라인 정의만 수용합니다.

Twice NAT 구성을 시작하려면 6 장, “Twice NAT”를 참조하십시오.

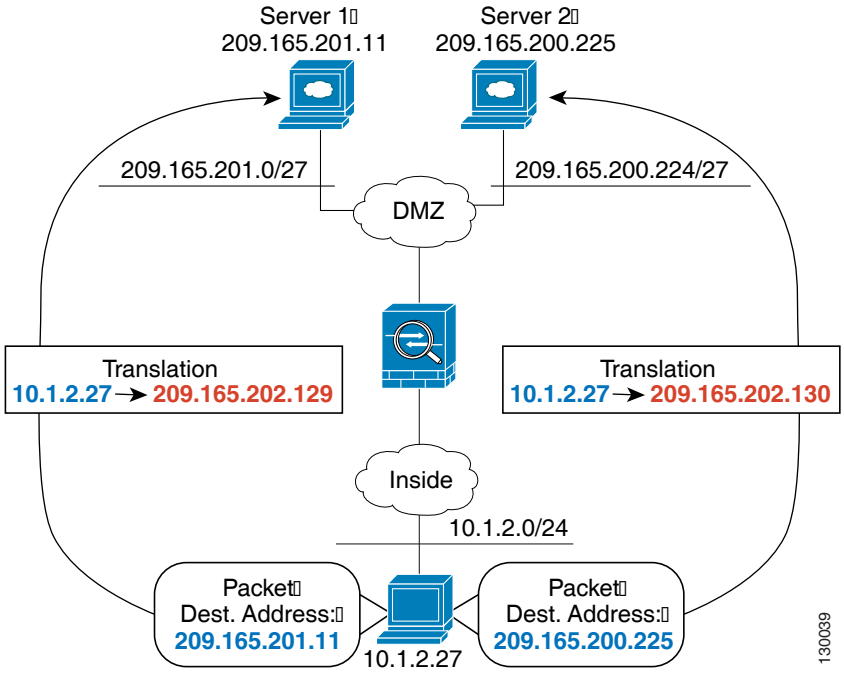
다음 항목에서는 Twice NAT의 몇 가지 예를 제공합니다.

- 4-17 페이지의 예: 서로 다른 수신 주소의 Twice NAT
- 4-18 페이지의 예: 서로 다른 목적지 포트의 Twice NAT
- 4-19 페이지의 예: 수신 주소가 변환되는 Twice NAT

예: 서로 다른 수신 주소의 Twice NAT

다음 그림은 두 개의 서로 다른 서버에 액세스하는 10.1.2.0/24 네트워크의 호스트를 보여줍니다. 호스트가 209.165.201.11의 서버에 액세스하면 실제 주소가 209.165.202.129로 변환됩니다. 호스트가 209.165.200.225의 서버에 액세스하면 실제 주소가 209.165.202.130으로 변환됩니다. 이 예의 구성 방법에 대한 자세한 내용은 5-21 페이지의 FTP, HTTP 및 SMTP용 단일 주소(Static NAT-with-Port-Translation) 섹션을 참조하십시오.

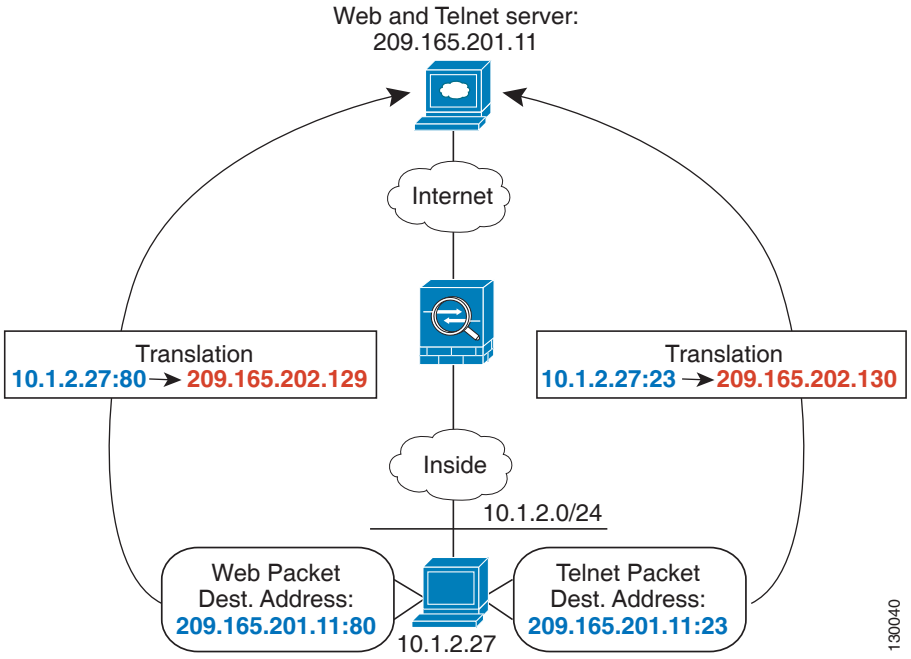
그림 4-14 서로 다른 수신 주소의 Twice NAT



예: 서로 다른 목적지 포트의 Twice NAT

다음 그림은 소스 포트와 목적지 포트의 사용법을 보여줍니다. 10.1.2.0/24 네트워크의 호스트가 웹 서비스와 텔넷 서비스를 모두 제공하는 단일 호스트에 액세스합니다. 호스트가 웹 서비스용 서버에 액세스하면 실제 주소가 209.165.202.129로 변환됩니다. 호스트가 동일한 텔넷 서비스용 서버에 액세스하면 실제 주소가 209.165.202.130으로 변환됩니다.

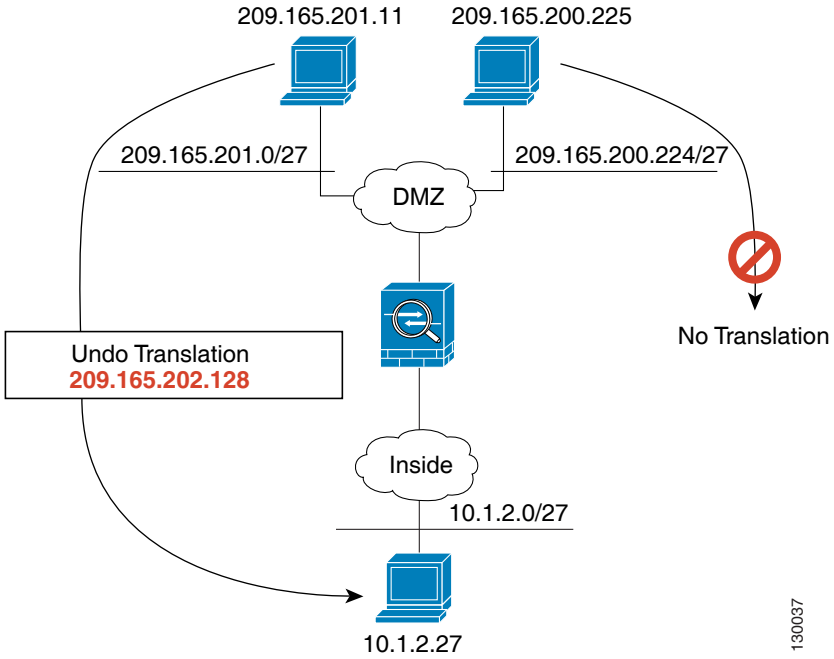
그림 4-15 서로 다른 목적지 포트의 Twice NAT



예: 수신 주소가 변환되는 Twice NAT

다음 그림은 매핑된 호스트에 연결되는 원격 호스트를 보여줍니다. 매핑된 호스트는 209.165.201.0/27 네트워크에서 왕래하는 트래픽에 대해서만 실제 주소를 변환하는 Twice Static NAT 변환을 가지고 있습니다. 209.165.200.224/27 네트워크에 대해서는 변환이 존재하지 않으므로 변환된 호스트를 해당 네트워크에 연결할 수 없고, 해당 네트워크의 호스트를 변환된 호스트에 연결할 수도 없습니다.

그림 4-16 수신 주소가 변환되는 Twice Static NAT



NAT 규칙 순서

네트워크 객체 NAT 규칙과 Twice NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예를 들어 섹션 1에서 일치가 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

표 4-1 NAT 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	Twice NAT	첫 번째 일치부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 Twice NAT 규칙은 섹션 1에 추가됩니다. **참고** EasyVPN remote를 구성하면 ASA에서는 보이지 않는 NAT 규칙을 이 섹션의 끝에 동적으로 추가합니다. 보이지 않는 규칙과 일치하는 대신 VPN 트래픽과 일치할 수 있는 Twice NAT 규칙은 이 섹션에서 구성하지 않아야 합니다. NAT 실패 때문에 VPN이 작동하지 않으면 Twice NAT 규칙을 섹션 3에 추가해볼 수 있습니다.
섹션 2	네트워크 객체 NAT	섹션 1에서 일치가 발견되지 않으면 ASA에서 자동으로 결정한 다음 순서로 섹션 2 규칙이 적용됩니다. 1. 고정 규칙. 2. 동적 규칙. **각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다.** 1. 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 객체가 주소가 10개인 객체보다 먼저 평가됩니다. 2. 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다. 3. IP 주소가 동일한 경우 네트워크 객체의 이름이 알파벳 순으로 사용됩니다. 예를 들면 abracadabra가 catwoman보다 먼저 평가됩니다.
섹션 3	Twice NAT	아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다. 규칙을 추가할 때 Twice NAT 규칙을 섹션 3에 추가할지 여부를 지정할 수 있습니다.

예를 들어 섹션 2 규칙의 경우 네트워크 객체 내에서 다음 IP 주소를 정의합니다.

192.168.1.0/24 (static)

192.168.1.0/24 (dynamic)

10.1.1.0/24 (static)

192.168.1.1/32 (static)

172.16.1.0/24 (dynamic) (object def)

172.16.1.0/24 (dynamic) (object abc)

결과 순서는 다음과 같습니다.

192.168.1.1/32 (static)

10.1.1.0/24 (static)

192.168.1.0/24 (static)

172.16.1.0/24 (dynamic) (object abc)

172.16.1.0/24 (dynamic) (object def)

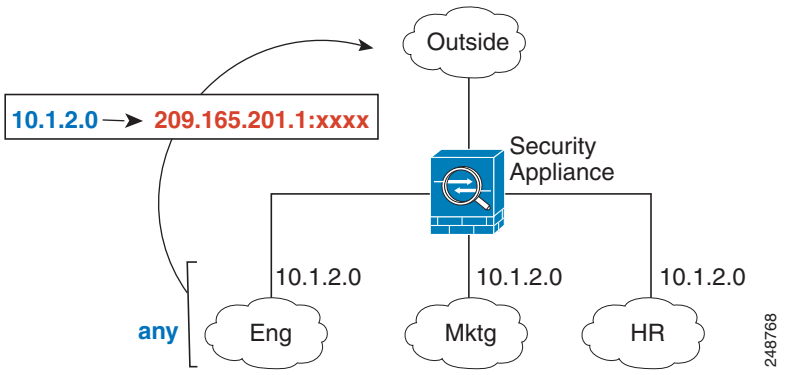
192.168.1.0/24 (dynamic)

NAT 인터페이스

임의의(any) 인터페이스(다시 말하면 모든 인터페이스)에 적용할 NAT 규칙을 구성할 수도 있고, 특정 실제 및 매핑된 인터페이스를 지정할 수도 있습니다. 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 특정 인터페이스를 지정하거나, 그 반대로 지정할 수도 있습니다.

예를 들어, 여러 인터페이스에서 동일한 사설 주소를 사용하며, 외부에 액세스할 때 이들을 모두 동일한 글로벌 풀로 변환하려는 경우 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 외부 인터페이스를 지정할 수 있습니다.

그림 4-17 임의의 인터페이스 지정



참고 투명 모드에서는 특정 소스 및 수신 인터페이스를 선택해야 합니다.

NAT 패킷 라우팅

ASA는 매핑된 주소로 전송된 모든 패킷의 수신지가 되어야 합니다. ASA는 또한 매핑된 주소로 가야 할 수신 패킷에 대한 이그레스(egress) 인터페이스를 결정해야 합니다. 이 섹션에서는 ASA가 NAT를 이용해 패킷을 수락하고 전달하는 방법에 대해 설명합니다.

매핑된 주소 및 라우팅

실제 주소를 매핑된 주소로 변환할 때, 사용자가 선택하는 매핑된 주소가 매핑된 주소용 라우팅(필요한 경우)을 구성하는 방법을 결정합니다.

매핑된 IP 주소에 대한 추가 지침은 5 장, “네트워크 객체 NAT” 및 6 장, “Twice NAT”를 참조하십시오.

다음 항목에서는 매핑된 주소 유형에 대해 설명합니다.

매핑된 인터페이스와 동일한 네트워크의 주소

매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 ASA는 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. ASA가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 이 솔루션은 외부 네트워크에 적절한 수의 여유 주소가 있는 경우 이상적이며, 동적 NAT 또는 고정 NAT 등 1:1 변환을 사용하는 경우 고려해볼 수 있습니다. 동적 PAT는 소수의 주소로 사용 가능한 변환의 수를 크게 확장합니다. 따라서 외부 네트워크에 사용 가능한 주소가 적어도 이 방법을 사용할 수 있습니다. PAT의 경우 매핑된 인터페이스의 IP 주소를 사용할 수도 있습니다.

참고 매핑된 인터페이스를 임의의(any) 인터페이스로 구성하고 동일한 네트워크의 매핑된 주소를 매핑된 인터페이스 중 하나로서 지정하면, 해당 매핑된 주소에 대한 ARP 요청이 *다른* 인터페이스에서 오는 경우 인그레스(ingress) 인터페이스에서 해당 네트워크에 대한 ARP 항목을 수동으로 구성하여 MAC 주소를 지정해야 합니다(의 **arp** 명령 참조). 일반적으로 매핑된 인터페이스에 대해 임의의 인터페이스를 지정하면 매핑된 주소에 대해 고유한 네트워크를 사용하게 되므로 이러한 상황이 발생하지 않습니다.

고유한 네트워크의 주소

매핑된 인터페이스 네트워크에서 사용할 수 있는 것보다 더 많은 주소가 필요한 경우 별도의 서브넷에서 주소를 지정할 수 있습니다. 업스트림 라우터에는 ASA를 가리키는, 매핑된 주소에 대한 고정 경로가 필요합니다. 라우팅된 모드에 대한 대안으로, 수신 네트워크의 IP 주소를 게이트웨이로 사용하여 ASA에서 매핑된 주소에 대해 고정 경로를 구성한 다음 라우팅 프로토콜을 사용하여 경로를 배재포할 수 있습니다. 예를 들어 내부 네트워크(10.1.1.0/24)에 대해 NAT를 사용하고 매핑된 IP 주소 209.165.201.5를 사용하는 경우, 재배포 가능한 다음의 고정 경로를 구성할 수 있습니다.

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

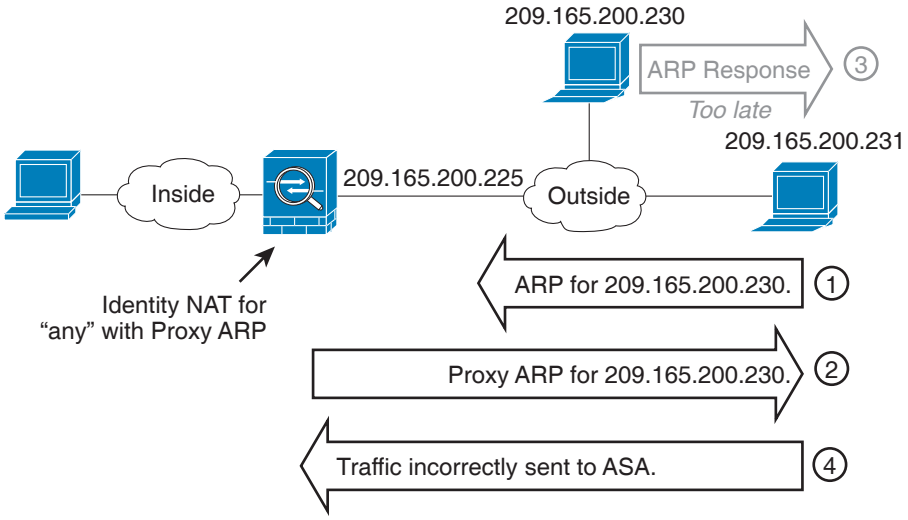
투명 모드에서 실제 호스트가 직접 연결된 경우 8.3에서는 업스트림 라우터의 고정 경로가 브리지 그룹 IP 주소를 지정합니다. 업스트림 라우터의 고정 경로, 투명 모드의 원격 호스트에 대해서는 다운스트림 라우터 IP 주소를 대신 지정할 수 있습니다.

실제 주소와 동일한 주소(아이덴티티 NAT)

아이덴티티 NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 원하는 경우 정기적인 고정 NAT에 대해 프록시 ARP를 비활성화할 수도 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다.

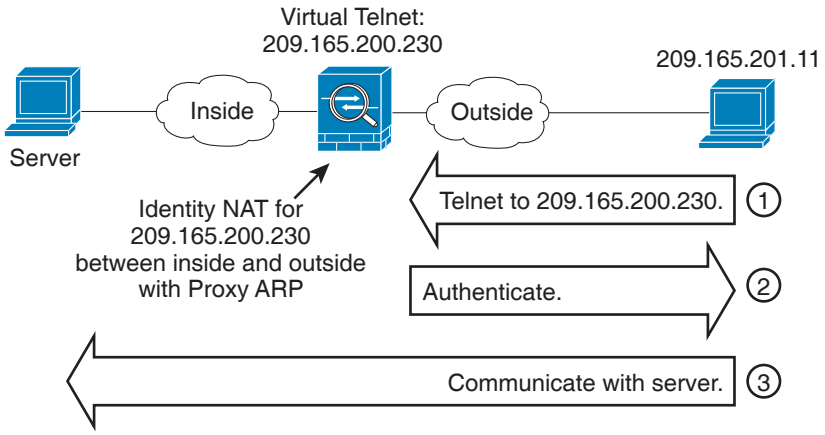
일반적으로 아이덴티티 NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다. 예를 들어 "any" IP 주소에 대해 광범위한 아이덴티티 NAT 규칙을 구성하고 프록시 ARP를 활성 상태로 유지하면 매핑된 인터페이스에 직접 연결된 네트워크에서 호스트 문제가 발생할 수 있습니다. 이 경우 매핑된 네트워크의 호스트가 동일한 네트워크의 다른 호스트와 통신하려면 ARP 요청의 주소가 NAT 규칙과 일치해야 합니다("any" 주소와 일치). 패킷이 실제로 ASA로 이동하도록 지정되지 않아도 ASA에서는 주소에 대해 프록시 ARP를 수행합니다. 이 문제는 Twice NAT 규칙이 있는 경우에도 발생합니다. NAT 규칙이 소스 주소 및 수신 주소와 모두 일치해야 하지만 프록시 ARP 결정은 "소스" 주소에 대해서만 내려집니다. 실제 호스트 ARP 응답 이전에 ASA ARP 응답이 수신되면 트래픽이 실수로 ASA로 전송됩니다(그림 4-18 참조).

그림 4-18 아이덴티티 NAT의 프록시 ARP 문제



드문 경우이지만 아이덴티티 NAT에 프록시 ARP가 필요할 수 있습니다(예: 가상 텔넷). 네트워크 액세스에 AAA를 사용하는 경우 호스트는 다른 트래픽이 통과하기 전에 텔넷과 같은 서비스를 사용하여 ASA의 인증을 받아야 합니다. ASA에서 가상 텔넷 서버를 구성하여 필요한 로그인을 제공할 수 있습니다. 외부에서 가상 텔넷 주소에 액세스할 경우 특히 프록시 ARP 기능에는 주소에 대해 아이덴티티 NAT 규칙을 구성해야 합니다. 가상 텔넷에 대한 내부 프로세스 때문에 프록시 ARP에서는 ASA가 가상 텔넷 주소로 이동할 트래픽을 NAT 규칙에 따라 소스 인터페이스로 내보내기보다는 유지하도록 합니다. (그림 4-19 참조).

그림 4-19 프록시 ARP 및 가상 텔넷



원격 네트워크에 대한 투명 모드 라우팅 요구 사항

투명 모드에서 NAT를 사용할 경우 몇 가지 트래픽 유형에는 고정 경로가 필요합니다. 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

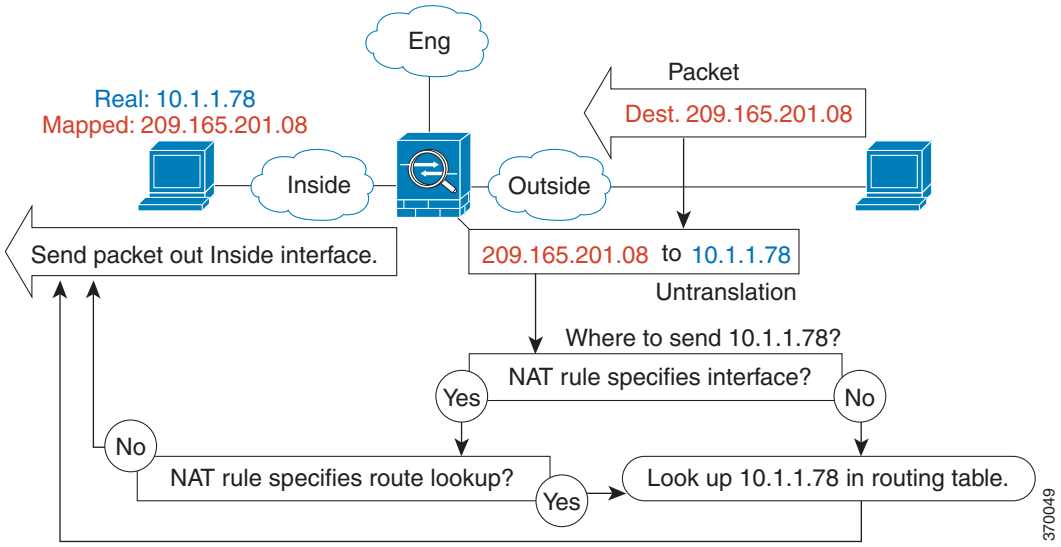
이그레스(egress) 인터페이스 결정

ASA에 매핑된 주소에 대한 트래픽이 도착하면 ASA에서는 NAT 규칙에 따라 수신 주소를 변환하지 않고, 패킷을 실제 주소로 전송합니다. ASA에서는 다음과 같은 방법으로 패킷에 대한 이그레스 인터페이스를 결정합니다.

- 투명 모드 - ASA에서는 NAT 규칙을 사용하여 실제 주소에 대한 이그레스 인터페이스를 결정합니다. 사용자는 NAT 규칙의 일부로서 소스(source) 및 수신(destination) 인터페이스를 지정해야 합니다.
- 라우팅된 모드 - ASA에서는 다음과 같은 방법 중 하나로 이그레스 인터페이스를 결정합니다.
  - 사용자가 NAT 규칙에서 인터페이스 구성 - ASA에서는 NAT 규칙을 사용하여 이그레스 인터페이스를 결정합니다. 그러나 항상 경로 조회를 대신 사용할 수 있는 옵션이 제공됩니다. 특정 시나리오에서는 경로 조회 재지정이 필요합니다. 예를 보려면 4-30 페이지의 NAT 및 VPN 관리 액세스를 참조하십시오.
  - 사용자가 NAT 규칙에서 인터페이스를 구성하지 않음 - ASA에서는 경로 조회를 사용하여 이그레스 인터페이스를 결정합니다.

다음 그림은 라우팅된 모드에서 이그레스 인터페이스를 선택하는 방법을 보여줍니다. 대부분의 경우 경로 조회는 NAT 규칙 인터페이스와 같지만, 일부 컨피그레이션에서는 두 방법이 다를 수 있습니다.

그림 4-20 라우팅된 모드 이그레스 인터페이스 선택



VPN용 NAT

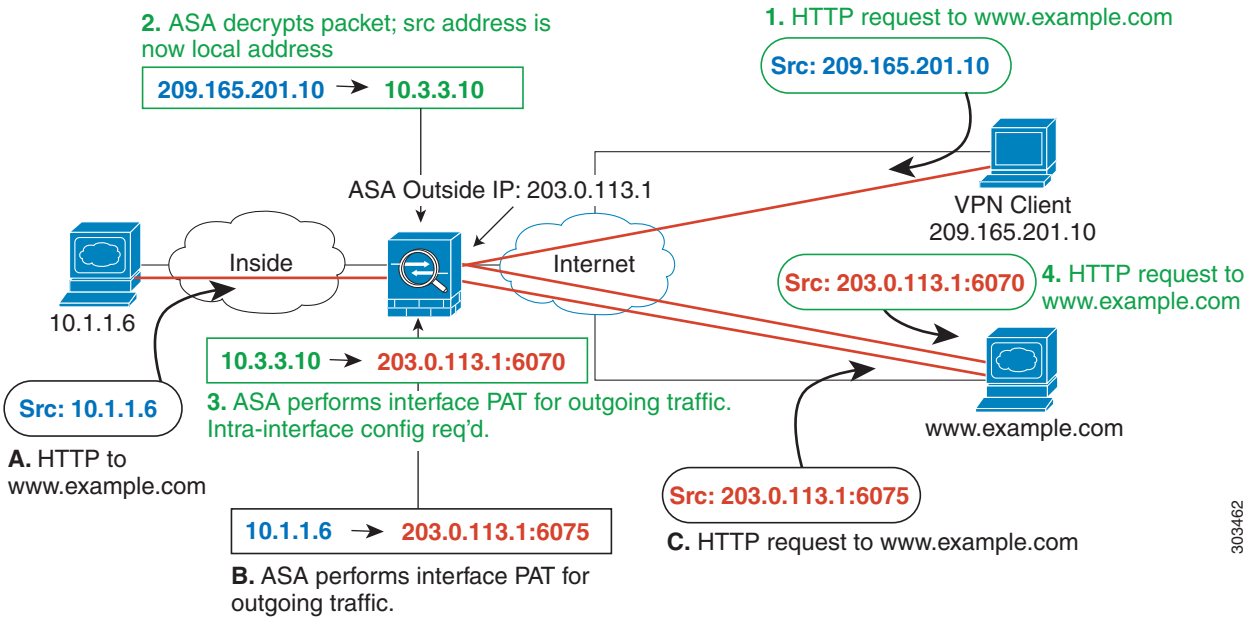
다음 항목에서는 다양한 유형의 VPN과 함께 NAT를 사용하는 방법에 대해 설명합니다.

- 4-26 페이지의 NAT 및 원격 액세스 VPN
- 4-28 페이지의 NAT 및 Site-to-Site VPN
- 4-30 페이지의 NAT 및 VPN 관리 액세스
- 4-32 페이지의 NAT 및 VPN 문제 해결

NAT 및 원격 액세스 VPN

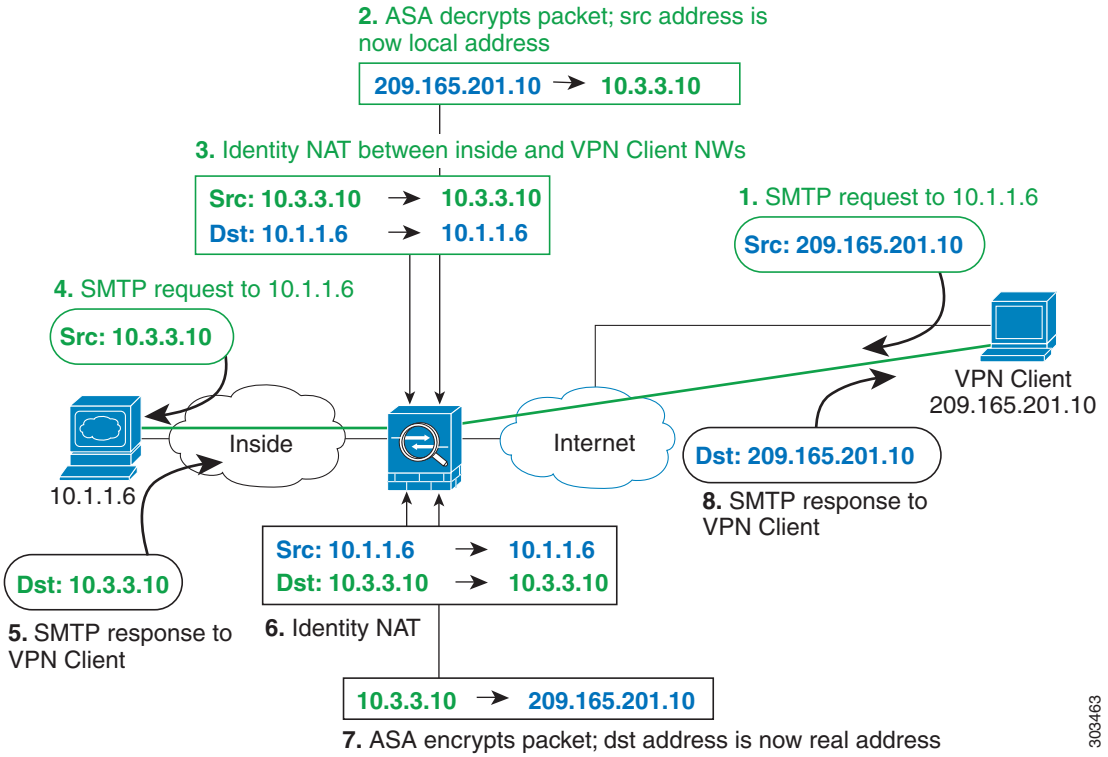
다음 그림은 인터넷에 액세스하는 내부 서버(10.1.1.6) 및 VPN 클라이언트(209.165.201.10)를 보여줍니다. VPN 클라이언트에 대해 스플릿 터널링(지정된 트래픽만 VPN 터널 통과)을 구성하지 않으면 인터넷 바인딩 VPN 트래픽도 ASA를 통과해야 합니다. VPN 트래픽이 ASA에 들어가면 ASA에서는 패킷을 암호 해독합니다. 해독된 패킷에는 VPN 클라이언트 로컬 주소(10.3.3.10)가 소스로서 포함되어 있습니다. 인터넷에 액세스하려면 내부 및 VPN 클라이언트 로컬 네트워크 모두에 대해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래의 예에서는 인터페이스 PAT 규칙을 사용합니다. VPN 트래픽이 들어간 곳과 동일한 인터페이스에서 나오도록 하려면 내부 인터페이스 통신("헤어핀(hairpin)" 네트워킹이라고도 함)을 활성화해야 합니다.

그림 4-21 인터넷 바인딩 VPN 트래픽을 위한 인터페이스 PAT(내부 인터페이스)



다음 그림은 내부 메일 서버에 액세스하려는 VPN 클라이언트를 보여줍니다. ASA는 내부 네트워크와 외부 네트워크 간 트래픽이 인터넷 액세스에 대해 설정한 인터페이스 PAT 규칙과 일치할 것을 기대하므로, VPN 클라이언트(10.3.3.10)에서 SMTP 서버(10.1.1.6)로의 트래픽이 역방향 경로 실패로 인해 삭제됩니다. 10.3.3.10에서 10.1.1.6으로의 트래픽은 NAT 규칙과 일치하지 않지만, 10.1.1.6에서 10.3.3.10으로의 반환 트래픽은 나가는 트래픽에 대해 인터페이스 PAT 규칙과 *반드시* 일치해야 합니다. 정방향 및 역방향 흐름이 일치하지 않으므로 ASA는 수신하는 패킷을 삭제합니다. 이 실패를 피하려면 이러한 네트워크 간에 아이덴티티 NAT 규칙을 사용하여 인터페이스 PAT 규칙에서 내부-VPN 클라이언트 트래픽을 제외해야 합니다. 아이덴티티 NAT는 단순히 주소를 동일한 주소로 변환합니다.

그림 4-22 VPN 클라이언트를 위한 아이덴티티 NAT



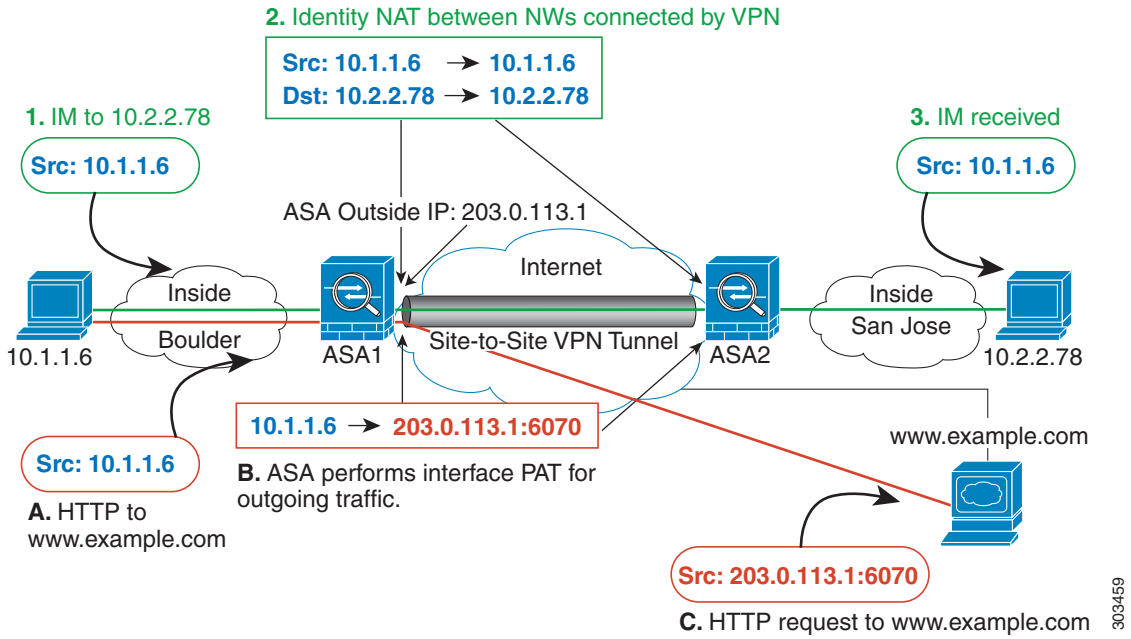
위 네트워크에 대한 다음의 샘플 NAT 컨피그레이션을 참조하십시오.

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local
vpn_local
```

NAT 및 Site-to-Site VPN

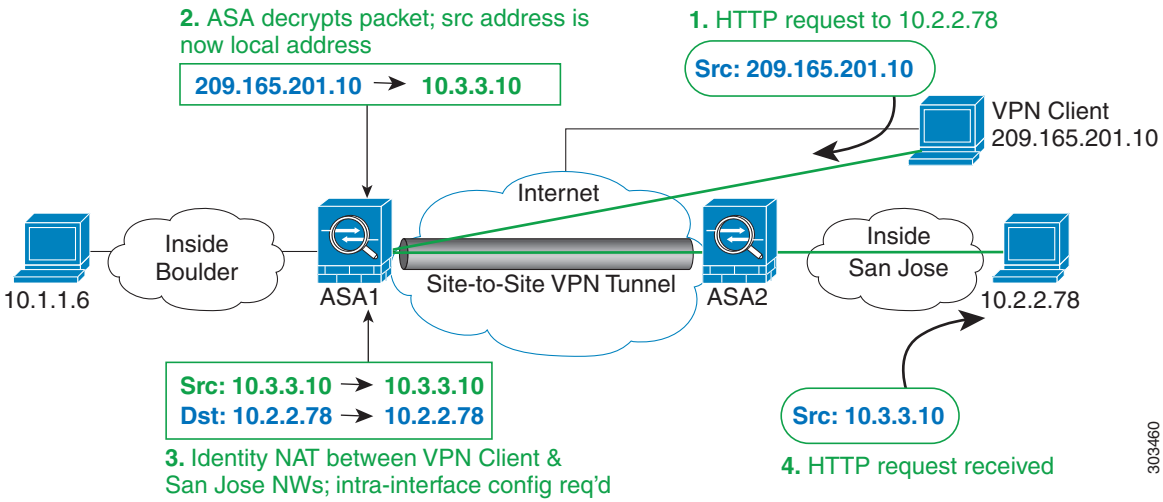
다음 그림은 Boulder 사무실과 San Jose 사무실을 연결하는 Site-to-Site 터널을 보여줍니다. 인터넷으로 이동할 트래픽(예: Boulder의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래의 예에서는 인터페이스 PAT 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: Boulder의 10.1.1.6에서 San Jose의 10.2.2.78로)에 대해서는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 아이덴티티 NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. 아이덴티티 NAT는 단순히 주소를 동일한 주소로 변환합니다.

그림 4-23 Site-to-Site VPN을 위한 인터페이스 PAT 및 아이덴티티 NAT



다음 그림은 ASA1(Boulder)과 ASA2(San Jose) 간 Site-to-Site 터널을 통해 액세스할 수 있는 서버(10.2.2.78)에 대한 텔넷 요청과 함께 ASA1에 연결된 VPN 클라이언트를 보여줍니다. 이것은 헤어핀 연결이므로 내부 인터페이스(intra-interface) 통신을 활성화해야 합니다. 이 기능은 VPN 클라이언트에서 오는 스플릿 터널링되지 않은(non-split-tunneled) 인터넷 바인딩 트래픽에도 필요합니다. 이 트래픽을 아웃바운드 NAT 규칙에서 제외하기 위해 VPN으로 연결된 모든 네트워크 간에 하는 것처럼, VPN 클라이언트와 Boulder 및 San Jose 네트워크 간에도 아이덴티티 NAT를 구성해야 합니다.

그림 4-24 Site-to-Site VPN에 대한 VPN 클라이언트 액세스



ASA1(Boulder)에 대한 다음의 샘플 NAT 컨피그레이션을 참조하십시오.

```
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside destination static
sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local destination static sanjose_inside
sanjose_inside
```

ASA2 (San Jose)에 대한 다음의 샘플 NAT 컨피그레이션을 참조하십시오.

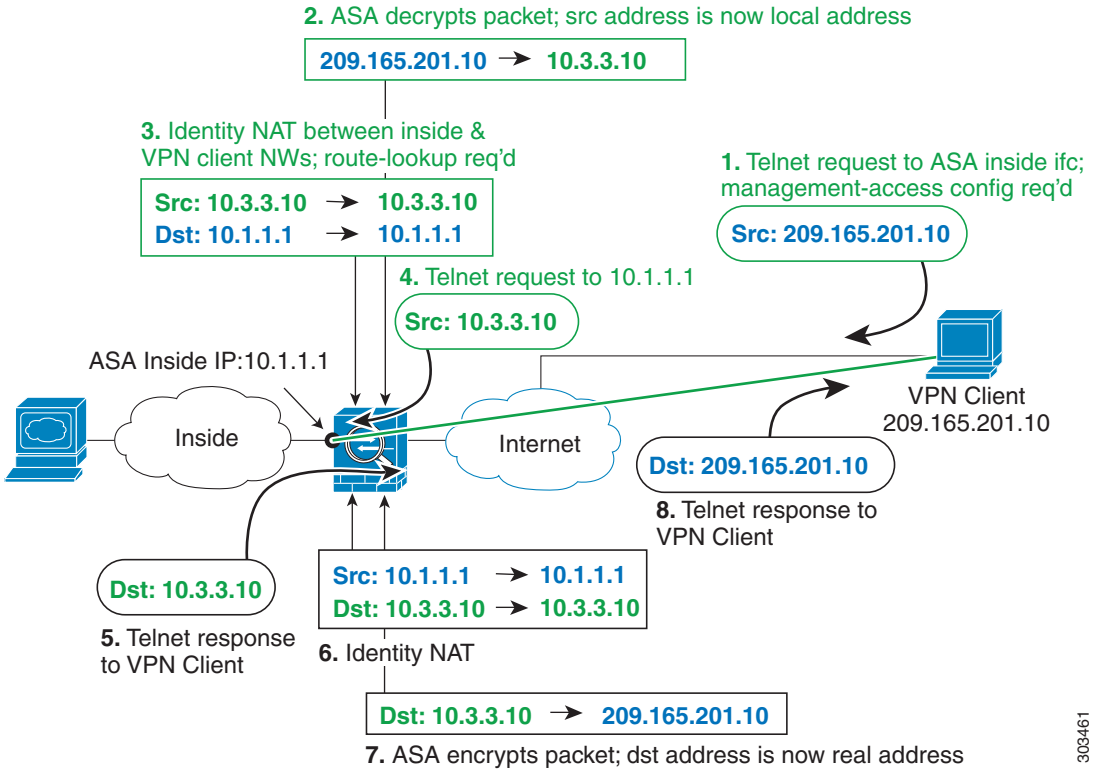
```
! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
    subnet 10.2.2.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
    subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
boulder_inside boulder_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside destination static
vpn_local vpn_local
```

NAT 및 VPN 관리 액세스

VPN 사용 시 ASA에 들어간 인터페이스 이외의 인터페이스에 대해 관리 액세스를 허용할 수 있습니다(**management-access** 명령 참조). 예를 들어, 외부 인터페이스에서 ASA에 들어간 경우 management-access 기능을 사용하면 ASDM, SSH, 텔넷 또는 SNMP를 사용하여 내부 인터페이스에 연결할 수 있습니다. 또는 내부 인터페이스에 ping할 수 있습니다.

다음 그림은 ASA 내부 인터페이스에 대한 VPN 클라이언트 텔넷 연결을 보여줍니다. management-access 인터페이스를 사용하며 4-26 페이지의 NAT 및 원격 액세스 VPN 또는 4-28 페이지의 NAT 및 Site-to-Site VPN에 따라 아이덴티티 NAT를 구성하는 경우 경로 조회 옵션과 함께 NAT를 구성해야 합니다. 경로 조회가 없으면 ASA에서는 라우팅 테이블의 내용과 상관없이 NAT 명령으로 지정한 인터페이스 외부로 트래픽을 전송합니다. 아래의 예에서 이그레스 인터페이스는 내부 인터페이스입니다. 여기에서는 ASA에서 관리 트래픽을 내부 네트워크로 전송하지 않도록 지정하려고 합니다. 트래픽은 내부 인터페이스 IP 주소로 반환되지 않습니다. 경로 조회 옵션을 사용하면 ASA는 트래픽을 내부 네트워크가 아니라 내부 인터페이스 IP 주소로 직접 전송합니다. VPN 클라이언트에서 내부 네트워크의 호스트로 이동하는 트래픽의 경우 경로 조회 옵션을 사용해도 여전히 올바른 이그레스 인터페이스(내부)로 이동하므로, 정상적인 트래픽 흐름에는 영향이 미치지 않습니다. 경로 조회 옵션에 대한 자세한 내용은 4-24 페이지의 이그레스(egress) 인터페이스 결정을 참조하십시오.

그림 4-25 VPN 관리 액세스



위 네트워크에 대한 다음의 샘플 NAT 컨피그레이션을 참조하십시오.

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Enable management access on inside ifc:
management-access inside

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
    subnet 10.3.3.0 255.255.255.0
    nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
    subnet 10.1.1.0 255.255.255.0
    nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local destination static inside_nw
inside_nw route-lookup
```

NAT 및 VPN 문제 해결

VPN과 관련된 NAT 문제를 해결하기 위한 다음의 모니터링 툴을 참조하십시오.

- 패킷 추적기 - 올바르게 사용하면 패킷 추적기는 패킷에 사용된 NAT 규칙을 표시합니다.
- **show nat detail** - 특정 NAT 규칙의 사용 횟수 및 변환되지 않은 트래픽을 표시합니다.
- **show conn all** - box 트래픽 왕복을 비롯한 활성 연결을 볼 수 있습니다.

비작동 컨피그레이션과 작동 컨피그레이션에 익숙해지려면 다음 단계를 수행할 수 있습니다.

1. 아이덴티티 NAT 없이 VPN을 구성합니다.
2. **show nat detail** 및 **show conn all**을 입력합니다.
3. 아이덴티티 NAT 컨피그레이션을 추가합니다.
4. **show nat detail** 및 **show conn all**을 반복합니다.

DNS 및 NAT

회신의 주소를 NAT 컨피그레이션과 일치하는 주소로 교체하여 DNS 회신을 수정하도록 ASA를 구성해야 할 수 있습니다. 각 변환 규칙을 구성할 때 DNS 수정을 구성할 수 있습니다.

이 기능은 NAT 규칙과 일치하는 DNS 쿼리 및 회신의 주소를 재작성합니다(예: IPv4의 A 레코드, IPv6의 AAAA 레코드 또는 역방향 DNS 쿼리의 PTR 레코드). 매핑된 인터페이스에서 다른 임의의 인터페이스로 이동하는 DNS 회신의 경우 매핑된 값에서 실제 값으로 레코드가 재작성됩니다. 반대로, 임의의 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 회신의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다.

다음은 DNS 재작성의 몇 가지 제한 사항입니다.

- 각 A 레코드에 여러 PAT 규칙을 적용할 수 있으며 사용할 PAT 규칙이 애매하므로 DNS 재작성은 PAT에 적용되지 않습니다.
- Twice NAT 규칙을 구성할 때 소스 주소와 수신 주소를 모두 지정하는 경우에는 DNS 수정을 구성할 수 없습니다. 이런 종류의 규칙은 A-B로 이동할 때 단일 주소에 대해 서로 다른 변환을 가질 수 있습니다. 따라서 ASA는 DNS 회신 내부의 IP 주소를 정확한 Twice NAT 규칙에 대해 올바르게 확인할 수 없습니다. DNS 회신에는 DNS 요청을 표시한 패킷에 어떤 source/destination 주소 조합이 있었는지에 대한 정보가 포함되어 있지 않습니다.
- DNS 재작성 기능을 이용하려면 이 기능이 기본적으로 켜져 있는 DNS 애플리케이션 검사를 활성화해야 합니다. 자세한 내용은 8-1 페이지의 DNS 검사 섹션을 참조하십시오.
- DNS 재작성은 실제로 NAT 규칙이 아니라 xlate 항목에서 수행됩니다. 따라서 동적 규칙에 대한 xlate가 없으면 재작성을 정확히 수행할 수 없습니다. 고정 NAT에 대해서는 동일한 문제가 발생하지 않습니다.

다음 항목에서는 DNS 재작성의 예를 제공합니다.

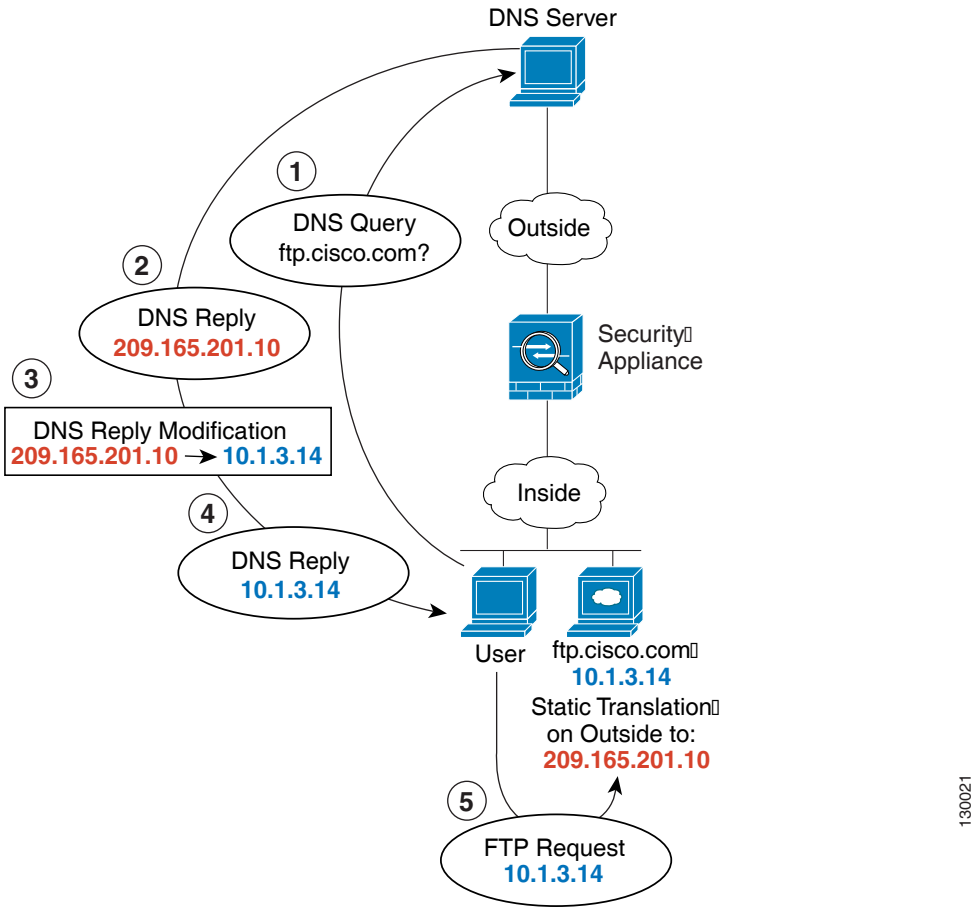
- 4-33 페이지의 DNS 회신 수정, 외부의 DNS 서버
- 4-34 페이지의 DNS 회신 수정, DNS 서버, 호스트, 별도의 네트워크에 있는 서버
- 4-35 페이지의 DNS 회신 수정, 호스트 네트워크의 DNS 서버
- 4-36 페이지의 외부 NAT를 사용한 DNS64 회신 수정
- 4-37 페이지의 PTR 수정, 호스트 네트워크의 DNS 서버

DNS 회신 수정, 외부의 DNS 서버

다음 그림은 인터페이스 외부에서 액세스할 수 있는 DNS 서버를 보여줍니다. ftp.cisco.com 서버는 내부 인터페이스에 있습니다. ftp.cisco.com 실제 주소(10.1.3.14)를 외부 네트워크에서 보이는 매핑된 주소(209.165.201.10)로 고정으로 변환하도록 ASA를 구성하십시오.

이 경우, 실제 주소를 사용하여 ftp.cisco.com에 액세스할 수 있는 내부 사용자가 DNS 서버에서 실제 주소(매핑된 주소가 아님)를 받을 수 있도록 고정 규칙에 대한 DNS 회신 수정을 활성화할 수 있습니다. 내부 호스트가 ftp.cisco.com 주소에 DNS 요청을 전송하면, DNS 서버는 매핑된 주소(209.165.201.10)로 회신합니다. ASA는 내부 서버에 대한 고정 규칙을 참조하여 DNS 회신에 있는 주소를 10.1.3.14로 변환합니다. DNS 회신 수정을 활성화하지 않으면 내부 호스트는 ftp.cisco.com에 직접 액세스하는 대신 트래픽을 209.165.201.10으로 전송하려고 시도하게 됩니다.

그림 4-26 DNS 회신 수정, 외부의 DNS 서버

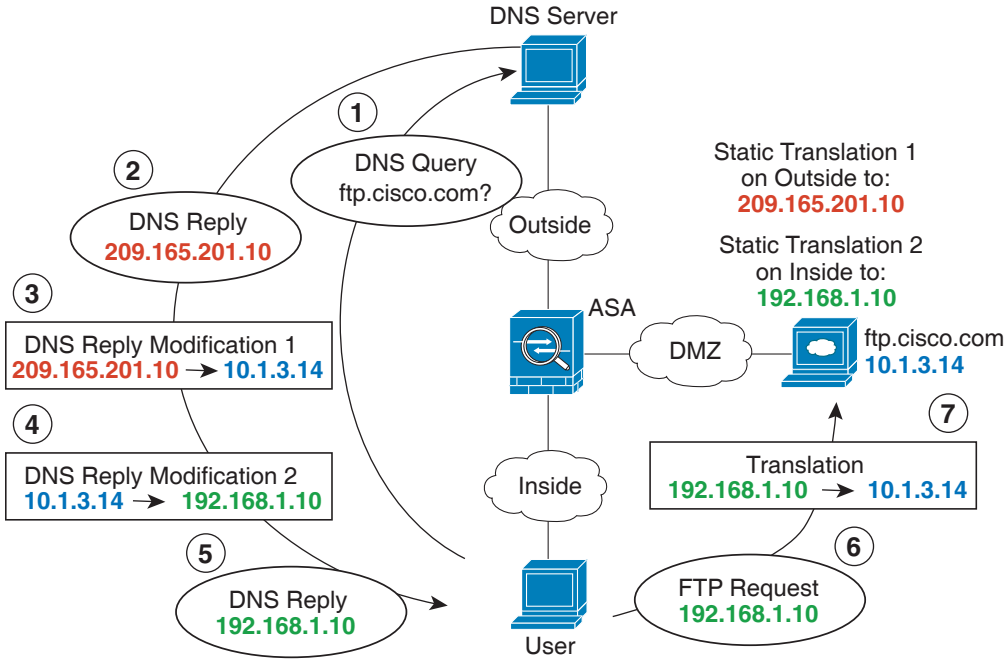


DNS 회신 수정, DNS 서버, 호스트, 별도의 네트워크에 있는 서버

다음 그림은 외부 DNS 서버에서 DMZ 네트워크에 있는 ftp.cisco.com에 대한 IP 주소를 요청하는 네트워크 내부의 사용자를 보여줍니다. 사용자가 DMZ 네트워크에 있지 않더라도 DNS 서버는 외부와 DMZ 간 고정 규칙에 따라, 매핑된 주소(209.165.201.10)로 응답합니다. ASA에서는 DNS 회신 내부의 주소를 10.1.3.14로 변환합니다.

사용자가 실제 주소를 사용해 ftp.cisco.com에 액세스해야 하는 경우에는 추가 컨피그레이션이 필요하지 않습니다. 내부 및 DMZ 간에도 고정 규칙이 있으면 이 규칙에 대한 DNS 회신 수정도 활성화해야 합니다. 그러면 DNS 회신이 두 번 수정됩니다. 이 경우 ASA에서는 내부와 DMZ 간 고정 규칙에 따라 DNS 회신 내부의 주소를 192.168.1.10으로 다시 변환합니다.

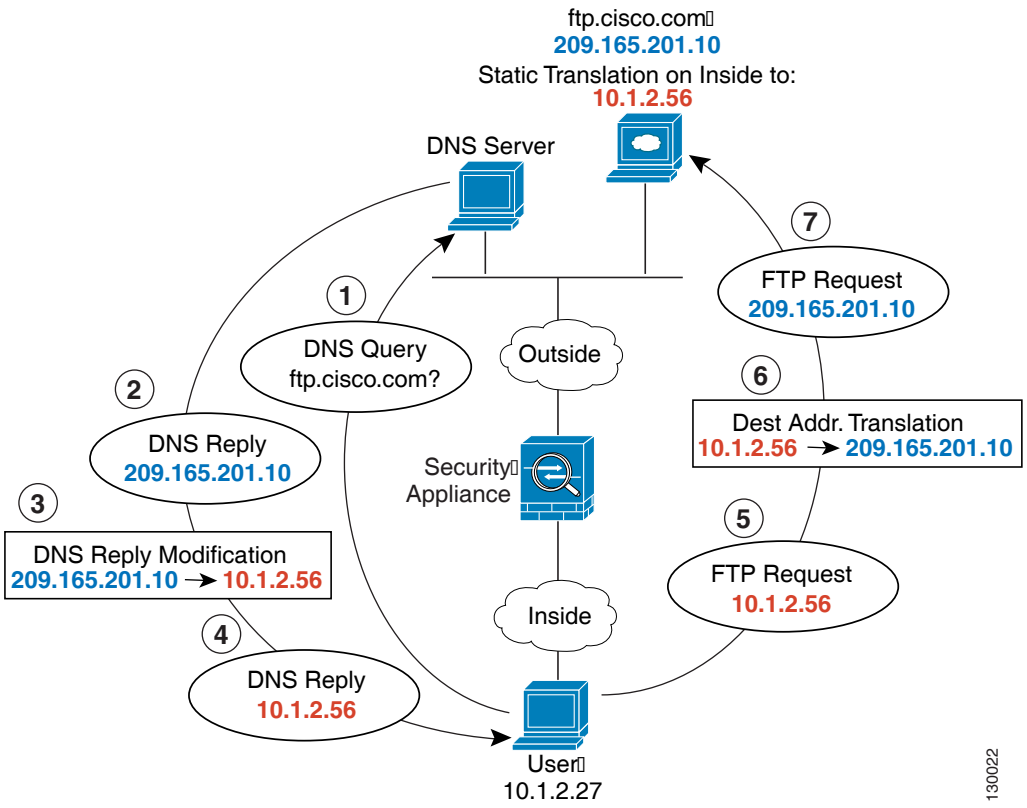
그림 4-27 DNS 회신 수정, DNS 서버, 호스트, 별도의 네트워크에 있는 서버



DNS 회신 수정, 호스트 네트워크의 DNS 서버

다음 그림은 외부의 FTP 서버 및 DNS 서버를 보여줍니다. ASA는 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.20.10으로 응답합니다. 내부 사용자가 ftp.cisco.com(10.1.2.56)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다.

그림 4-28 DNS 회신 수정, 호스트 네트워크의 DNS 서버

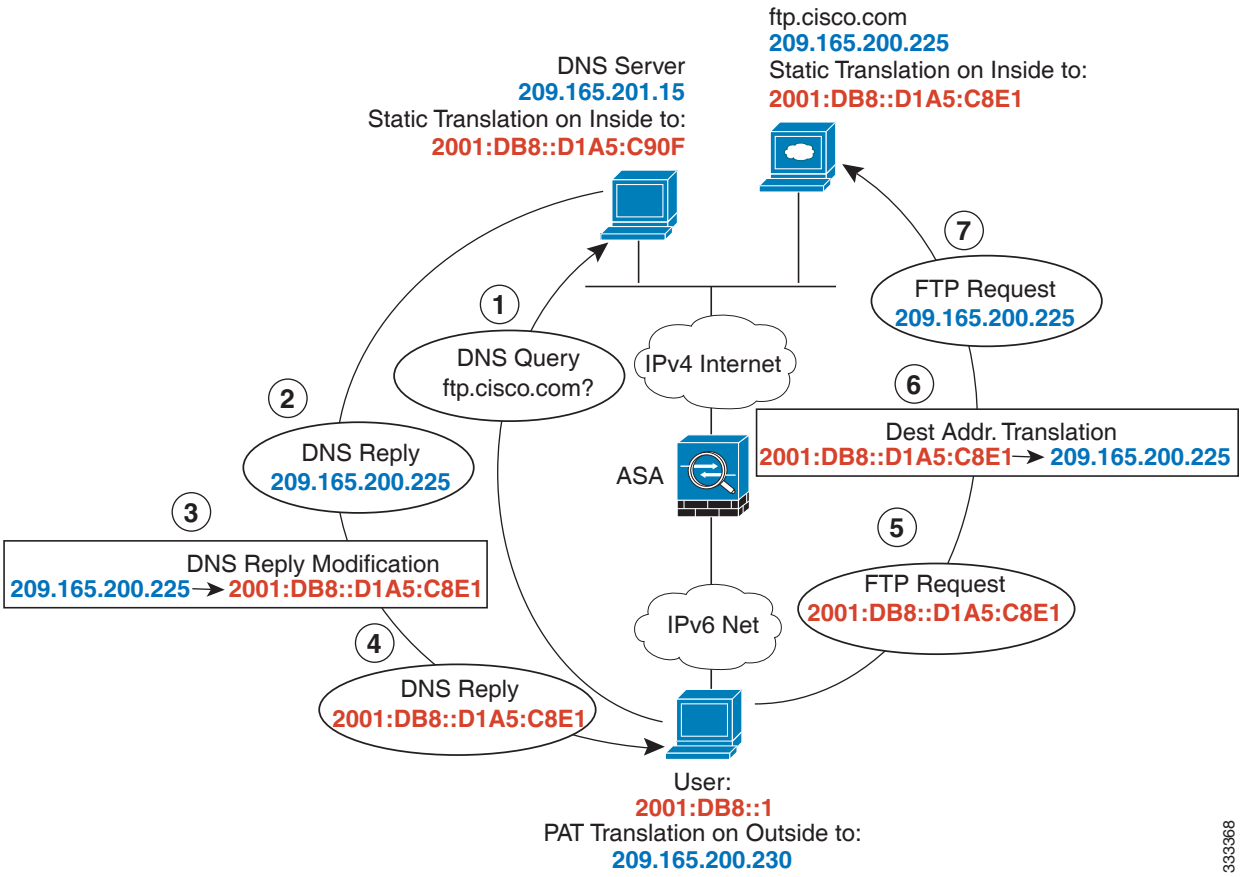


외부 NAT를 사용한 DNS64 회신 수정

다음 그림은 외부 IPv4 네트워크의 FTP 서버 및 DNS 서버를 보여줍니다. ASA는 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 IPv6 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.200.225로 응답합니다.

내부 사용자가 ftp.cisco.com(2001:DB8::D1A5:C8E1)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다. 이 예에는 DNS 서버용 고정 NAT 변환 및 내부 IPv6 호스트용 PAT 규칙도 포함되어 있습니다.

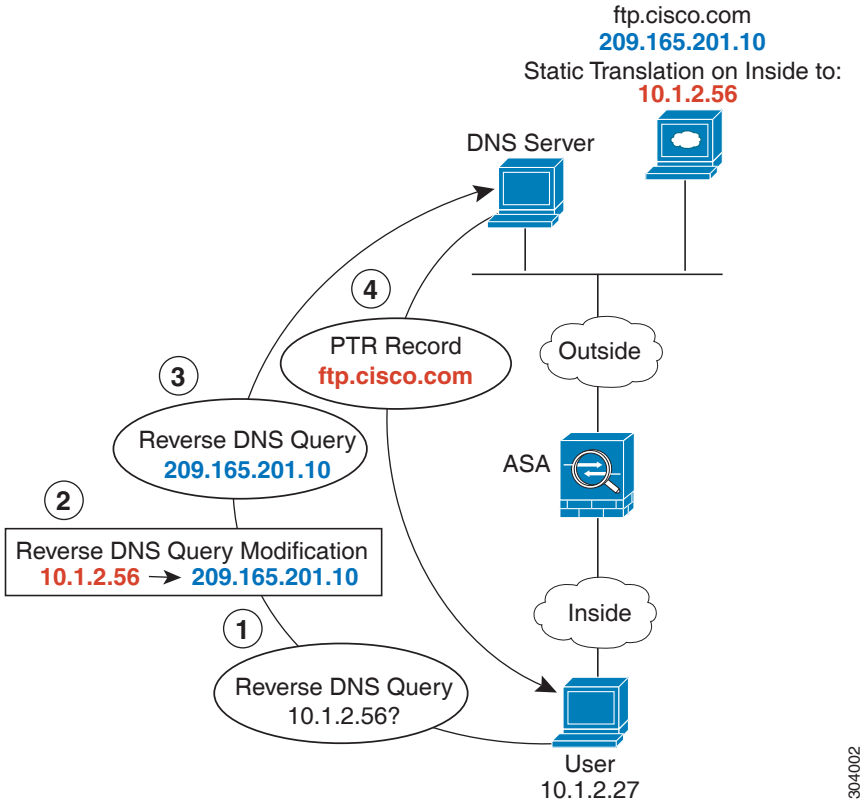
그림 4-29 외부 NAT를 사용한 DNS64 회신 수정



PTR 수정, 호스트 네트워크의 DNS 서버

다음 그림은 외부의 FTP 서버 및 DNS 서버를 보여줍니다. ASA는 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 사용자가 10.1.2.56에 대해 역방향 DNS 조회를 수행하면 ASA는 역방향 DNS 쿼리를 실제 주소로 수정하며, DNS 서버는 서버 이름인 ftp.cisco.com으로 응답합니다.

그림 4-30 PTR 수정, 호스트 네트워크의 DNS 서버



다음 학습 내용

네트워크 객체 NAT를 구성하려면 5 장, “네트워크 객체 NAT” 를 참조하십시오.

Twice NAT를 구성하려면 6 장, “Twice NAT”를 참조하십시오.

다음 학습 내용

5 장

네트워크 객체 NAT

네트워크 객체의 매개변수로서 구성되는 모든 NAT 규칙은 *네트워크 객체 NAT* 규칙으로 간주됩니다. 네트워크 객체 NAT는 단일 IP 주소, 주소 범위 또는 서브넷에 대해 NAT를 구성하기 위한 빠르고 쉬운 방법입니다. 네트워크 객체를 구성한 후에는 해당 객체에 대해 매핑된 주소를 식별할 수 있습니다.

이 장의 다음 섹션에서는 네트워크 객체 NAT를 구성하는 방법에 대해 설명합니다.

참고 NAT 작동 방식에 대한 자세한 내용은 4 장, “NAT(Network Address Translation)”을 참조하십시오.

네트워크 객체 NAT에 대한 정보

패킷이 ASA로 들어가면 소스 및 수신 IP 주소 모두에서 네트워크 객체 NAT 규칙의 점검이 수행됩니다. 별도의 일치를 만든 경우 별도의 규칙을 통해 패킷의 소스 및 수신 주소를 변환할 수 있습니다. 이러한 규칙은 서로 연결되어 있지 않습니다. 트래픽에 따라 규칙의 서로 다른 조합을 사용할 수 있습니다.

규칙은 쌍을 이루지 않으므로 소스 주소가 수신 주소 X로 이동할 때 A로 변환되도록, 수신 주소 Y로 이동할 때 B로 변환되도록 지정할 수 없습니다. 그런 종류의 기능이 필요한 경우 Twice NAT를 사용하십시오. Twice NAT를 사용하면 단일 규칙으로 소스 및 수신 주소를 식별할 수 있습니다.

Twice NAT 및 네트워크 객체 NAT의 차이에 대한 자세한 내용은 4-15 페이지의 NAT 구현 방법을 참조하십시오.

네트워크 객체 NAT 규칙은 NAT 규칙 테이블의 섹션 2에 추가됩니다. NAT 순서에 대한 자세한 내용은 4-20 페이지의 NAT 규칙 순서를 참조하십시오.

네트워크 객체 NAT의 라이센싱 요구 사항

다음 표에서는 이 기능의 라이센싱 요구 사항을 보여줍니다.

모델	라이센스 요구 사항
ASAv	표준 또는 프리미엄 라이센스
모든 다른 모델	기본 라이센스

네트워크 객체 NAT 전제 조건

컨피그레이션에 따라 원하는 경우 매핑된 주소를 인라인으로 구성할 수도 있고, 매핑된 주소에 대해 별도의 네트워크 객체 또는 네트워크 객체 그룹을 만들 수도 있습니다(**object network** 또는 **object-group network** 명령). 네트워크 객체 그룹은 비연속 IP 주소 범위 또는 다중 호스트나 서브넷을 이용해 매핑된 주소 풀을 만드는 데 특히 유용합니다. 네트워크 객체 또는 그룹을 만들려면 일반 운영 컨피그레이션 가이드를 참조하십시오.

객체 및 그룹에 대한 특정 지침은 구성할 NAT 유형에 대한 컨피그레이션 섹션을 참조하십시오. 또한 5-2 페이지의 지침 및 제한 섹션을 참조하십시오.

지침 및 제한

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원됩니다.

방화벽 모드 지침

- 투명 및 라우팅된 방화벽 모드에서 지원됩니다.
- 투명 모드에서는 실제(real) 및 매핑된(mapped) 인터페이스를 지정해야 합니다. **any**는 사용할 수 없습니다.
- 투명 모드에서는 인터페이스 PAT를 구성할 수 없습니다. 투명 모드 인터페이스에는 IP 주소가 없기 때문입니다. 관리 IP 주소를 매핑된 주소로서 사용할 수도 없습니다.
- 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 두 IPv6 네트워크 간 변환 또는 두 IPv4 네트워크 간 변환은 지원됩니다.

IPv6 지침

- IPv6을 지원합니다. 4-15 페이지의 NAT 및 IPv6도 참조하십시오.
- 라우팅된 모드에서는 IPv4와 IPv6 간에 변환할 수 있습니다.
- 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 두 IPv6 네트워크 간 변환 또는 두 IPv4 네트워크 간 변환은 지원됩니다.
- 투명 모드에서는 IPv6에 대해 PAT 풀이 지원되지 않습니다.
- 고정(Static) NAT에서는 IPv6 서브넷을 최대 /64까지 지정할 수 있습니다. 더 큰 서브넷은 지원되지 않습니다.

- FTP with NAT46을 사용할 때, IPv4 FTP 클라이언트가 IPv6 FTP 서버에 연결될 때 클라이언트는 확장 패시브 모드(EPSV) 또는 확장 포트 모드(EPRT)를 사용해야 하며, PASV 및 PORT 명령은 IPv6에서 지원되지 않습니다.

추가 지침

- 한 객체에는 단일 NAT 규칙만 정의할 수 있습니다. 한 객체에 대해 여러 NAT 규칙을 구성하려면 동일한 IP 주소를 지정하는 서로 다른 이름의 여러 객체를 만들어야 합니다(예: **object network obj-10.10.10.1-01**, **object network obj-10.10.10.1-02** 등).
- NAT 컨피그레이션을 변경한 경우 새 NAT 컨피그레이션이 사용되기 전 기존 변환이 시간 초과되기까지 기다리고 싶지 않다면 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 변환을 사용하는 현재의 모든 연결이 해제됩니다.

참고 동적 NAT 또는 PAT 규칙을 제거한 후 제거된 규칙의 주소와 겹치는 매핑된 주소로 새 규칙을 추가하는 경우, 새 규칙을 사용하려면 제거된 규칙과 관련된 모든 연결이 시간 초과되기까지 기다리거나 **clear xlate** 명령으로 해당 연결을 지워야 합니다. 이러한 안전 조치는 동일한 주소가 여러 호스트에 할당되는 것을 방지합니다.

- NAT의 객체 및 객체 그룹은 정의하지 않고 사용할 수 없으며, IP 주소를 반드시 포함해야 합니다.
- IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
- 여러 NAT 규칙에서 동일한 매핑된 객체 또는 그룹을 사용할 수 있습니다.
- 매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.
  - 매핑된 인터페이스 IP 주소. 규칙에 대해 **any** 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅된 모드만)의 경우 IP 주소 대신 **interface** 키워드를 사용합니다.
  - (투명 모드) 관리 IP 주소.
  - (동적 NAT) VPN이 활성화된 경우의 대기 인터페이스 IP 주소.
  - 기존의 VPN 풀 주소.
- 고정 및 동적 NAT 정책에서는 겹치는 주소 사용을 피해야 합니다. 예를 들어, PPTP의 보조 연결이 동적 xlate 대신 고정 상태인 경우 겹치는 주소를 사용하면 PPTP 연결 설정에 실패할 수 있습니다.
- NAT 또는 PAT의 애플리케이션 검사 제한 사항은 7 장, “애플리케이션 계층 프로토콜 검사 시작”의 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오.

기본 설정

- (라우팅된 모드) 기본적인 실제 및 매핑된 인터페이스는 모든 인터페이스에 규칙을 적용하는 Any입니다.
- 아이덴티티 NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 자세한 내용은 4-22 페이지의 NAT 패킷 라우팅 섹션을 참조하십시오.
- 사용자가 선택적인 인터페이스를 지정하는 경우 ASA에서는 NAT 컨피그레이션을 사용하여 이그레스(egress) 인터페이스를 결정합니다, 대신 항상 경로 조회를 사용할 수 있는 옵션이 사용자에게 제공됩니다. 자세한 내용은 4-22 페이지의 NAT 패킷 라우팅 섹션을 참조하십시오.

네트워크 객체 NAT 구성

이 섹션에서는 네트워크 객체 NAT 구성 방법에 대해 설명합니다.

매핑된 주소에 대해 네트워크 객체 추가

동적 NAT의 경우 매핑된 주소에 대해 항상 객체 또는 그룹을 사용해야 합니다. 기타 NAT 유형에는 인라인 주소를 사용할 수 있는 옵션이 있지만, 이 섹션의 내용에 따라 객체 또는 그룹을 만들 수 있습니다. 네트워크 객체 또는 그룹 구성에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

지침

- 네트워크 객체 그룹은 IPv4 또는 IPv6 주소의 인라인 주소 및/또는 객체를 포함할 수 있습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.
- 허용되지 않는 매핑된 IP 주소에 대한 자세한 내용은 5-2 페이지의 지침 및 제한을 참조하십시오.
- Dynamic NAT:
  - 인라인 주소는 사용할 수 없으며, 네트워크 객체 또는 그룹을 구성해야 합니다.
  - 객체 또는 그룹에 서브넷을 포함할 수 없습니다. 객체는 범위를 정의해야 하고, 그룹은 호스트와 범위를 포함할 수 있습니다.
  - 매핑된 네트워크 객체에 범위와 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안(fallback)으로 사용됩니다.
- Dynamic PAT (Hide):
  - 객체를 사용하는 대신 선택적으로 인라인 호스트 주소를 구성하거나 인터페이스 주소를 지정할 수 있습니다.
  - 객체를 사용하는 경우 객체 또는 그룹에 서브넷을 포함할 수 없습니다. 객체는 호스트를 정의하거나 PAT 풀에 대해 범위를 정의해야 합니다. 그룹(PAT 풀)은 호스트와 범위를 포함할 수 있습니다.
- Static NAT 또는 Static NAT with port translation:
  - 객체를 사용하는 대신 인라인 주소를 구성하거나 인터페이스 주소를 지정할 수 있습니다(static NAT-with-port-translation).
  - 객체를 사용하는 경우 객체 또는 그룹에 호스트, 범위 또는 서브넷을 포함할 수 있습니다.
- 아이덴티티 NAT
  - 객체를 사용하는 대신 인라인 주소를 구성할 수 있습니다.
  - 객체를 사용하는 경우 변환하려는 실제 주소와 객체가 일치해야 합니다.

자세한 단계

명령	목적

object network *obj_name* {**host** *ip_address* | **range** *ip_address_1 ip_address_2* | **subnet** *subnet_address netmask*}
 	
예:
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
	네트워크 객체 IPv4 또는 IPv6을 추가합니다.

object-group network *grp_name* {**network-object** {**object** *net_obj_name* | *subnet_address netmask* | **host** *ip_address*} | **group-object** *grp_obj_name*}
 	
예:
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
 	
`hostname(config)# object network TEST2`
`hostname(config-network-object)# range 10.1.2.1 10.1.2.70`
 	
`hostname(config-network-object)# object-group network MAPPED_IPS`
`hostname(config-network)# network-object object TEST`
`hostname(config-network)# network-object object TEST2`
`hostname(config-network)# network-object host 10.1.2.79`
	네트워크 객체 그룹 IPv4 또는 IPv6을 추가합니다.

동적 NAT

이 섹션에서는 동적 NAT에 대해 네트워크 객체 NAT를 구성하는 방법에 대해 설명합니다. 자세한 내용은 4-8 페이지의 동적 NAT를 참조하십시오.

자세한 단계

	명령	목적
1단계	`Create a network object or group for the mapped addresses.`	5-4 페이지의 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오.
2단계	**object network** *obj_name* 예: `hostname(config)# object network my-host-obj1`	NAT를 구성하려는 네트워크 객체를 구성하거나, 기존 네트워크 객체에 대해 객체 네트워크 컨피그레이션 모드로 들어갑니다.

	명령	목적
3단계	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} 예: `hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`	새 네트워크 객체를 만드는 경우 변환할 **실제** IP 주소(IPv4 또는 IPv6)를 정의합니다.
4단계	**nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** *mapped_obj* [**interface** [**ipv6**]] [**dns**] 예: `hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface`	객체 IP 주소에 대해 **dynamic NAT**를 구성합니다. **참고** 한 객체에는 단일 NAT 규칙만 정의할 수 있습니다. 5-3 페이지의 추가 지침 섹션을 참조하십시오. 다음 지침을 참조하십시오. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • 매핑된 IP 주소 - 매핑된 IP 주소를 다음과 같이 지정합니다. – 기존 네트워크 객체(1단계 참조). – 기존 네트워크 객체 그룹(1단계 참조). • 인터페이스 PAT 대안 - (선택 사항) **interface** 키워드는 인터페이스 PAT 대안을 활성화합니다. 매핑된 IP 주소가 모두 사용되면, 그 다음에는 매핑된 인터페이스의 IP 주소가 사용됩니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 투명 모드에서는 **interface**를 지정할 수 없습니다. • DNS - (선택 사항) **dns** 키워드는 DNS 회신을 변환합니다. DNS 검사를 사용하도록 설정해야 합니다(기본적으로 사용됨). 자세한 내용은 4-32 페이지의 DNS 및 NAT 섹션을 참조하십시오.

예

다음 예는 192.168.2.0 네트워크를 10.2.2.1~10.2.2.10의 외부 주소 범위 뒤에 숨기는 동적 NAT를 구성합니다.

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

다음 예는 동적 PAT 백업으로 동적 NAT를 구성합니다. 내부 네트워크 10.76.11.0의 호스트는 먼저 nat-range1 풀(10.10.10.10~10.10.10.20)에 매핑됩니다. nat-range1 풀의 모든 주소가 할당된 후에는 pat-ip1 주소(10.10.10.21)를 사용해 동적 PAT가 수행됩니다. 잘 발생하지는 않지만, PAT 변환도 모두 사용되면 외부 인터페이스 주소를 사용해 동적 PAT가 수행됩니다.

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20
```

```
hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

다음 예는 IPv6 호스트를 IPv4로 변환하기 위해 동적 PAT 백업으로 동적 NAT를 구성합니다. 내부 네트워크 2001:DB8::/96의 호스트가 먼저 IPv4_NAT_RANGE 풀(209.165.201.1~209.165.201.30)에 매핑됩니다. IPv4_NAT_RANGE 풀의 모든 주소가 할당되면 IPv4_PAT 주소(209.165.201.31)를 사용해 동적 PAT가 수행됩니다. PAT 변환도 모두 사용되면 외부 인터페이스 주소를 사용해 동적 PAT가 수행됩니다.

```
hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

동적 PAT(숨김) 구성

이 섹션에서는 동적 PAT(숨김)용 네트워크 객체 NAT 구성 방법에 대해 설명합니다. 자세한 내용은 4-10 페이지의 동적 PAT 섹션을 참조하십시오.

지침

PAT 풀의 경우:

- 사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 *없*는 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다. (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 낮은 포트 범위를 사용하는 트래픽이 많은 경우 이제 크기가 서로 다른 세 가지 계층 대신 균일한 포트 범위(1024~65535 또는 1~65535)를 사용하도록 지정할 수 있습니다.
- 별개의 두 규칙에서 동일한 PAT 풀 객체를 사용하는 경우 각 규칙에 대해 동일한 옵션을 지정해야 합니다. 예를 들어, 한 규칙에서 확장 PAT와 균일한 범위를 지정하는 경우 다른 규칙에서도 확장 PAT와 균일한 범위를 지정해야 합니다.

PAT 풀용 확장 PAT의 경우:

- 확장 PAT를 지원하지 않는 애플리케이션 검사가 많습니다. 지원되지 않는 검사 리스트는 7 장, “애플리케이션 계층 프로토콜 검사 시작”의 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오.

- 동적 PAT 규칙에 대해 확장 PAT를 활성화하면, PAT 풀의 주소를 별도의 static NAT-with-port-translation 규칙에서 PAT 주소로서 사용할 수 없습니다. 예를 들어 PAT 풀이 10.1.1.1을 포함하면, 10.1.1.1을 PAT 주소로 사용하는 static NAT-with-port-translation 규칙을 만들 수 없습니다.
- PAT 풀을 사용하고 대안용 인터페이스를 지정하는 경우 확장 PAT를 지정할 수 없습니다.
- ICE 또는 TURN을 사용하는 VoIP 배포에는 확장 PAT를 사용할 수 없습니다. ICE 및 TURN은 모든 목적지에 대해 PAT 바인딩이 동일할 것으로 신뢰합니다.

PAT 풀용 라운드 로빈의 경우:

- 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. **참고**: 장애 조치 이후에는 "동질성"이 해제됩니다. ASA에서 장애 조치를 수행하면 호스트의 후속 연결에는 초기 IP 주소가 사용되지 않을 수 있습니다.
- 라운드 로빈은 특히 확장 PAT와 함께 사용할 경우 대량의 메모리를 소모할 수 있습니다. NAT 풀은 모든 매핑된 프로토콜/IP 주소/포트 범위에 대해 생성되므로, 라운드 로빈에서 대량의 동시 NAT 풀이 생성되며 여기에서 메모리를 사용합니다. 확장 PAT를 사용하면 동시 NAT 풀의 수가 더 많아집니다.

자세한 단계

	명령	목적
1단계	(선택 사항) 매핑된 주소용 네트워크 객체 또는 그룹을 만듭니다.	5-4 페이지의 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오.
2단계	**object network** *obj_name* **예:** `hostname(config)# object network my-host-obj1`	NAT를 구성하려는 네트워크 객체를 구성하거나, 기존 네트워크 객체에 대해 객체 네트워크 컨피그레이션 모드로 들어갑니다.
3단계	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **예:** `hostname(config-network-object)# range 10.1.1.1 10.1.1.90`	새 네트워크 객체를 만드는 경우 변환할 **실제** IP 주소(IPv4 또는 IPv6)를 정의합니다.

	명령	목적
4단계	**nat** [(*real_ifc*,*mapped_ifc*)] **dynamic** {*mapped_inline_host_ip* | *mapped_obj* | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] | **interface** [**ipv6**]} [**interface** [**ipv6**]] [**dns**] **예:** `hostname(config-network-object)# nat (any,outside) dynamic interface`	객체 IP 주소에 대해 **dynamic PAT**를 구성합니다. 한 객체에는 단일 NAT 규칙만 정의할 수 있습니다. 5-3 페이지의 추가 지침 섹션을 참조하십시오. 다음 지침을 참조하십시오. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • Mapped IP address - 매핑된 IP 주소를 다음과 같이 지정할 수 있습니다. – 인라인 호스트 주소. – 호스트로서 정의된 기존 네트워크 객체(1단계 참조). – **pat-pool** - 여러 주소가 포함된 기존 네트워크 객체 또는 그룹. – **interface** - (라우팅된 모드 전용) 매핑된 인터페이스의 IP 주소가 매핑된 주소로서 사용됩니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 인터페이스 IP 주소를 사용하려면 이 키워드를 사용해야 하며, 인라인으로 또는 객체로서 입력할 수 없습니다. • PAT 풀에 대해 다음 옵션 중 하나 이상을 지정할 수 있습니다. – Round robin - **round-robin** 키워드는 PAT 풀에 대한 라운드 로빈 주소 할당을 활성화합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다. (계속)

명령	목적
	(계속) – Extended PAT - **extended** 키워드는 확장 PAT를 활성화합니다. 확장 PAT는 변환 정보의 수신 주소 및 포트를 포함하여 *서비스*당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 목적지 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. – Flat range - **flat** 키워드는 포트 할당 시 1024~65535의 전체 포트 범위 사용을 활성화합니다. 변환용의 매핑된 포트 번호를 선택하면 ASA에서는 사용 가능한 경우 실제 소스 포트 번호를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 *없*는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **include-reserve** 키워드도 지정합니다. • Interface PAT fallback - (선택 사항) **interface** 키워드는 기본 PAT 주소 뒤에 입력할 경우 인터페이스 PAT 대안을 활성화합니다. 기본 PAT 주소가 모두 사용되면 매핑된 인터페이스의 IP 주소가 사용됩니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 투명 모드에서는 **interface**를 지정할 수 없습니다. • DNS - (선택 사항) **dns** 키워드는 DNS 회신을 변환합니다. DNS 검사를 사용하도록 설정해야 합니다(기본적으로 사용됨). 자세한 내용은 4-32 페이지의 DNS 및 NAT 섹션을 참조하십시오.

예

다음 예는 192.168.2.0 네트워크를 주소 10.2.2.2 뒤에 숨기는 동적 PAT를 구성합니다.

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

다음 예는 192.168.2.0 네트워크를 외부 인터페이스 주소 뒤에 숨기는 동적 PAT를 구성합니다.

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

다음 예는 내부 IPv6 네트워크를 외부 IPv4 네트워크로 변환할 수 있도록 PAT 풀이 있는 동적 PAT를 구성합니다.

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

Static NAT 또는 Static NAT-with-Port-Translation 구성

이 섹션에서는 네트워크 객체 NAT를 사용하여 Static NAT를 구성하는 방법에 대해 설명합니다. 자세한 내용은 4-3 페이지의 고정 NAT 섹션을 참조하십시오.

자세한 단계

	명령	목적
1단계	(선택 사항) 매핑된 주소용 네트워크 객체 또는 그룹을 만듭니다.	5-4 페이지의 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오.
2단계	**object network** *obj_name* **예:** `hostname(config)# object network my-host-obj1`	NAT를 구성하려는 네트워크 객체를 구성하거나, 기존 네트워크 객체에 대해 객체 네트워크 컨피그레이션 모드로 들어갑니다.
3단계	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} **예:** `hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0`	새 네트워크 객체를 만드는 경우 변환할 **실제** IP 주소(IPv4 또는 IPv6)를 정의합니다.

	명령	목적
4단계	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj* | **interface** [**ipv6**]} [**net-to-net**] [**dns** | **service** {**tcp** | **udp**} *real_port mapped_port*] [**no-proxy-arp**] **예:** `hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS service tcp 80 8080`	객체 IP 주소에 대해 **static NAT**를 구성합니다. 한 객체에는 단일 NAT 규칙만 정의할 수 있습니다. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • 매핑된 IP 주소 - 매핑된 IP 주소를 다음과 같이 지정할 수 있습니다. – 인라인 IP 주소. 매핑된 네트워크의 범위 또는 넷마스크가 실제 네트워크와 동일합니다. 예를 들어 실제 네트워크가 호스트이면 이 주소도 호스트 주소입니다. 범위의 경우 매핑된 주소에는 동일한 주소 번호가 실제 범위로서 포함됩니다. 예를 들어 실제 주소의 범위를 10.1.1.1~10.1.1.6으로 정의하고 매핑된 주소로 172.20.1.1을 지정하는 경우 매핑된 범위에는 172.20.1.1~172.20.1.6이 포함됩니다. – 기존 네트워크 객체 또는 그룹(1단계 참조). – **interface** - (Static NAT-with-port-translation 전용, 라우팅된 모드) 이 옵션의 경우 *mapped_ifc*에 대해 특정 인터페이스를 구성해야 합니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. **service** 키워드도 지정하십시오. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다. 4-3 페이지의 고정 NAT 섹션을 참조하십시오. • Net-to-net - (선택 사항) NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째를 두 번째로 등과 같이 변환하려면 **net-to-net**을 지정합니다. 이 옵션이 없으면 IPv4-embedded 메서드가 사용됩니다. 일대일 변환에는 이 키워드를 반드시 사용해야 합니다. • DNS - (선택 사항) **dns** 키워드는 DNS 회신을 변환합니다. DNS 검사를 사용하도록 설정해야 합니다(기본적으로 사용됨). 4-32 페이지의 DNS 및 NAT 섹션을 참조하십시오. **service** 키워드를 지정하면 이 옵션을 사용할 수 없습니다. • 포트 변환 - (Static NAT-with-port-translation 전용) **tcp** 또는 **udp**와 실제 및 매핑된 포트를 지정합니다. 포트 번호 또는 잘 알려진 포트 이름(예: **ftp**)을 입력할 수 있습니다. • No Proxy ARP - (선택 사항) 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화하려면 **no-proxy-arp**를 지정합니다. 자세한 내용은 4-22 페이지의 매핑된 주소 및 라우팅 섹션을 참조하십시오.

예

다음 예는 DNS 재작성을 활성화하여 내부의 10.1.1.1에서 외부의 10.2.2.2로 실제 호스트에 대한 static NAT를 구성합니다.

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

다음 예는 매핑된 객체를 사용하여 내부의 10.1.1.1에서 외부의 10.2.2.2로 실제 호스트에 대한 static NAT를 구성합니다.

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

다음 예는 TCP 포트 21의 10.1.1.1에서 포트 2121의 외부 인터페이스로 static NAT-with-port-translation을 구성합니다.

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

다음 예는 내부 IPv4 네트워크를 외부 IPv6 네트워크로 매핑합니다.

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

다음 예는 내부 IPv6 네트워크를 외부 IPv6 네트워크로 매핑합니다.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

아이덴티티 NAT 구성

이 섹션에서는 네트워크 객체 NAT를 사용하여 아이덴티티 NAT를 구성하는 방법에 대해 설명합니다. 자세한 내용은 4-12 페이지의 아이덴티티 NAT 섹션을 참조하십시오.

자세한 단계

	명령	목적
1단계	(선택 사항) 매핑된 주소용 네트워크 객체를 만듭니다.	변환하려는 동일한 주소를 객체에 포함해야 합니다. 5-4 페이지의 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오.
2단계	**object network** *obj_name* **예:** `hostname(config)# object network my-host-obj1`	아이덴티티 NAT를 수행하려는 네트워크 객체를 구성하거나, 기존 네트워크 객체에 대해 객체 네트워크 컨피그레이션 모드로 들어갑니다. 이 네트워크 객체는 매핑된 네트워크 객체와 이름이 다르며(1단계 참조), 둘 모두 동일한 IP 주소를 포함하더라도 마찬가지입니다.

	명령	목적
3단계	{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*} 예: `hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`	새 네트워크 객체를 만드는 경우 아이덴티티 NAT를 수행할 실제 IP 주소(IPv4 또는 IPv6)를 정의합니다. 1단계에서 매핑된 주소용 네트워크 객체를 구성한 경우 해당 주소가 일치해야 합니다.
4단계	**nat** [(*real_ifc*,*mapped_ifc*)] **static** {*mapped_inline_ip* | *mapped_obj*} [**no-proxy-arp**] [**route-lookup**] 예: `hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS`	객체 IP 주소에 대해 **identity NAT**를 구성합니다. **참고** 한 객체에는 단일 NAT 규칙만 정의할 수 있습니다. 5-3 페이지의 추가 지침 섹션을 참조하십시오. 다음 지침을 참조하십시오. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • Mapped IP addresses - 매핑된 주소 및 실제 주소 모두에 대해 동일한 IP 주소를 구성해야 합니다. 다음 중 하나를 사용합니다. – 네트워크 객체 - 실제 객체와 동일한 IP 주소를 포함합니다(1단계 참조). – 인라인 IP 주소 - 매핑된 네트워크의 범위 또는 넷마스크가 실제 네트워크와 동일합니다. 예를 들어 실제 네트워크가 호스트이면 이 주소도 호스트 주소입니다. 범위의 경우 매핑된 주소에는 동일한 주소 번호가 실제 범위로서 포함됩니다. 예를 들어 실제 주소의 범위를 10.1.1.1~10.1.1.6으로 정의하고 매핑된 주소로 10.1.1.1을 지정하는 경우 매핑된 범위에는 10.1.1.1~10.1.1.6이 포함됩니다. • No Proxy ARP - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화하려면 **no-proxy-arp**를 지정합니다. 자세한 내용은 4-22 페이지의 매핑된 주소 및 라우팅 섹션을 참조하십시오. • Route lookup - (라우팅된 모드 전용, 인터페이스 지정) NAT 명령으로 지정한 인터페이스를 사용하는 대신 경로 조회를 사용하여 이그레스(egress) 인터페이스를 확인하려면 **route-lookup**을 지정합니다. 자세한 내용은 4-24 페이지의 이그레스(egress) 인터페이스 결정 섹션을 참조하십시오.

예

다음 예제는 인라인 매핑된 주소를 사용하여 호스트 주소를 자체에 매핑합니다.

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

다음 예제는 네트워크 객체를 사용하여 호스트 주소를 자체에 매핑합니다.

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

Per-Session PAT 규칙 구성

기본적으로 모든 TCP PAT 트래픽 및 모든 UDP DNS 트래픽은 Per-Session PAT를 사용합니다. 트래픽에 Multi-Session PAT를 사용하려면 Per-Session PAT 규칙을 구성할 수 있습니다. 허용 규칙은 Per-Session PAT를 사용하고 거부 규칙은 Multi-Session PAT를 사용합니다. Per-Session PAT 대 다중 세션 PAT에 대한 자세한 내용은 4-11 페이지의 Per-Session PAT 대 Multi-Session PAT을 참조하십시오.

기본값

기본적으로 다음 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 수동으로 만든 규칙 뒤에 항상 존재합니다. 규칙은 순서대로 평가되므로 기본 규칙을 재지정할 수 있습니다. 예를 들어 이러한 규칙을 완전히 무효화하려면 다음을 추가할 수 있습니다.

```
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
```

자세한 단계

명령	목적
xlate per-session {**permit** | **deny**} {**tcp** | **udp**} *source_ip* [*operator src_port*] *destination_ip operator dest_port* **예:** `hostname(config)# xlate per-session deny tcp any4 209.165.201.3 eq 1720`	허용 또는 거부 규칙을 만듭니다. 이 규칙은 기본 규칙 위에 배치되지만, 수동으로 만든 다른 모든 규칙 아래에 배치됩니다. 적용하고자 하는 순서대로 규칙을 만드십시오. 소스 및 수신 IP 주소에는 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*는 소스 주소 및 수신 주소에서 사용하는 포트 번호를 확인합니다. 허용되는 연산자는 다음과 같습니다. • lt - 보다 작음 • gt - 보다 큼 • eq - 같음 • neq - 같지 않음 • range - 포함하는 값의 범위. 이 연산자를 사용할 때는 예를 들면 다음과 같이 두 개의 포트 번호를 지정합니다. `range 100 200`

예

다음 예는 Multi-Session PAT를 사용할 수 있도록 H.323 트래픽용 거부 규칙을 만듭니다.

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

네트워크 객체 NAT 모니터링

객체 NAT를 모니터링하려면 다음 명령 중 하나를 입력합니다.

명령	목적
show nat	각 NAT 규칙의 건수를 포함한 NAT 통계를 표시합니다.
show nat pool	할당된 주소와 포트, 할당된 횟수 등을 포함한 NAT 풀 통계를 표시합니다.

명령	목적

`show running-config nat`	NAT 컨피그레이션을 표시합니다.
	
	참고 **show running-config object** 명령으로는 NAT 컨피그레이션을 볼 수 없습니다. **nat** 명령으로 아직 생성되지 않은 객체 또는 객체 그룹은 참조할 수 없습니다. **show** 명령 출력에서 전환 참조 또는 순환 참조를 피할 수 있도록 **show running-config** 명령은 **object** 명령을 두 번 표시합니다. 처음에는 IP 주소를 정의하고 다음에는 **nat** 명령을 정의합니다. 이 명령 출력에서는 객체가 먼저 정의되고 그 다음에 객체 그룹이 정의되며, 마지막으로 NAT가 정의됩니다. 예:
	
	`hostname# show running-config`
	`...`
	`object network obj1`
	`  range 192.168.49.1 192.150.49.100`
	`object network obj2`
	`  object 192.168.49.100`
	`object network network-1`
	`  subnet <network-1>`
	`object network network-2`
	`  subnet <network-2>`
	`object-group network pool`
	`  network-object object obj1`
	`  network-object object obj2`
	`...`
	`object network network-1`
	`  nat (inside,outside) dynamic pool`
	`object network network-2`
	`  nat (inside,outside) dynamic pool`

show xlate	현재의 NAT 세션 정보를 표시합니다.

네트워크 객체 NAT의 컨피그레이션 예

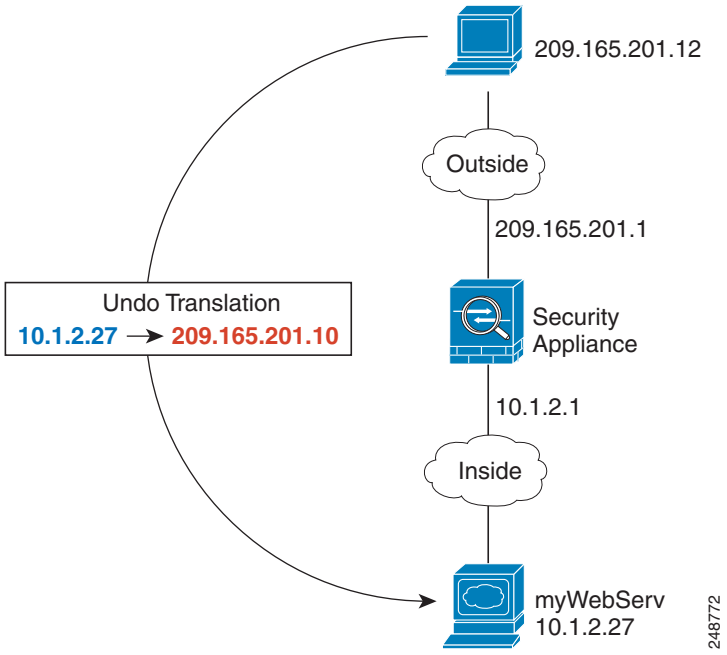
이 섹션에서는 다음 컨피그레이션 예를 다룹니다.

- 5-18 페이지의 내부 웹 서버에 대한 액세스 제공(고정 NAT)
- 5-19 페이지의 내부 호스트용 NAT(동적 NAT) 및 외부 웹 서버용 NAT(고정 NAT)
- 5-20 페이지의 여러 매핑된 주소가 있는 내부 로드 밸런서(Static NAT, 일대다)
- 5-21 페이지의 FTP, HTTP 및 SMTP용 단일 주소(Static NAT-with-Port-Translation)
- 5-22 페이지의 매핑된 인터페이스의 DNS 서버, 실제 인터페이스의 웹 서버(고정 NAT와 DNS 수정)
- 5-24 페이지의 매핑된 인터페이스의 DNS 서버 및 FTP 서버, FTP 서버 변환됨(고정 NAT와 DNS 수정)
- 5-25 페이지의 매핑된 인터페이스의 IPv4 DNS 서버 및 FTP 서버, 실제 인터페이스의 IPv6 호스트(고정 NAT64와 DNS64 수정)

내부 웹 서버에 대한 액세스 제공(고정 NAT)

다음 예제는 내부 웹 서버에 대해 고정(static) NAT를 수행합니다. 실제 주소는 사설 네트워크에 있으므로 공용 주소가 필요합니다. 호스트가 고정된 주소에서 웹 서버에 대한 트래픽을 시작할 수 있으려면 고정 NAT가 필요합니다. (그림 5-1 참조).

그림 5-1 내부 웹 서버에 대한 고정 NAT



1단계 내부 웹 서버용 네트워크 객체를 만듭니다.

```
hostname(config)# object network myWebServ
```

2단계 웹 서버 주소를 정의합니다.

```
hostname(config-network-object)# host 10.1.2.27
```

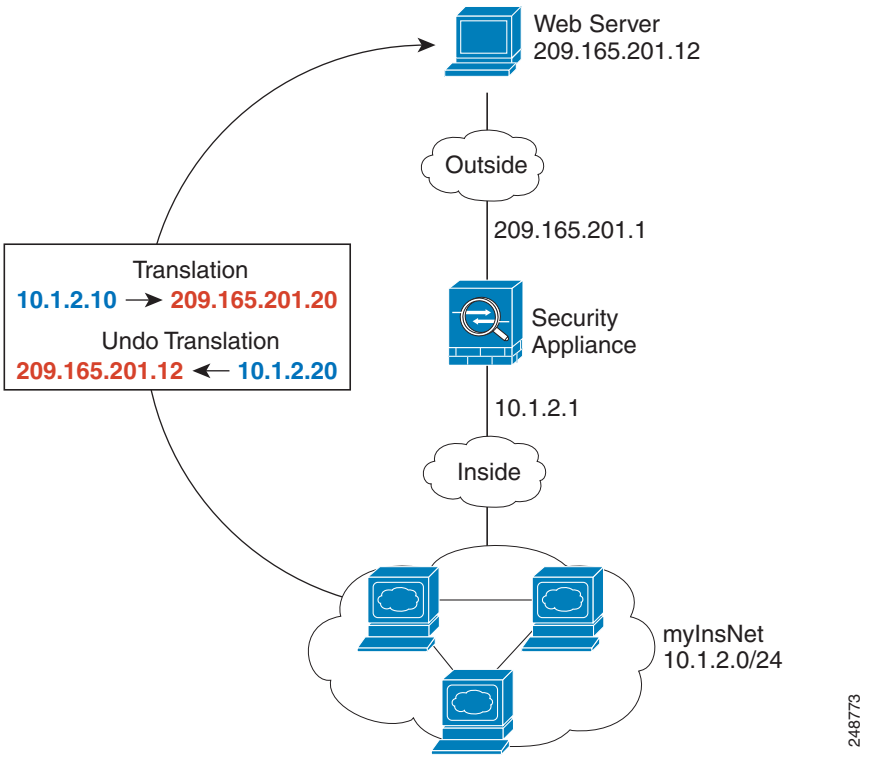
3단계 객체용 고정 NAT를 구성합니다.

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

내부 호스트용 NAT(동적 NAT) 및 외부 웹 서버용 NAT(고정 NAT)

다음 예는 사설 네트워크의 내부 사용자가 외부에서 액세스하는 경우를 위한 동적 NAT를 구성합니다. 내부 사용자가 외부 웹 서버에 연결하는 경우도 포함됩니다. 이 경우 웹 서버 주소가 내부 네트워크에 있는 것처럼 보이는 주소로 변환됩니다. (그림 5-2 참조).

그림 5-2 내부용 동적 NAT, 외부 웹 서버용 고정 NAT



1단계 내부 주소를 변환할 동적 NAT 풀용 네트워크 객체를 만듭니다.

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

2단계 내부 네트워크용 네트워크 객체를 만듭니다.

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

3단계 내부 네트워크용 동적 NAT를 활성화합니다.

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

4단계 외부 웹 서버용 네트워크 객체를 만듭니다.

```
hostname(config)# object network myWebServ
```

5단계 웹 서버 주소를 정의합니다.

```
hostname(config-network-object)# host 209.165.201.12
```

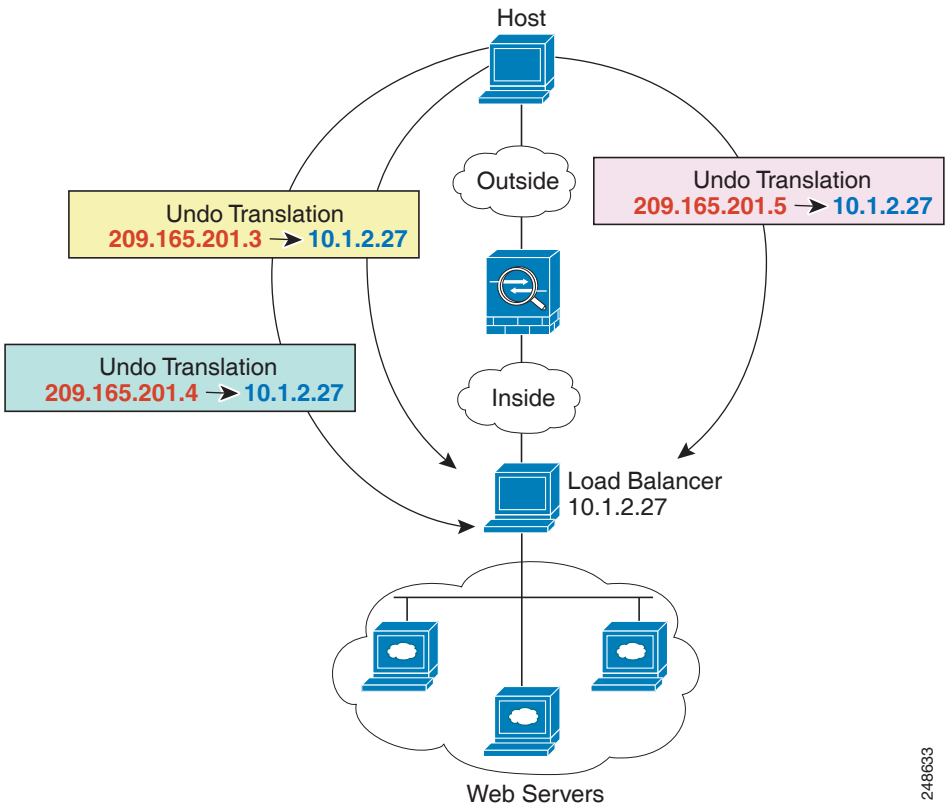
6단계 웹 서버용 고정 NAT를 구성합니다.

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

여러 매핑된 주소가 있는 내부 로드 밸런서(Static NAT, 일대다)

다음 예는 여러 IP 주소로 변환되는 내부 로드 밸런서를 보여줍니다. 외부 호스트가 매핑된 IP 주소 중 하나에 액세스하는 경우 단일 로드 밸런서 주소로 변환되지 않습니다. 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다. (그림 5-3 참조).

그림 5-3 내부 로드 밸런서용 일대다 고정 NAT



1단계 로드 밸런서를 매핑하려는 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

2단계 로드 밸런서용 네트워크 객체를 만듭니다.

```
hostname(config)# object network myLBHost
```

3단계 로드 밸런서 주소를 정의합니다.

```
hostname(config-network-object)# host 10.1.2.27
```

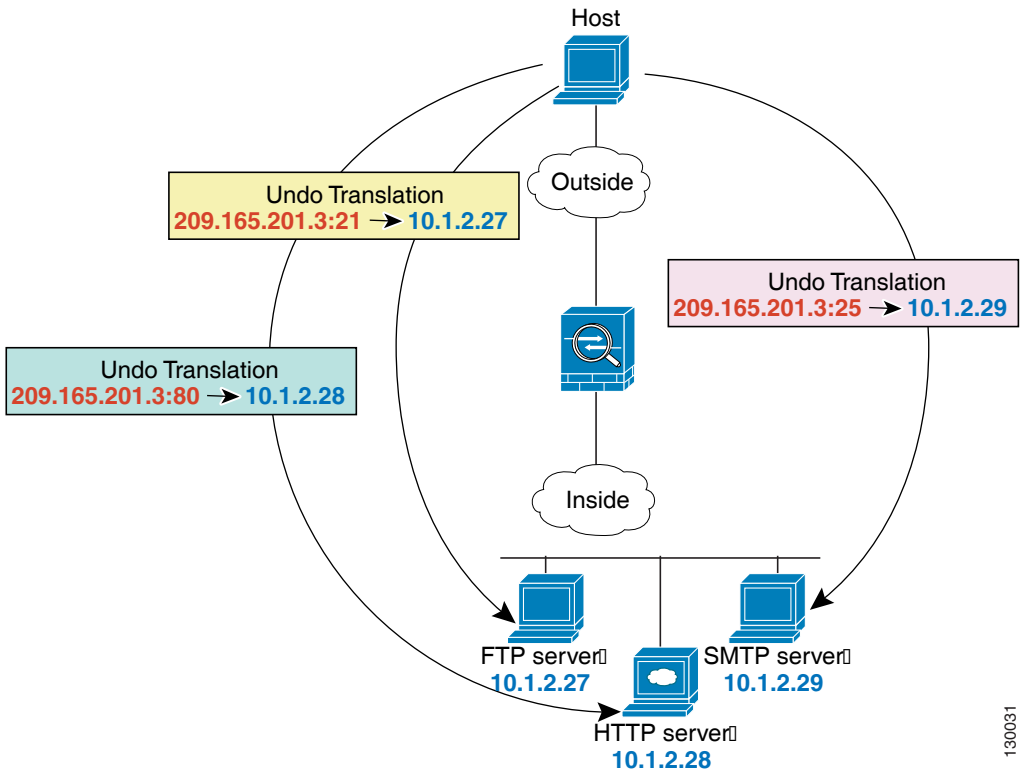
4단계 로드 밸런서용 고정(static) NAT를 구성합니다.

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

FTP, HTTP 및 SMTP용 단일 주소(Static NAT-with-Port-Translation)

다음의 static NAT-with-port-translation 예는 원격 사용자가 FTP, HTTP 및 SMTP에 액세스하기 위해 사용할 단일 주소를 제공합니다. 이러한 서버는 실제 네트워크에서 실제로 서로 다른 디바이스이지만, 각 서버에 대해 동일한 매핑된 IP 주소를 사용하되 포트는 다른 static NAT-with-port-translation 규칙을 지정할 수 있습니다. (그림 5-4 참조.)

그림 5-4 Static NAT-with-Port-Translation



1단계 FTP 서버 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network FTP_SERVER
```

2단계 FTP 서버 주소를 정의하고, FTP 서버용 아이덴티티 포트 변환으로 고정 NAT를 구성합니다.

```
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
ftp
```

3단계 HTTP 서버 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network HTTP_SERVER
```

4단계 HTTP 서버 주소를 정의하고, HTTP 서버용 아이덴티티 포트 변환으로 고정 NAT를 구성합니다.

```
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
http http
```

5단계 SMTP 서버 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network SMTP_SERVER
```

6단계 SMTP 서버 주소를 정의하고, SMTP 서버용 아이덴티티 포트 변환으로 고정 NAT를 구성합니다.

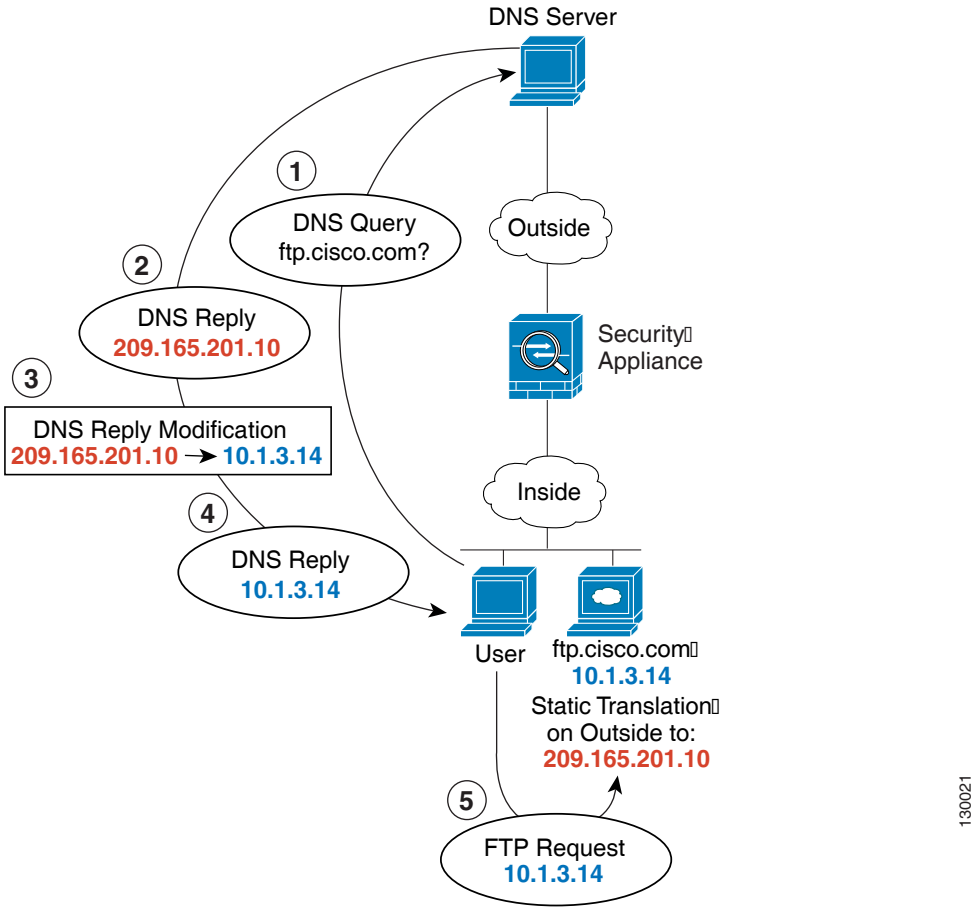
```
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
smtp smtp
```

매핑된 인터페이스의 DNS 서버, 실제 인터페이스의 웹 서버(고정 NAT와 DNS 수정)

예를 들어 DNS 서버는 외부 인터페이스에서 액세스 가능합니다. ftp.cisco.com 서버는 내부 인터페이스에 있습니다. ftp.cisco.com 실제 주소(10.1.3.14)를 외부 네트워크에서 보이는 매핑된 주소(209.165.201.10)로 고정으로 변환하도록 ASA를 구성하십시오. (그림 5-5 참조.) 이 경우, 실제 주소를 사용하여 ftp.cisco.com에 액세스할 수 있는 내부 사용자가 DNS 서버에서 실제 주소(매핑된 주소가 아님)를 받을 수 있도록 고정 규칙에 대한 DNS 회신 수정을 활성화할 수 있습니다.

내부 호스트가 ftp.cisco.com 주소에 DNS 요청을 전송하면, DNS 서버는 매핑된 주소(209.165.201.10)로 회신합니다. ASA는 내부 서버에 대한 고정 규칙을 참조하여 DNS 회신에 있는 주소를 10.1.3.14로 변환합니다. DNS 회신 수정을 활성화하지 않으면 내부 호스트는 ftp.cisco.com에 직접 액세스하는 대신 트래픽을 209.165.201.10으로 전송하려고 시도하게 됩니다.

그림 5-5 DNS 회신 수정



1단계 FTP 서버 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network FTP_SERVER
```

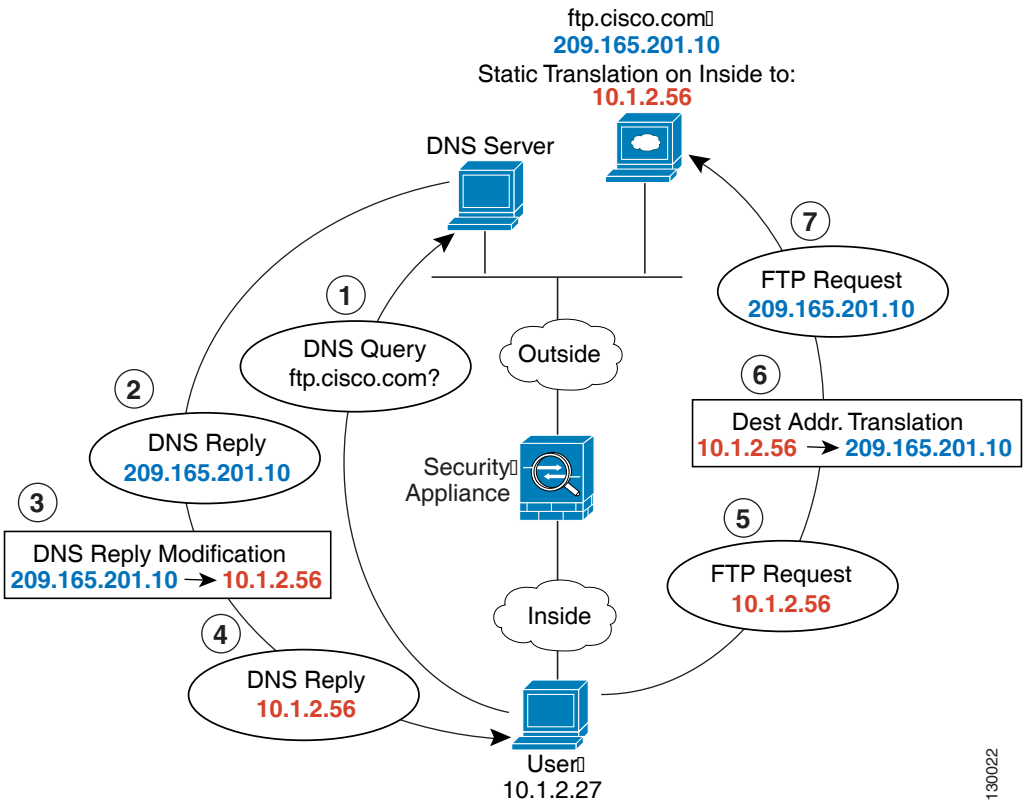
2단계 DNS 서버 주소를 정의하고, DNS 수정으로 고정 NAT를 구성합니다.

```
hostname(config-network-object)# host 10.1.3.14
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

매핑된 인터페이스의 DNS 서버 및 FTP 서버, FTP 서버 변환됨(고정 NAT와 DNS 수정)

그림 5-6에서는 외부의 FTP 서버 및 DNS 서버를 보여줍니다. ASA는 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.201.10으로 응답합니다. 내부 사용자가 ftp.cisco.com(10.1.2.56)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다.

그림 5-6 외부 NAT를 사용한 DNS 회신 수정



1단계 FTP 서버 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network FTP_SERVER
```

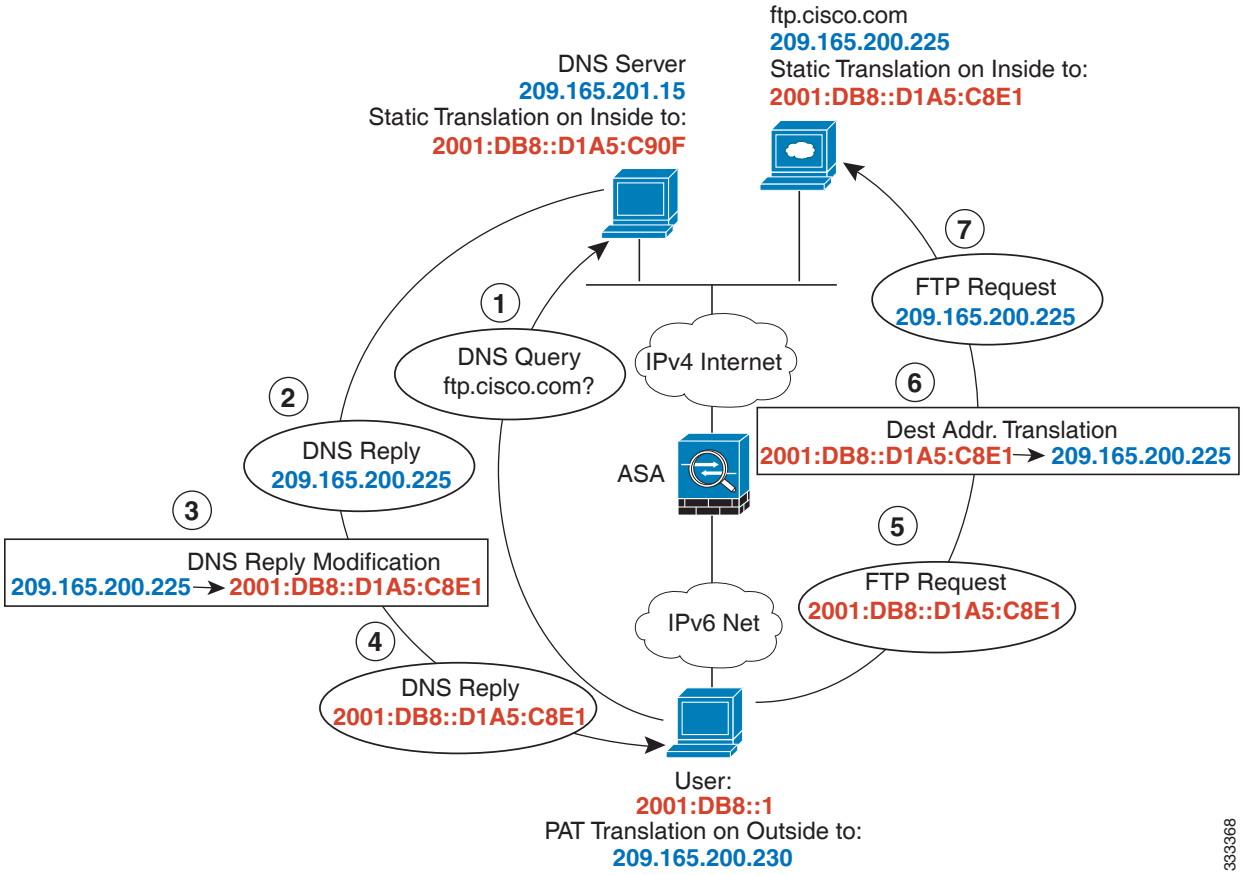
2단계 DNS 서버 주소를 정의하고, DNS 수정으로 고정 NAT를 구성합니다.

```
hostname(config-network-object)# host 209.165.201.10
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

매핑된 인터페이스의 IPv4 DNS 서버 및 FTP 서버, 실제 인터페이스의 IPv6 호스트(고정 NAT64와 DNS64 수정)

그림 5-6에서는 외부의 IPv4 네트워크에 있는 FTP 서버 및 DNS 서버를 보여줍니다. ASA는 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 IPv6 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.200.225로 응답합니다. 내부 사용자가 ftp.cisco.com(2001:DB8::D1A5:C8E1)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다. 이 예에는 DNS 서버용 고정 NAT 변환 및 내부 IPv6 호스트용 PAT 규칙도 포함되어 있습니다.

그림 5-7 외부 NAT를 사용한 DNS 회신 수정



1단계 FTP 서버에 대해 DNS 수정으로 고정 NAT를 구성합니다.

a. FTP 서버 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network FTP_SERVER
```

b. FTP 서버 주소를 정의하고, DNS 수정으로 고정 NAT를 구성합니다. 이 변환은 일대일 방식이므로 NAT46에 대해 net-to-net 메서드를 구성합니다.

```
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

2단계 DNS 서버용 NAT를 구성합니다.

a. DNS 서버 주소용 네트워크 객체를 만듭니다.

```
hostname(config)# object network DNS_SERVER
```

b. DNS 서버 주소를 정의하고, net-to-net 메서드를 사용해 고정 NAT를 구성합니다.

```
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

3단계 내부 IPv6 네트워크 변환을 위한 IPv4 PAT 풀을 구성합니다.

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
```

4단계 내부 IPv6 네트워크용 PAT를 구성합니다.

a. 내부 IPv6 네트워크용 네트워크 객체를 만듭니다.

```
hostname(config)# object network IPv6_INSIDE
```

b. IPv6 네트워크 주소를 정의하고, PAT 풀을 사용하여 동적 NAT를 구성합니다.

```
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

네트워크 객체 NAT의 기능 기록

표 5-1에는 각 기능 변경 사항 및 그것이 구현된 플랫폼 릴리스가 나열되어 있습니다.

표 5-1 네트워크 객체 NAT의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
네트워크 객체 NAT	8.3(1)	네트워크 객체 IP 주소용 NAT를 구성합니다. 추가 또는 수정된 명령: **nat**(객체 네트워크 컨피그레이션 모드), **show nat**, **show xlate**, **show nat pool**.
아이덴티티 NAT 구성 가능 프록시 ARP 및 경로 조회	8.4(2)/8.5(1)	아이덴티티 NAT의 이전 릴리스에서는 프록시 ARP가 비활성화되었고, 이그레스(egress) 인터페이스를 확인하는 데 항상 경로 조회가 사용되었습니다. 이러한 설정을 구성할 수 없었습니다. 8.4(2) 이상에서는 아이덴티티 NAT에 대한 기본 동작이 다른 고정 NAT 컨피그레이션의 동작과 일치하도록 변경되었습니다. 프록시 ARP가 활성화되며, 기본적으로 NAT 컨피그레이션이 이그레스(egress) 인터페이스(지정한 경우)를 확인합니다. 이러한 설정을 그대로 둘 수도 있고, 별도로 활성화 또는 비활성화할 수도 있습니다. 이제 정기적인 고정 NAT를 위해 프록시 ARP를 비활성화할 수도 있습니다. 8.3(1), 8.3(2) 및 8.4(1)에서 8.4(2)로 업그레이드하면, 이제 기존 기능을 유지할 수 있도록 모든 아이덴티티 NAT 컨피그레이션에 **no-proxy-arp** 및 **route-lookup** 키워드가 포함됩니다. 수정된 명령: **nat static** [**no-proxy-arp**] [**route-lookup**].
PAT 풀 및 라운드 로빈 주소 할당	8.4(2)/8.5(1)	이제 단일 주소 대신 PAT 주소의 풀을 지정할 수 있습니다. 풀의 다음 주소를 사용하기 전에 먼저 PAT 주소의 모든 포트를 사용하는 대신, 선택적으로 PAT 주소를 라운드 로빈 방식으로 할당할 수도 있습니다. 이 기능을 이용하면 단일 PAT 주소에서 많은 연결이 설정되는 것(DoS 공격의 일부처럼 보임)을 효과적으로 방지하고, 다수의 PAT 주소를 손쉽게 구성할 수 있습니다. 수정된 명령: **nat dynamic** [**pat-pool** *mapped_object* [**round-robin**]].
라운드 로빈 PAT 풀 할당은 기존 호스트에 동일한 IP 주소를 사용합니다.	8.4(3)	라운드 로빈 할당으로 PAT 풀을 사용할 때 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. 수정된 명령이 없습니다. *이 기능은 8.5(1) 또는 8.6(1)에서 사용할 수 없습니다.*

표 5-1 네트워크 객체 NAT의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
AT 풀용 PAT 포트의 균일한 범위	8.4(3)	사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 *없는* 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다. PAT 풀을 사용할 때 낮은 포트 범위를 사용하는 트래픽이 많은 경우 이제 크기가 서로 다른 세 가지 계층 대신 균일한 포트 범위(1024~65535 또는 1~65535)를 사용하도록 지정할 수 있습니다. 수정된 명령: **nat dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]]. *이 기능은 8.5(1) 또는 8.6(1)에서 사용할 수 없습니다.*
PAT 풀용 확장 PAT	8.4(3)	각 PAT IP 주소는 최대 65535개 포트를 허용합니다. 65535개 포트가 충분한 변환을 제공하지 않으면 이제 PAT 풀용 확장 PAT를 활성화할 수 있습니다. 확장 PAT는 변환 정보의 수신 주소 및 포트를 포함하여 *서비스*당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 수정된 명령: **nat dynamic** [**pat-pool** *mapped_object* [**extended**]]. *이 기능은 8.5(1) 또는 8.6(1)에서 사용할 수 없습니다.*

표 5-1 네트워크 객체 NAT의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
VPN 피어의 로컬 IP 주소를 피어의 실제 IP 주소로 변환하는 자동 NAT 규칙	8.4(3)	드문 경우이지만 할당된 로컬 IP 주소 대신 내부 네트워크에 있는 VPN 피어의 실제 IP 주소를 사용하고자 할 수 있습니다. 일반적으로 VPN에서는 내부 네트워크에 액세스할 수 있도록, 할당된 로컬 IP 주소를 피어에 제공합니다. 그러나 예를 들어 내부 서버 및 네트워크 보안이 피어의 실제 IP 주소를 기반으로 하는 경우, 로컬 IP 주소를 피어의 실제 공개 IP 주소로 다시 변환할 수 있습니다. 터널 그룹당 한 인터페이스에서 이 기능을 활성화할 수 있습니다. VPN 세션이 설정되거나 연결이 해제되면 객체 NAT 규칙이 동적으로 추가 및 삭제됩니다. **show nat** 명령을 사용하여 규칙을 볼 수 있습니다. **참고** 라우팅 문제 때문에, 반드시 필요한 경우가 아니면 이 기능을 사용하지 않는 것이 좋습니다. 네트워크와의 기능 호환성을 확인하려면 Cisco TAC에 문의하십시오. 다음 제한을 참조하십시오. • Cisco IPsec 및 AnyConnect 클라이언트만 지원합니다. • NAT 정책과 VPN 정책이 적용될 수 있도록, 공개 IP 주소로 반환되는 트래픽을 ASA로 다시 라우팅해야 합니다. • 부하 균형을 지원하지 않습니다(라우팅 문제 때문). • 로밍을 지원하지 않습니다(공개 IP 변경). 추가된 명령: **nat-assigned-to-public-ip** *interface*(tunnel-group general-attributes 구성 모드).
NAT에서 IPv6 지원	9.0(1)	NAT는 이제 IPv6 트래픽은 물론 IPv4 및 IPv6 간 변환도 지원합니다. 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 수정된 명령: **nat**(객체 네트워크 컨피그레이션 모드), **show nat**, **show nat pool**, **show xlate**.

표 5-1 네트워크 객체 NAT의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
NAT에서 역 DNS 조회 지원	9.0(1)	NAT 규칙용 DNS 검사를 활성화하여 IPv4 NAT, IPv6 NAT 및 NAT64를 사용할 경우 NAT는 이제 역 DNS 조회를 위한 DNS PTR 레코드의 변환을 지원합니다.
Per-Session PAT	9.0(1)	Per-Session PAT 기능은 PAT의 확장성을 개선하며, 클러스터링의 경우 각 멤버 유닛이 PAT 연결을 소유하도록 허용합니다. Multi-Session PAT 연결은 마스터 유닛에서 전달 및 소유해야 합니다. Per-Session PAT 세션이 끝날 무렵 ASA는 재설정을 전송하고 xlate를 즉시 제거합니다. 재설정을 통해 종료 노드에서 연결을 즉시 해제하므로 TIME_WAIT 상태를 피할 수 있습니다. 반면 다중 세션 PAT는 PAT 시간 제한을 사용합니다(기본값 30초). "hit-and-run" 트래픽(예: HTTP 또는 HTTPS)의 경우 Per-Session 기능은 한 주소에 의해 지원되는 연결 속도를 극적으로 높일 수 있습니다. Per-Session 기능을 사용하지 않으면 IP 프로토콜에 대한 한 주소의 최대 연결 속도는 약 초당 2000입니다. Per-Session 기능을 사용하면 IP 프로토콜에 대한 한 주소의 연결 속도는 65535/*average-lifetime*입니다. 기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽은 Per-Session PAT xlate를 사용합니다. Multi-Session PAT가 필요한 트래픽(예: H.323, SIP 또는 Skinny)의 경우 Per-Session 거부 규칙을 만들어 Per-Session PAT를 비활성화할 수 있습니다. 추가된 명령: **xlate per-session**, **show nat pool**.

6 장

Twice NAT

Twice NAT에서는 소스 주소와 수신 주소를 단일 규칙에서 식별할 수 있습니다. 이 장에서는 Twice NAT 구성 방법에 대해 설명합니다.

참고 NAT 작동 방식에 대한 자세한 내용은 4 장, “NAT(Network Address Translation)”을 참조하십시오.

Twice NAT에 대한 정보

Twice NAT에서는 소스 주소와 수신 주소를 단일 규칙에서 식별할 수 있습니다. 소스 주소와 수신 주소를 모두 지정하면, 예를 들어 수신 X로 이동할 경우 소스 주소가 A로 변환되고 수신 Y로 이동할 경우 B로 변환되도록 지정할 수 있습니다.

참고 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "소스(source)"와 "수신(destination)"이 사용됩니다. 특정 연결이 "수신" 주소에서 시작되는 경우에도 마찬가지입니다. Static NAT with port address translation을 구성하고, 소스 주소를 텔넷 서버로 지정하며, 텔넷 서버로 이동하는 모든 트래픽에 대해 포트를 2323에서 23으로 변환하려면 명령에서 *source* 포트가 변환되도록 지정해야 합니다(real: 23, mapped: 2323). 텔넷 서버 주소를 소스 주소로 지정했기 때문에 소스 포트를 지정하는 것입니다.

수신 주소는 선택 사항입니다. 수신 주소를 지정하는 경우 이를 수신 주소 자신에게 매핑할 수도 있고(아이덴티티 NAT) 다른 주소에 매핑할 수도 있습니다. 수신 주소 매핑은 항상 고정 매핑입니다.

또한 Twice NAT를 사용하는 경우 static NAT-with-port-translation에 대해 서비스 객체를 사용할 수 있습니다. 네트워크 객체 NAT는 인라인 정의만 수용합니다.

Twice NAT 및 네트워크 객체 NAT의 차이에 대한 자세한 내용은 4-15 페이지의 NAT 구현 방법을 참조하십시오.

Twice NAT 규칙은 NAT 규칙 테이블의 섹션 1(지정한 경우 섹션 3)에 추가됩니다. NAT 순서에 대한 자세한 내용은 4-20 페이지의 NAT 규칙 순서를 참조하십시오.

Twice NAT의 라이센싱 요구 사항

모델	라이센스 요구 사항
ASAv	표준 또는 프리미엄 라이센스
모든 다른 모델	기본 라이센스

Twice NAT 전제 조건

- 실제 주소와 매핑된 주소 모두에 대해 네트워크 객체 또는 네트워크 객체 그룹을 구성합니다(**object network** 또는 **object-group network** 명령). 네트워크 객체 그룹은 비연속 IP 주소 범위 또는 다중 호스트나 서브넷을 이용해 매핑된 주소 풀을 만드는 데 특히 유용합니다. 네트워크 객체 또는 그룹을 만들려면 일반 운영 컨피그레이션 가이드를 참조하십시오.
- Static NAT-with-port-translation에 대해 TCP 또는 UDP 서비스 객체를 구성합니다(**object service** 명령). 서비스 객체를 만들려면 일반 운영 컨피그레이션 가이드을 참조하십시오.

객체 및 그룹에 대한 특정 지침은 구성할 NAT 유형에 대한 컨피그레이션 섹션을 참조하십시오. 또한 6-2 페이지의 지침 및 제한 섹션을 참조하십시오.

지침 및 제한

이 섹션에서는 이 기능의 지침 및 제한에 대해 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원됩니다.

방화벽 모드 지침

- 투명 및 라우팅된 방화벽 모드에서 지원됩니다.
- 투명 모드에서는 실제(real) 및 매핑된(mapped) 인터페이스를 지정해야 합니다. **any**는 사용할 수 없습니다.
- 투명 모드에서는 인터페이스 PAT를 구성할 수 없습니다. 투명 모드 인터페이스에는 IP 주소가 없기 때문입니다. 관리 IP 주소를 매핑된 주소로서 사용할 수도 없습니다.
- 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 두 IPv6 네트워크 간 변환 또는 두 IPv4 네트워크 간 변환은 지원됩니다.

IPv6 지침

- IPv6을 지원합니다.
- 라우팅된 모드에서는 IPv4와 IPv6 간에 변환할 수 있습니다.
- 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 두 IPv6 네트워크 간 변환 또는 두 IPv4 네트워크 간 변환은 지원됩니다.
- 투명 모드에서는 IPv6에 대해 PAT 풀이 지원되지 않습니다.
- 고정(Static) NAT에서는 IPv6 서브넷을 최대 /64까지 지정할 수 있습니다. 더 큰 서브넷은 지원되지 않습니다.
- FTP with NAT46을 사용할 때, IPv4 FTP 클라이언트가 IPv6 FTP 서버에 연결될 때 클라이언트는 확장 패시브 모드(EPSV) 또는 확장 포트 모드(EPRT)를 사용해야 하며, PASV 및 PORT 명령은 IPv6에서 지원되지 않습니다.

추가 지침

- 소스 IP 주소가 서브넷이면(또는 보조 연결을 사용하는 기타 애플리케이션이면) FTP 목적지 포트 변환을 구성할 수 없으며, FTP 데이터 채널을 성공적으로 설정할 수 없습니다. 예를 들어 다음 컨피그레이션은 작동하지 않습니다.

```
object network MyInsNet
 subnet 10.1.2.0 255.255.255.0
object network MapInsNet
 subnet 209.165.202.128 255.255.255.224
object network Server1
 host 209.165.200.225
object network Server1_mapped
 host 10.1.2.67
object service REAL_ftp
 service tcp destination eq ftp
object service MAPPED_ftp
 service tcp destination eq 2021
object network MyOutNet
 subnet 209.165.201.0 255.255.255.224

nat (inside,outside) source static MyInsNet MapInsNet destination static
Server1_mapped Server1 service MAPPED_ftp REAL_ftp
```

- NAT 컨피그레이션을 변경한 경우 새 NAT 정보가 사용되기 전 기존 변환이 시간 초과되기까지 기다리고 싶지 않다면 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 변환을 사용하는 현재의 모든 연결이 해제됩니다.

참고 동적 NAT 또는 PAT 규칙을 제거한 후 제거된 규칙의 주소와 겹치는 매핑된 주소로 새 규칙을 추가하는 경우, 새 규칙을 사용하려면 제거된 규칙과 관련된 모든 연결이 시간 초과되기까지 기다리거나 **clear xlate** 명령으로 해당 연결을 지워야 합니다. 이러한 안전 조치는 동일한 주소가 여러 호스트에 할당되는 것을 방지합니다.

- IPv4 및 IPv6 주소를 모두 포함하는 객체 그룹은 사용할 수 없습니다. 객체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
- NAT 규칙에서 **any** 키워드를 사용하는 경우 "any" 트래픽의 정의(IPv4 대 IPv6)는 규칙에 따라 다릅니다. ASA가 패킷에 대해 NAT를 수행하기 전에 패킷은 IPv6-to-IPv6 또는 IPv4-to-IPv4여야 합니다. 이 전제 조건하에 ASA는 NAT 규칙에서 **any**의 값을 결정할 수 있습니다. 예를 들어 "any"에서 IPv6 서버로 규칙을 구성하며 해당 서버가 IPv4 주소에서 매핑된 것이면 **any**는 "모든 IPv6 트래픽"을 의미합니다. "any"에서 "any"로 규칙을 구성하며 소스를 인터페이스 IPv4 주소로 매핑하면 **any**는 "모든 IPv4 트래픽"을 의미합니다. 매핑된 인터페이스 주소는 수신 주소도 IPv4임을 암시하기 때문입니다.

- NAT의 객체 및 객체 그룹은 정의하지 않고 사용할 수 없으며, IP 주소를 반드시 포함해야 합니다.
- 여러 규칙에서 동일한 객체를 사용할 수 있습니다.
- 매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.
  - 매핑된 인터페이스 IP 주소. 규칙에 대해 **any** 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅된 모드만)의 경우 IP 주소 대신 **interface** 키워드를 사용합니다.
  - (투명 모드) 관리 IP 주소.
  - (동적 NAT) VPN이 활성화된 경우의 대기 인터페이스 IP 주소.
  - 기존의 VPN 풀 주소.
- 고정 및 동적 NAT 정책에서는 겹치는 주소 사용을 피해야 합니다. 예를 들어, PPTP의 보조 연결이 동적 xlate 대신 고정 상태인 경우 겹치는 주소를 사용하면 PPTP 연결 설정에 실패할 수 있습니다.
- NAT용 트랜잭션 커밋 모델을 사용하여 시스템 성능과 신뢰성을 높일 수 있습니다. 자세한 내용은 일반 운영 컨피그레이션 가이드의 기본 설정 장을 참조하십시오. **asp rule-engine transactional-commit nat** 명령을 사용하십시오.

기본 설정

- 기본적으로 규칙은 NAT 테이블의 섹션 1 끝에 추가됩니다.
- (라우팅된 모드) 기본적인 실제 및 매핑된 인터페이스는 모든 인터페이스에 규칙을 적용하는 Any입니다.
- 사용자가 선택적인 인터페이스를 지정하는 경우 ASA에서는 NAT 컨피그레이션을 사용하여 이그레스(egress) 인터페이스를 결정합니다, 대신 항상 경로 조회를 사용할 수 있는 옵션이 사용자에게 제공됩니다.

Twice NAT 구성

이 섹션에서는 Twice NAT 구성 방법에 대해 설명합니다.

- 6-5 페이지의 실제 및 매핑된 주소에 대해 네트워크 객체 추가
- 6-6 페이지의 (선택 사항) 실제 및 매핑된 포트에 대해 서비스 객체 추가
- 6-8 페이지의 동적 NAT
- 6-10 페이지의 동적 PAT(숨김) 구성
- 6-15 페이지의 Static NAT 또는 Static NAT-with-Port-Translation 구성
- 6-18 페이지의 아이덴티티 NAT 구성
- 6-20 페이지의 Per-Session PAT 규칙 구성

실제 및 매핑된 주소에 대해 네트워크 객체 추가

각 NAT 규칙에 대해 최대 4개의 네트워크 객체 또는 그룹을 구성합니다.

- **소스 실제 주소**
- **소스 매핑된 주소**
- **수신 실제 주소**
- **수신 매핑된 주소**

모든 트래픽을 나타내기 위해 **any** 키워드 인라인을 지정하지 않는 경우 또는 일부 NAT 유형에서 인터페이스 주소를 나타내기 위해 **interface** 키워드를 지정하지 않는 경우 객체가 필요합니다. 네트워크 객체 또는 그룹 구성에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

지침

- 네트워크 객체 그룹은 IPv4 또는 IPv6 주소의 인라인 주소 및/또는 객체를 포함할 수 있습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.
- 허용되지 않는 매핑된 IP 주소에 대한 자세한 내용은 6-2 페이지의 지침 및 제한을 참조하십시오.
- Source Dynamic NAT:
  - 일반적으로 더 큰 실제 주소 그룹을 더 작은 그룹에 매핑하도록 구성합니다.
  - 매핑된 객체 또는 그룹에 서브넷을 포함할 수 없습니다. 객체는 범위를 정의해야 하고, 그룹은 호스트와 범위를 포함할 수 있습니다.
  - 매핑된 네트워크 객체에 범위와 호스트 IP 주소가 모두 포함되어 있으면 범위는 동적 NAT에 사용되고 호스트 IP 주소는 PAT 대안(fallback)으로 사용됩니다.
- Source Dynamic PAT(Hide):
  - 매핑된 객체 또는 그룹은 서브넷을 포함할 수 없습니다. 네트워크 객체는 호스트(또는 PAT 풀의 경우 범위)를 정의해야 합니다. 네트워크 객체 그룹(PAT 풀의 경우)은 호스트와 범위를 포함할 수 있습니다.
- Source Static NAT 또는 Static NAT with port translation:
  - 매핑된 객체 또는 그룹은 호스트, 범위 또는 서브넷을 포함할 수 있습니다.
  - 고정 매핑은 일반적으로 1대1이므로, 실제 주소의 수가 매핑된 주소의 수와 같습니다. 그러나 원하는 경우 수량을 다르게 지정할 수 있습니다. 자세한 내용은 4-3 페이지의 고정 NAT 섹션을 참조하십시오.
- Source Identity NAT
  - 실제 객체 및 매핑된 객체가 일치해야 합니다. 동일한 객체를 사용할 수도 있고, 동일한 IP 주소를 포함하는 별도의 객체를 만들 수도 있습니다.
- Destination Static NAT 또는 Static NAT with port translation(대상 변환은 항상 고정임):
  - Twice NAT의 주요 기능은 수신 IP 주소를 포함하는 것이지만, 수신 주소는 선택 사항입니다. 수신 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 아이덴티티 NAT를 사용할 수도 있습니다. 실제 주소에 네트워크 객체 그룹 사용, 수동으로 규칙 순서 지정 등을 비롯한 Twice NAT의 몇 가지 다른 기능을 활용하려면 수신 주소 없이 Twice NAT를 구성할 수 있습니다. 자세한 내용은 4-15 페이지의 네트워크 객체 NAT와 Twice NAT의 주요 차이점 섹션을 참조하십시오.
  - 아이덴티티 NAT의 경우 실제 객체 및 매핑된 객체가 일치해야 합니다. 양쪽에 동일한 객체를 사용할 수도 있고, 동일한 IP 주소를 포함하는 별도의 객체를 만들 수도 있습니다.

- 고정 매핑은 일반적으로 1대1이므로, 실제 주소의 수가 매핑된 주소의 수와 같습니다. 그러나 원하는 경우 수량을 다르게 지정할 수 있습니다. 자세한 내용은 4-3 페이지의 고정 NAT 섹션을 참조하십시오.
- Static interface NAT with port translation(라우팅된 모드 전용)의 경우 매핑된 주소의 네트워크 객체/그룹 대신 **interface** 키워드를 지정할 수 있습니다. 자세한 내용은 4-5 페이지의 Static Interface NAT with Port Translation 섹션을 참조하십시오.

자세한 단계

명령	목적

object network *obj_name*
{**host** *ip_address* | **subnet** *subnet_address netmask* | **range** *ip_address_1 ip_address_2*}
 	
예:
`hostname(config)# object network MyInsNet`
`hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0`
	네트워크 객체 IPv4 또는 IPv6을 추가합니다.

object-group network *grp_name*
{**network-object** {**object** *net_obj_name* | *subnet_address netmask* |
host *ip_address*} |
group-object *grp_obj_name*}
 	
예:
`hostname(config)# object network TEST`
`hostname(config-network-object)# range 10.1.1.1 10.1.1.70`
 	
`hostname(config)# object network TEST2`
`hostname(config-network-object)# range 10.1.2.1 10.1.2.70`
 	
`hostname(config-network-object)# object-group network MAPPED_IPS`
`hostname(config-network)# network-object object TEST`
`hostname(config-network)# network-object object TEST2`
`hostname(config-network)# network-object host 10.1.2.79`
	네트워크 객체 그룹 IPv4 또는 IPv6을 추가합니다.

(선택 사항) 실제 및 매핑된 포트에 대해 서비스 객체 추가

다음에 대해 서비스 객체를 구성합니다.

- **소스 실제 포트(Static 전용)** *또는* **목적지 실제 포트**
- **소스 매핑된 포트(Static 전용)** *또는* **목적지 매핑된 포트**

서비스 객체 구성에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

지침

- NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 객체의 프로토콜과 매핑된 서비스 객체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP).
- "not equal"(**neq**) 연산자는 지원되지 않습니다.
- 아이덴티티 포트 변환의 경우 실제 포트와 매핑된 포트에 동일한 서비스 객체를 사용할 수 있습니다.
- Source Dynamic NAT - Source Dynamic NAT는 포트 변환을 지원하지 않습니다.
- Source Dynamic PAT(Hide) - Source Dynamic PAT는 포트 변환을 지원하지 않습니다.
- Source Static NAT 또는 Static NAT with port translation - 서비스 객체는 소스 포트와 목적지 포트를 모두 포함할 수 있습니다. 그러나 두 서비스 객체에 대해 소스 포트 *또는* 목적지 포트 중 *하나*만 지정해야 합니다. 애플리케이션이 고정된 소스 포트(예: 일부 DNS 서버)를 사용하는 경우에만 소스 포트와 목적지 포트를 *모두* 지정해야 합니다. 그러나 고정된 소스 포트는 매우 드뭅니다. 예를 들어, 소스 호스트에 대한 포트를 변환하려면 소스 서비스를 구성해야 합니다.
- Source Static NAT - 서비스 객체는 소스 포트와 목적지 포트를 모두 포함할 수 있습니다. 그러나 두 서비스 객체에 대해 소스 포트 *또는* 목적지 포트 중 *하나*만 지정해야 합니다. 애플리케이션이 고정된 소스 포트(예: 일부 DNS 서버)를 사용하는 경우에만 소스 포트와 목적지 포트를 *모두* 지정해야 합니다. 그러나 고정된 소스 포트는 매우 드뭅니다. 예를 들어, 소스 호스트에 대한 포트를 변환하려면 소스 서비스를 구성해야 합니다.
- Destination Static NAT 또는 Static NAT with port translation(대상 변환은 항상 고정임) - 비 Static Source NAT의 경우 목적지에 대해서만 포트 변환을 수행할 수 있습니다. 서비스 객체는 소스 포트와 목적지 포트를 모두 포함할 수 있지만, 이 경우에는 목적지 포트만 사용됩니다. 소스 포트를 지정하면 무시됩니다.

자세한 단계

	명령	목적

1단계	**object service** *obj_name*
	service {**tcp** | **udp**} [**source** *operator port*] [**destination** *operator port*]
	
	예:
	`hostname(config)# object service REAL_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 80`
	
	`hostname(config)# object service MAPPED_SRC_SVC`
	`hostname(config-service-object)# service tcp source eq 8080`
		서비스 객체를 추가합니다.

동적 NAT

이 섹션에서는 동적 NAT에 대해 Twice NAT를 구성하는 방법에 대해 설명합니다. 자세한 내용은 4-8 페이지의 동적 NAT를 참조하십시오.

자세한 단계

	명령	목적
1단계	다음에 대한 네트워크 객체 또는 그룹을 만듭니다. • 소스 실제 주소 • 소스 매핑된 주소 • 수신 실제 주소 • 수신 매핑된 주소	6-5 페이지의 실제 및 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오. 모든 소스 트래픽을 변환하려면 소스 실제 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **any** 키워드를 지정할 수 있습니다. Destination static interface NAT with port translation만 구성하려면 수신 매핑된 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **interface** 키워드를 지정할 수 있습니다.
2단계	(선택 사항) 다음에 대한 서비스 객체를 만듭니다. • 목적지 실제 포트 • 목적지 매핑된 포트	6-6 페이지의 (선택 사항) 실제 및 매핑된 포트에 대해 서비스 객체 추가 섹션을 참조하십시오.
3단계	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real_obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*] **예:** `hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC`	**dynamic NAT**를 구성합니다. 다음 지침을 참조하십시오. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • 섹션 및 줄 - (선택 사항) 기본적으로 NAT 규칙은 NAT 테이블의 섹션 1 끝에 추가됩니다(4-20 페이지의 NAT 규칙 순서 참조). 대신 섹션 3에 규칙을 추가하려면(네트워크 객체 NAT 규칙 이후) **after-auto** 키워드를 사용합니다. *line* 인수를 사용하여 해당 섹션의 어디에나 규칙을 삽입할 수 있습니다. • 소스 주소: – 실제 주소 - 네트워크 객체, 그룹 또는 **any** 키워드를 지정합니다. – 매핑된 주소 - 다른 네트워크 객체 또는 그룹을 지정합니다. 선택적으로 다음대안을 구성할 수 있습니다. 인터페이스 PAT 대안 - (라우팅된 모드 전용) **interface** 키워드는 인터페이스 PAT 대안을 활성화합니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. 매핑된 IP 주소가 모두 사용되면, 그 다음에는 매핑된 인터페이스의 IP 주소가 사용됩니다. 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다.

명령	목적
	(계속) • 수신 주소(선택 사항): – 매핑된 주소 - 네트워크 객체 또는 그룹을 지정하거나, Static interface NAT with port translation의 경우에만 **interface** 키워드를 지정합니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. **interface**를 지정할 경우 **service** 키워드도 구성해야 합니다. 이 옵션의 경우 *real_ifc*에 대한 특정 인터페이스를 구성해야 합니다.자세한 내용은 4-5 페이지의 Static Interface NAT with Port Translation 섹션을 참조하십시오. – 실제 주소 - 네트워크 객체 또는 그룹을 지정합니다. 아이덴티티 NAT의 경우 실제 주소와 매핑된 주소 모두에 동일한 객체 또는 그룹을 사용합니다. • 목적지 포트 - (선택 사항) 실제 및 매핑된 서비스 객체와 함께 **service** 키워드를 지정합니다. 아이덴티티 포트 변환의 경우 실제 포트와 매핑된 포트에 동일한 서비스 객체를 사용합니다. • DNS - (선택 사항, 소스 전용 규칙) **dns** 키워드는 DNS 응답을 변환합니다. DNS 검사를 사용하도록 설정해야 합니다(기본적으로 사용됨). **destination** 주소를 구성하는 경우 **dns** 키워드를 구성할 수 없습니다. 자세한 내용은 4-32 페이지의 DNS 및 NAT 섹션을 참조하십시오. • 단방향 - (선택 사항) 수신 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 **unidirectional**을 지정합니다. • 비활성 - (선택 사항) 명령을 삭제하지 않은 채 이 규칙을 비활성화하려면 **inactive** 키워드를 사용합니다. 다시 활성화하려면 **inactive** 키워드 없이 명령 전체를 다시 입력합니다. • 설명 - (선택 사항) **description** 키워드를 사용하여 최대 200자로 설명을 제공합니다.

예

다음 예는 209.165.201.1/27 네트워크의 서버 및 203.0.113.0/24 네트워크의 서버에 액세스할 때 내부 네트워크 10.1.1.0/24에 대해 동적 NAT를 구성합니다.

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0
```

```
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

다음 예는 IPv4 209.165.201.1/27 네트워크의 서버 및 203.0.113.0/24 네트워크의 서버에 액세스할 때 IPv6 내부 네트워크 2001:DB8:AAAA::/96에 대해 동적 NAT를 구성합니다.

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

동적 PAT(숨김) 구성

이 섹션에서는 동적 PAT(숨김)용 Twice NAT 구성 방법에 대해 설명합니다. 자세한 내용은 4-10 페이지의 동적 PAT 섹션을 참조하십시오.

지침

PAT 풀의 경우:

- 사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 *없*는 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다. (8.4(3) 이상, 8.5(1) 또는 8.6(1) 제외) 낮은 포트 범위를 사용하는 트래픽이 많은 경우 이제 크기가 서로 다른 세 가지 계층 대신 균일한 포트 범위(1024~65535 또는 1~65535)를 사용하도록 지정할 수 있습니다.
- 별개의 두 규칙에서 동일한 PAT 풀 객체를 사용하는 경우 각 규칙에 대해 동일한 옵션을 지정해야 합니다. 예를 들어, 한 규칙에서 확장 PAT와 균일한 범위를 지정하는 경우 다른 규칙에서도 확장 PAT와 균일한 범위를 지정해야 합니다.

PAT 풀용 확장 PAT의 경우:

- 확장 PAT를 지원하지 않는 애플리케이션 검사가 많습니다. 지원되지 않는 검사 리스트는 7 장, “애플리케이션 계층 프로토콜 검사 시작”의 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오.
- 동적 PAT 규칙에 대해 확장 PAT를 활성화하면, PAT 풀의 주소를 별도의 static NAT-with-port-translation 규칙에서 PAT 주소로서 사용할 수 없습니다. 예를 들어 PAT 풀이 10.1.1.1을 포함하면, 10.1.1.1을 PAT 주소로 사용하는 static NAT-with-port-translation 규칙을 만들 수 없습니다.

- PAT 풀을 사용하고 대안용 인터페이스를 지정하는 경우 확장 PAT를 지정할 수 없습니다.
- ICE 또는 TURN을 사용하는 VoIP 배포에는 확장 PAT를 사용할 수 없습니다. ICE 및 TURN은 모든 목적지에 대해 PAT 바인딩이 동일할 것으로 신뢰합니다.

PAT 풀용 라운드 로빈의 경우:

- 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. **참고**: 장애 조치 이후에는 "동질성"이 해제됩니다. ASA에서 장애 조치를 수행하면 호스트의 후속 연결에는 초기 IP 주소가 사용되지 않을 수 있습니다.
- 라운드 로빈은 특히 확장 PAT와 함께 사용할 경우 대량의 메모리를 소모할 수 있습니다. NAT 풀은 모든 매핑된 프로토콜/IP 주소/포트 범위에 대해 생성되므로, 라운드 로빈에서 대량의 동시 NAT 풀이 생성되며 여기에서 메모리를 사용합니다. 확장 PAT를 사용하면 동시 NAT 풀의 수가 더 많아집니다.

자세한 단계

	명령	목적
1단계	다음에 대한 네트워크 객체 또는 그룹을 만듭니다. • 소스 실제 주소 • 소스 매핑된 주소 • 수신 실제 주소 • 수신 매핑된 주소	6-5 페이지의 실제 및 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오. 모든 소스 트래픽을 변환하려면 소스 실제 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **any** 키워드를 지정할 수 있습니다. 인터페이스 주소를 매핑된 주소로서 사용하려면 소스 매핑된 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **interface** 키워드를 지정할 수 있습니다. Destination static interface NAT with port translation만 구성하려면 수신 매핑된 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **interface** 키워드를 지정할 수 있습니다.
2단계	(선택 사항) 다음에 대한 서비스 객체를 만듭니다. • 목적지 실제 포트 • 목적지 매핑된 포트	6-6 페이지의 (선택 사항) 실제 및 매핑된 포트에 대해 서비스 객체 추가 섹션을 참조하십시오.

	명령	목적
3단계	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-auto** [*line*]}] **source dynamic** {*real-obj* | **any**} {*mapped_obj* [**interface** [**ipv6**]] | [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**interface** [**ipv6**]] | **interface** [**ipv6**]} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *mapped_dest_svc_obj real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*] **예:** `hostname(config)# nat (inside,outside) source dynamic MyInsNet interface destination static Server1 Server1 description Interface PAT for inside addresses when going to server 1`	**dynamic PAT (hide)**를 구성합니다. 다음 지침을 참조하십시오. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • 섹션 및 줄 - (선택 사항) 기본적으로 NAT 규칙은 NAT 테이블의 섹션 1 끝에 추가됩니다(4-20 페이지의 NAT 규칙 순서 참조). 대신 섹션 3에 규칙을 추가하려면(네트워크 객체 NAT 규칙 이후) **after-auto** 키워드를 사용합니다. *line* 인수를 사용하여 해당 섹션의 어디에나 규칙을 삽입할 수 있습니다. • 소스 주소: – 실제 주소 - 네트워크 객체, 그룹 또는 **any** 키워드를 지정합니다. 실제 인터페이스에서 매핑된 인터페이스로 모든 트래픽을 전환하려면 **any** 키워드를 사용합니다. – 매핑된 주소 - 다음 중 하나를 구성합니다. - 네트워크 객체 - 호스트 주소를 포함하는 네트워크 객체를 지정합니다. - **pat-pool** - 여러 주소를 포함하는 네트워크 객체 또는 그룹 및 **pat-pool** 키워드를 지정합니다. - **interface** - (라우팅된 모드 전용) 인터페이스 PAT만 사용하려면 **interface** 키워드만 지정합니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. PAT 풀 또는 네트워크 객체와 함께 지정하면 **interface** 키워드는 인터페이스 PAT 대안을 활성화합니다. PAT IP 주소가 모두 사용되면, 그 다음에는 매핑된 인터페이스의 IP 주소가 사용됩니다. 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다. (계속)

명령	목적
	(계속) PAT 풀에 대해 다음 옵션 중 하나 이상을 지정할 수 있습니다. -- Round robin - **round-robin** 키워드는 PAT 풀에 대한 라운드 로빈 주소 할당을 활성화합니다. 기본적으로, 라운드 로빈이 아니면 PAT 주소에 대한 모든 포트는 다음 PAT 주소가 사용되기 전에 할당됩니다. 라운드 로빈 방식은 첫 번째 주소를 다시 사용하게 되기 전(그 다음에는 두 번째 주소, 세 번째 주소 등) 풀의 각 PAT 주소에서 하나의 주소/포트를 할당합니다. -- Extended PAT - **extended** 키워드는 확장 PAT를 활성화합니다. 확장 PAT는 변환 정보의 수신 주소 및 포트를 포함하여 *서비스*당(IP 주소당이 아니라) 65535개 포트를 사용합니다. 일반적으로 PAT 변환을 만들 때 목적지 포트 및 주소는 고려되지 않으므로 PAT 주소당 65535개 포트로 제한됩니다. 예를 들어 확장 PAT를 사용하면, 192.168.1.7:23으로 이동할 경우 10.1.1.1:1027의 변환을 만들고 192.168.1.7:80로 이동할 경우에도 10.1.1.1:1027 변환을 만들 수 있습니다. -- Flat range - **flat** 키워드는 포트 할당 시 1024~65535의 전체 포트 범위 사용을 활성화합니다. 변환용의 매핑된 포트 번호를 선택하면 ASA에서는 사용 가능한 경우 실제 소스 포트 번호를 사용합니다. 그러나 이 옵션이 아니면, 실제 포트를 사용할 수 *없*는 경우 기본적으로 실제 포트 번호와 동일한 포트 범위(1~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 낮은 범위에서 포트가 부족하지 않게 하려면 이 설정을 구성하십시오. 1~65535의 전체 범위를 사용하려면 **include-reserve** 키워드도 지정합니다. (계속)

명령	목적
	(계속) • 수신 주소(선택 사항): – 매핑된 주소 - 네트워크 객체 또는 그룹을 지정하거나, Static interface NAT with port translation의 경우에만 (라우팅된 모드) **interface** 키워드를 지정합니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. **interface**를 지정할 경우 **service** 키워드도 구성해야 합니다. 이 옵션의 경우 *real_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 자세한 내용은 4-5 페이지의 Static Interface NAT with Port Translation 섹션을 참조하십시오. – 실제 주소 - 네트워크 객체 또는 그룹을 지정합니다. 아이덴티티 NAT의 경우 실제 주소와 매핑된 주소 모두에 동일한 객체 또는 그룹을 사용합니다. • 목적지 포트 - (선택 사항) 실제 및 매핑된 서비스 객체와 함께 **service** 키워드를 지정합니다. 아이덴티티 포트 변환의 경우 실제 포트와 매핑된 포트에 동일한 서비스 객체를 사용합니다. • DNS - (선택 사항, 소스 전용 규칙) **dns** 키워드는 DNS 응답을 변환합니다. DNS 검사를 사용하도록 설정해야 합니다(기본적으로 사용됨). **destination** 주소를 구성하는 경우 **dns** 키워드를 구성할 수 없습니다. 자세한 내용은 4-32 페이지의 DNS 및 NAT 섹션을 참조하십시오. • 단방향 - (선택 사항) 수신 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 **unidirectional**을 지정합니다. • 비활성 - (선택 사항) 명령을 삭제하지 않은 채 이 규칙을 비활성화하려면 **inactive** 키워드를 사용합니다. 다시 활성화하려면 **inactive** 키워드 없이 명령 전체를 다시 입력합니다. • 설명 - (선택 사항) **description** 키워드를 사용하여 최대 200자로 설명을 제공합니다.

예

다음 예는 외부 텔넷 서버 209.165.201.23에 액세스할 때 내부 네트워크 192.168.1.0/24에 대해 인터페이스 PAT를 구성하고 203.0.113.0/24 네트워크에 있는 서버에 액세스할 때 PAT 풀을 이용한 동적 PAT를 구성합니다.

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23
```

```
hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

다음 예는 외부 IPv6 텔넷 서버 2001:DB8::23에 액세스할 때 내부 네트워크 192.168.1.0/24에 대해 인터페이스 PAT를 구성하고 2001:DB8:AAAA::/96 네트워크에 있는 서버에 액세스할 때 PAT 풀을 이용한 동적 PAT를 구성합니다.

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

Static NAT 또는 Static NAT-with-Port-Translation 구성

이 섹션에서는 Twice NAT를 사용하여 Static NAT를 구성하는 방법에 대해 설명합니다. Static NAT에 대한 자세한 내용은 4-3 페이지의 고정 NAT를 참조하십시오.

자세한 단계

	명령	목적
1단계	다음에 대한 네트워크 객체 또는 그룹을 만듭니다. • 소스 실제 주소 • 소스 매핑된 주소 • 수신 실제 주소 • 수신 매핑된 주소	6-5 페이지의 실제 및 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오. Source static interface NAT with port translation만 구성하려면 소스 매핑된 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **interface** 키워드를 지정할 수 있습니다. Destination static interface NAT with port translation만 구성하려면 수신 매핑된 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **interface** 키워드를 지정할 수 있습니다.
2단계	(선택 사항) 다음에 대한 서비스 객체를 만듭니다. • Source *또는* Destination 실제 포트 • Source *또는* Destination 매핑된 포트	6-6 페이지의 (선택 사항) 실제 및 매핑된 포트에 대해 서비스 객체 추가 섹션을 참조하십시오.

	명령	목적
3단계	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** *real_ob* [*mapped_obj* | **interface** [**ipv6**]] [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | **no-proxy-arp**] [**inactive**] [**description** *desc*] **예:** `hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC`	**static NAT**를 구성합니다. 다음 지침을 참조하십시오. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • 섹션 및 줄 - (선택 사항) 기본적으로 NAT 규칙은 NAT 테이블의 섹션 1 끝에 추가됩니다. 섹션에 대한 자세한 내용은 4-20 페이지의 NAT 규칙 순서를 참조하십시오. 대신 섹션 3에 규칙을 추가하려면(네트워크 객체 NAT 규칙 이후) **after-auto** 키워드를 사용합니다. *line* 인수를 사용하여 해당 섹션의 어디에나 규칙을 삽입할 수 있습니다. • 소스 주소: – 실제 주소 - 네트워크 객체 또는 그룹을 지정합니다. – 매핑된 주소 - 다른 네트워크 객체 또는 그룹을 지정합니다. Static interface NAT with port translation의 경우에만 **interface** 키워드를 지정할 수 있습니다(라우팅된 모드 전용). **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. **interface**를 지정하는 경우 **service** 키워드도 구성해야 합니다(이 경우 서비스 객체에는 소스 포트만 포함해야 합니다). 이 옵션의 경우 *mapped_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 자세한 내용은 4-5 페이지의 Static Interface NAT with Port Translation 섹션을 참조하십시오. • 수신 주소(선택 사항): – 매핑된 주소 - 네트워크 객체 또는 그룹을 지정하거나, Static interface NAT with port translation의 경우에만 **interface** 키워드를 지정합니다. **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. **interface**를 지정하는 경우 **service** 키워드도 구성해야 합니다(이 경우 서비스 객체에는 목적지 포트만 포함해야 합니다). 이 옵션의 경우 *real_ifc*에 대한 특정 인터페이스를 구성해야 합니다. – 실제 주소 - 네트워크 객체 또는 그룹을 지정합니다. 아이덴티티 NAT의 경우 실제 주소와 매핑된 주소 모두에 동일한 객체 또는 그룹을 사용합니다.

명령	목적
	(계속) • 포트 - (선택 사항) 실제 및 매핑된 서비스 객체와 함께 **service** 키워드를 지정합니다. 소스 포트 변환의 경우 객체는 소스 서비스를 지정해야 합니다. 소스 포트 변환을 위한 명령에서 서비스 객체의 순서는 **service** *real_obj mapped_obj*입니다. 목적지 포트 변환의 경우 객체는 목적지 서비스를 지정해야 합니다. 목적지 포트 변환을 위한 서비스 객체의 순서는 **service** *mapped_obj real_obj*입니다. 드문 경우이지만 객체에서 소스 포트와 목적지 포트를 모두 지정하는 경우, 첫 번째 서비스 객체는 실제 소스 포트/매핑된 목적지 포트를 포함하고, 두 번째 서비스 객체는 매핑된 소스 포트/실제 목적지 포트를 포함합니다. 아이덴티티 포트 변환의 경우 실제 포트와 매핑된 포트에 동일한 서비스 객체를 사용합니다(컨피그레이션에 따라 소스 및/또는 목적지 포트). • Net-to-net - (선택 사항) NAT 46의 경우 첫 번째 IPv4 주소를 첫 번째 IPv6 주소로, 두 번째를 두 번째로 등과 같이 변환하려면 **net-to-net**을 지정합니다. 이 옵션이 없으면 IPv4-embedded 메서드가 사용됩니다. 일대일 변환에는 이 키워드를 반드시 사용해야 합니다. • DNS - (선택 사항, 소스 전용 규칙) **dns** 키워드는 DNS 응답을 변환합니다. DNS 검사를 사용하도록 설정해야 합니다(기본적으로 사용됨). **destination** 주소를 구성하는 경우 **dns** 키워드를 구성할 수 없습니다. 자세한 내용은 4-32 페이지의 DNS 및 NAT 섹션을 참조하십시오. • 단방향 - (선택 사항) 수신 주소가 소스 주소에 대한 트래픽을 시작하지 못하게 하려면 **unidirectional**을 지정합니다. • No Proxy ARP - (선택 사항) 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화하려면 **no-proxy-arp**를 지정합니다. 자세한 내용은 4-22 페이지의 매핑된 주소 및 라우팅 섹션을 참조하십시오. • 비활성 - (선택 사항) 명령을 삭제하지 않은 채 이 규칙을 비활성화하려면 **inactive** 키워드를 사용합니다. 다시 활성화하려면 **inactive** 키워드 없이 명령 전체를 다시 입력합니다. • 설명 - (선택 사항) **description** 키워드를 사용하여 최대 200자로 설명을 제공합니다.

예

다음 예는 Static interface NAT with port translation의 사용법을 보여줍니다. 외부의 호스트가 목적지 포트 65000~65004로 외부 인터페이스 IP 주소에 연결하여 내부의 FTP 서버에 액세스합니다. 192.168.10.100:6500~:65004에서는 트래픽이 내부 FTP 서버로 변환되지 않습니다. 소스 주소와 포트를 명령에 지정된 대로 변환하고자 하기 때문에 서비스 객체에서 소스 포트 범위를 지정하는 것입니다(목적지 포트는 지정하지 않음). 목적지 포트는 "any"입니다. 고정 NAT는 양방향이므로 "source" 및 "destination"은 기본적으로 명령 키워드를 가리킵니다. 패킷의 실제 소스 및 수신 주소와 포트는 어떤 호스트가 패킷을 보냈는가에 따라 달라집니다. 이 예에서는 연결이 외부에서 시작되어 내부로 들어오므로 FTP 서버의 "source" 주소 및 포트는 실제로 원래 패킷의 수신 주소 및 포트입니다.

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

다음 예는 IPv6 네트워크에 액세스할 때 한 IPv6 네트워크에서 다른 IPv6으로의 고정 변환, 그리고 IPv4 네트워크에 액세스할 때 IPv4 PAT 풀로의 동적 PAT 변환을 보여줍니다.

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254

hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW destination
static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

아이덴티티 NAT 구성

이 섹션에서는 Twice NAT를 사용하여 아이덴티티 NAT 규칙을 구성하는 방법에 대해 설명합니다. 아이덴티티 NAT 순서에 대한 자세한 내용은 4-12 페이지의 아이덴티티 NAT를 참조하십시오.

자세한 단계

	명령	목적
1단계	다음에 대한 네트워크 객체 또는 그룹을 만듭니다. • 소스 실제 주소(일반적으로 소스 매핑된 주소에 대해 동일한 객체를 사용함) • 수신 실제 주소 • 수신 매핑된 주소	6-5 페이지의 실제 및 매핑된 주소에 대해 네트워크 객체 추가 섹션을 참조하십시오. 모든 주소에 대해 아이덴티티 NAT를 수행하려면 소스 실제 주소에 대한 객체 생성을 건너뛰고 대신 **nat** 명령에서 **any any** 키워드를 지정할 수 있습니다. Destination static interface NAT with port translation만 구성하려면 수신 매핑된 주소에 대한 객체 추가를 건너뛰고 대신 **nat** 명령에서 **interface** 키워드를 지정할 수 있습니다.
2단계	(선택 사항) 다음에 대한 서비스 객체를 만듭니다. • Source 또는 Destination 실제 포트 • Source 또는 Destination 매핑된 포트	6-6 페이지의 (선택 사항) 실제 및 매핑된 포트에 대해 서비스 객체 추가 섹션을 참조하십시오.

	명령	목적
3단계	**nat** [(*real_ifc*,*mapped_ifc*)] [*line* | {**after-object** [*line*]}] **source static** {*nw_obj nw_obj* | **any any**} [**destination static** {*mapped_obj* | **interface** [**ipv6**]} *real_obj*] [**service** *real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj*] [**no-proxy-arp**] [**route-lookup**] [**inactive**] [**description** *desc*] **예:** `hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet destination static Server1 Server1`	**identity NAT**를 구성합니다. 다음 지침을 참조하십시오. • 인터페이스 - (투명 모드에 필요) 실제(real) 및 매핑된(mapped) 인터페이스를 지정합니다. 명령에 괄호를 포함하십시오. 라우팅된 모드에서 실제 인터페이스와 매핑된 인터페이스를 지정하지 않으면 모든 인터페이스가 사용됩니다. 인터페이스 하나 또는 둘 다에 대해 **any** 키워드를 지정할 수도 있습니다. • 섹션 및 줄 - (선택 사항) 기본적으로 NAT 규칙은 NAT 테이블의 섹션 1 끝에 추가됩니다. 섹션에 대한 자세한 내용은 4-20 페이지의 NAT 규칙 순서를 참조하십시오. 대신 섹션 3에 규칙을 추가하려면(네트워크 객체 NAT 규칙 이후) **after-auto** 키워드를 사용합니다. *line* 인수를 사용하여 해당 섹션의 어디에나 규칙을 삽입할 수 있습니다. • 소스 주소 - 실제 및 매핑된 주소 모두에 대해 네트워크 객체, 그룹 또는 **any** 키워드를 지정합니다. • 수신 주소(선택 사항): – 매핑된 주소 - 네트워크 객체 또는 그룹을 지정합니다. 또는 Static interface NAT with port translation의 경우에만 **interface** 키워드를 지정합니다(라우팅된 모드 전용). **ipv6**을 지정하면 인터페이스의 IPv6 주소가 사용됩니다. **interface**를 지정하는 경우 **service** 키워드도 구성해야 합니다(이 경우 서비스 객체에는 목적지 포트만 포함해야 합니다). 이 옵션의 경우 *real_ifc*에 대한 특정 인터페이스를 구성해야 합니다. 자세한 내용은 4-5 페이지의 Static Interface NAT with Port Translation 섹션을 참조하십시오. – 실제 주소 - 네트워크 객체 또는 그룹을 지정합니다. 아이덴티티 NAT의 경우 실제 주소와 매핑된 주소 모두에 동일한 객체 또는 그룹을 사용합니다. • 포트 - (선택 사항) 실제 및 매핑된 서비스 객체와 함께 **service** 키워드를 지정합니다. 소스 포트 변환의 경우 객체는 소스 서비스를 지정해야 합니다. 소스 포트 변환을 위한 명령에서 서비스 객체의 순서는 **service** *real_obj mapped_obj*입니다. 목적지 포트 변환의 경우 객체는 목적지 서비스를 지정해야 합니다. 목적지 포트 변환을 위한 서비스 객체의 순서는 **service** *mapped_obj real_obj*입니다. 드문 경우이지만 객체에서 소스 포트와 목적지 포트를 모두 지정하는 경우, 첫 번째 서비스 객체는 실제 소스 포트/매핑된 목적지 포트를 포함하고, 두 번째 서비스 객체는 매핑된 소스 포트/실제 목적지 포트를 포함합니다. 아이덴티티 포트 변환의 경우 실제 포트와 매핑된 포트에 동일한 서비스 객체를 사용합니다(컨피그레이션에 따라 소스 및/또는 목적지 포트).

명령	목적
	(계속) • No Proxy ARP - (선택 사항) 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화하려면 **no-proxy-arp**를 지정합니다. 자세한 내용은 4-22 페이지의 매핑된 주소 및 라우팅 섹션을 참조하십시오. • Route lookup - (선택 사항, 라우팅된 모드 전용, 인터페이스 지정) NAT 명령으로 지정한 인터페이스를 사용하는 대신 경로 조회를 사용하여 이그레스(egress) 인터페이스를 결정하려면 **route-lookup**을 지정합니다. 자세한 내용은 4-24 페이지의 이그레스(egress) 인터페이스 결정 섹션을 참조하십시오. • 비활성 - (선택 사항) 명령을 삭제하지 않은 채 이 규칙을 비활성화하려면 **inactive** 키워드를 사용합니다. 다시 활성화하려면 **inactive** 키워드 없이 명령 전체를 다시 입력합니다. • 설명 - (선택 사항) **description** 키워드를 사용하여 최대 200자로 설명을 제공합니다.

Per-Session PAT 규칙 구성

기본적으로 모든 TCP PAT 트래픽 및 모든 UDP DNS 트래픽은 Per-Session PAT를 사용합니다. 트래픽에 Multi-Session PAT를 사용하려면 Per-Session PAT 규칙을 구성할 수 있습니다. 허용 규칙은 Per-Session PAT를 사용하고 거부 규칙은 Multi-Session PAT를 사용합니다. Per-Session PAT 대 다중 세션 PAT에 대한 자세한 내용은 4-11 페이지의 Per-Session PAT 대 Multi-Session PAT을 참조하십시오.

자세한 단계

Per-Session PAT 규칙을 구성하려면 5-15 페이지의 Per-Session PAT 규칙 구성을 참조하십시오.

Twice NAT 모니터링

Twice NAT를 모니터링하려면 다음 명령 중 하나를 입력합니다.

명령	목적
`show nat`	각 NAT 규칙의 건수를 포함한 NAT 통계를 표시합니다.
`show nat pool`	할당된 주소와 포트, 할당된 횟수 등을 포함한 NAT 풀 통계를 표시합니다.
`show xlate`	현재의 NAT 세션 정보를 표시합니다.
`show nat divert-table`	모든 NAT 규칙이 NAT divert 테이블에서 하나의 항목을 형성합니다. 일치하는 규칙에 대해 NAT divert 필드가 ignore=yes NAT로 설정되어 있으면 ASA는 조회를 중지하고 수신 IP를 기반으로 경로 조회를 수행하여 이그레스(egress) 인터페이스를 결정합니다. 일치하는 규칙에 대해 NAT divert 필드가 ignore=no로 설정되어 있으면, 발견된 input_ifc 및 output_ifc를 기반으로 NAT 테이블을 살펴보고 필요한 변환을 수행하십시오. 이그레스 인터페이스는 output_ifc가 됩니다.

Twice NAT의 컨피그레이션 예

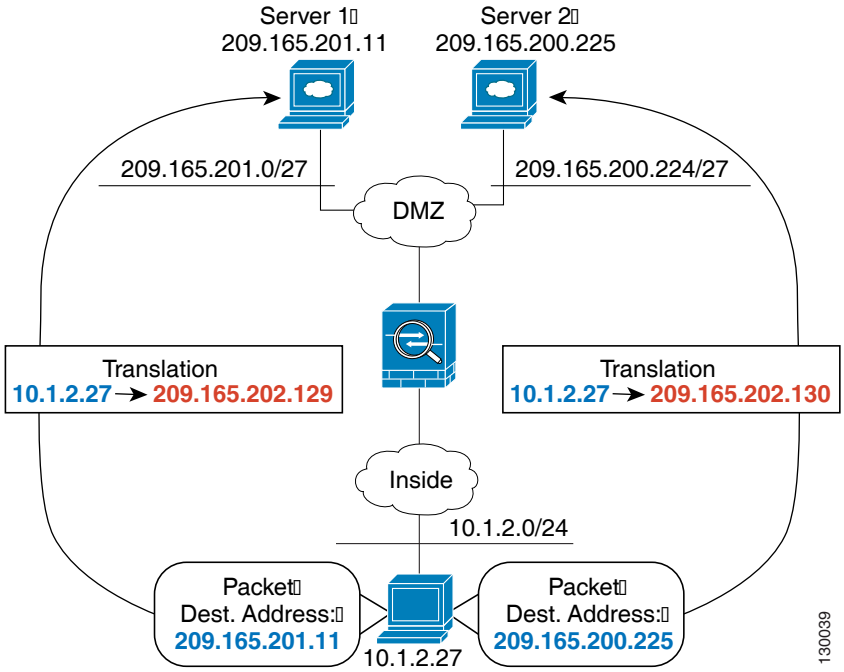
이 섹션에서는 다음 컨피그레이션 예를 다룹니다.

- 6-21 페이지의 대상에 따라 다른 변환(동적 PAT)
- 6-22 페이지의 수신 주소 및 포트에 따라 다른 변환(동적 PAT)

대상에 따라 다른 변환(동적 PAT)

그림 6-1은 두 개의 서로 다른 서버에 액세스하는 10.1.2.0/24 네트워크의 호스트를 보여줍니다. 호스트가 209.165.201.11의 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 209.165.200.225의 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

그림 6-1 서로 다른 수신 주소의 Twice NAT



1단계 내부 네트워크용 네트워크 객체를 추가합니다.

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

2단계 DMZ 네트워크 1용 네트워크 객체를 만듭니다.

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

3단계 PAT 주소용 네트워크 객체를 추가합니다.

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

4단계 첫 번째 Twice NAT 규칙을 구성합니다.

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
static DMZnetwork1 DMZnetwork1
```

수신 주소를 변환하지 않을 것이기 때문에 실제 및 매핑된 수신 주소에 대해 동일한 주소를 지정하여 수신 주소에 대한 아이덴티티 NAT를 구성해야 합니다.

기본적으로 NAT 규칙이 NAT 테이블의 섹션 1 끝에 추가됩니다. NAT 규칙의 섹션 및 줄 번호 지정에 대한 자세한 내용은 6-10 페이지의 동적 PAT(숨김) 구성을 참조하십시오.

5단계 DMZ 네트워크 2용 네트워크 객체를 만듭니다.

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

6단계 PAT 주소용 네트워크 객체를 추가합니다.

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

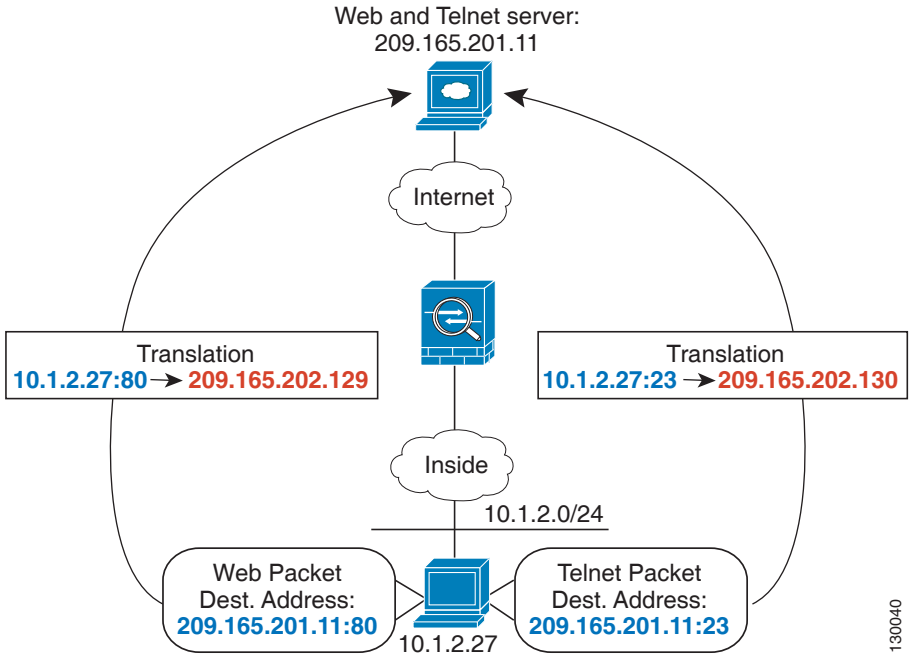
7단계 Twice NAT 규칙을 구성합니다.

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
static DMZnetwork2 DMZnetwork2
```

수신 주소 및 포트에 따라 다른 변환(동적 PAT)

그림 6-2는 소스 및 목적지 포트의 사용을 보여줍니다. 10.1.2.0/24 네트워크의 호스트가 웹 서비스와 텔넷 서비스를 모두 제공하는 단일 호스트에 액세스합니다. 호스트가 텔넷 서비스용 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 동일한 웹 서비스용 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

그림 6-2 서로 다른 목적지 포트의 Twice NAT



1단계 내부 네트워크용 네트워크 객체를 추가합니다.

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

2단계 Telnet/Web 서버용 네트워크 객체를 만듭니다.

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

3단계 텔넷 사용 시 PAT 주소용 네트워크 객체를 추가합니다.

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

4단계 텔넷용 서비스 객체를 추가합니다.

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

5단계 첫 번째 Twice NAT 규칙을 구성합니다.

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

수신 주소 또는 포트를 변환하지 않을 것이기 때문에 실제 및 매핑된 수신 주소에 대해 동일한 주소를 지정하고 실제 및 매핑된 서비스에 대해 동일한 포트를 지정하여, 수신 주소 또는 포트에 대한 아이덴티티 NAT를 구성해야 합니다.

기본적으로 NAT 규칙이 NAT 테이블의 섹션 1 끝에 추가됩니다. NAT 규칙의 섹션 및 줄 번호 지정에 대한 자세한 내용은 6-10 페이지의 동적 PAT(숨김) 구성을 참조하십시오.

6단계 HTTP 사용 시 PAT 주소용 네트워크 객체를 추가합니다.

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

7단계 HTTP용 서비스 객체를 추가합니다.

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

8단계 Twice NAT 규칙을 구성합니다.

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

Twice NAT의 기능 기록

표 6-1에는 각 기능 변경 사항 및 그것이 구현된 플랫폼 릴리스가 나열되어 있습니다.

표 6-1 Twice NAT의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
Twice NAT	8.3(1)	Twice NAT에서는 소스 주소와 수신 주소를 단일 규칙에서 식별할 수 있습니다. 수정 또는 추가된 명령: **nat**, **show nat**, **show xlate**, **show nat pool**.
아이덴티티 NAT 구성 가능 프록시 ARP 및 경로 조회	8.4(2)/8.5(1)	아이덴티티 NAT의 이전 릴리스에서는 프록시 ARP가 비활성화되었고, 이그레스(egress) 인터페이스를 확인하는 데 항상 경로 조회가 사용되었습니다. 이러한 설정을 구성할 수 없었습니다. 8.4(2) 이상에서는 아이덴티티 NAT에 대한 기본 동작이 다른 고정 NAT 컨피그레이션의 동작과 일치하도록 변경되었습니다. 프록시 ARP가 활성화되며, 기본적으로 NAT 컨피그레이션이 이그레스(egress) 인터페이스(지정한 경우)를 확인합니다. 이러한 설정을 그대로 둘 수도 있고, 별도로 활성화 또는 비활성화할 수도 있습니다. 이제 정기적인 고정 NAT를 위해 프록시 ARP를 비활성화할 수도 있습니다. 8.3 이전 컨피그레이션의 경우 NAT 예외 규칙(**nat 0 access-list** 명령)을 8.4(2) 이상으로 마이그레이션하려면 **no-proxy-arp** 및 **route-lookup** 키워드를 포함하여 프록시 ARP를 비활성화하고 경로 조회를 사용해야 합니다. 8.3(2) 및 8.4(1)로 마이그레이션하는 데 사용된 **unidirectional** 키워드는 더 이상 마이그레이션에 사용되지 않습니다. 8.3(1), 8.3(2) 및 8.4(1)에서 8.4(2)로 업그레이드하면, 이제 기존 기능을 유지할 수 있도록 모든 아이덴티티 NAT 컨피그레이션에 **no-proxy-arp** 및 **route-lookup** 키워드가 포함됩니다. **unidirectional** 키워드는 제거됩니다. 수정된 명령: **nat source static** [**no-proxy-arp**] [**route-lookup**].
PAT 풀 및 라운드 로빈 주소 할당	8.4(2)/8.5(1)	이제 단일 주소 대신 PAT 주소의 풀을 지정할 수 있습니다. 풀의 다음 주소를 사용하기 전에 먼저 PAT 주소의 모든 포트를 사용하는 대신, 선택적으로 PAT 주소를 라운드 로빈 방식으로 할당할 수도 있습니다. 이 기능을 이용하면 단일 PAT 주소에서 많은 연결이 설정되는 것(DoS 공격의 일부처럼 보임)을 효과적으로 방지하고, 다수의 PAT 주소를 손쉽게 구성할 수 있습니다. 수정된 명령: **nat source dynamic** [**pat-pool** *mapped_object* [**round-robin**]].

표 6-1 Twice NAT의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
라운드 로빈 PAT 풀 할당은 기존 호스트에 동일한 IP 주소를 사용합니다.	8.4(3)	라운드 로빈 할당으로 PAT 풀을 사용할 때 호스트에 기존 연결이 있으면, 포트가 사용 가능한 경우 해당 호스트의 후속 연결에는 동일한 PAT IP 주소가 사용됩니다. 수정된 명령이 없습니다. *이 기능은 8.5(1) 또는 8.6(1)에서 사용할 수 없습니다.*
PAT 풀용 PAT 포트의 균일한 범위	8.4(3)	사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 *없는* 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511, 512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다. PAT 풀을 사용할 때 낮은 포트 범위를 사용하는 트래픽이 많은 경우 이제 크기가 서로 다른 세 가지 계층 대신 균일한 포트 범위(1024~65535 또는 1~65535)를 사용하도록 지정할 수 있습니다. 수정된 명령: **nat source dynamic** [**pat-pool** *mapped_object* [**flat** [**include-reserve**]]]. *이 기능은 8.5(1) 또는 8.6(1)에서 사용할 수 없습니다.*
PAT 풀용 확장 PAT	8.4(3)	각 PAT IP 주소는 최대 65535개 포트를 허용합니다. 65535개 포트가 충분한 변환을 제공하지 않으면 이제 PAT 풀용 확장 PAT를 활성화할 수 있습니다. 확장 PAT는 변환 정보의 수신 주소 및 포트를 포함하여 *서비스*당 (IP 주소당이 아니라) 65535개 포트를 사용합니다. 수정된 명령: **nat source dynamic** [**pat-pool** *mapped_object* [**extended**]]. *이 기능은 8.5(1) 또는 8.6(1)에서 사용할 수 없습니다.*

표 6-1 Twice NAT의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
VPN 피어의 로컬 IP 주소를 피어의 실제 IP 주소로 변환하는 자동 NAT 규칙	8.4(3)	드문 경우이지만 할당된 로컬 IP 주소 대신 내부 네트워크에 있는 VPN 피어의 실제 IP 주소를 사용하고자 할 수 있습니다. 일반적으로 VPN에서는 내부 네트워크에 액세스할 수 있도록, 할당된 로컬 IP 주소를 피어에 제공합니다. 그러나 예를 들어 내부 서버 및 네트워크 보안이 피어의 실제 IP 주소를 기반으로 하는 경우, 로컬 IP 주소를 피어의 실제 공개 IP 주소로 다시 변환할 수 있습니다. 터널 그룹당 한 인터페이스에서 이 기능을 활성화할 수 있습니다. VPN 세션이 설정되거나 연결이 해제되면 객체 NAT 규칙이 동적으로 추가 및 삭제됩니다. **show nat** 명령을 사용하여 규칙을 볼 수 있습니다. **참고** 라우팅 문제 때문에, 반드시 필요한 경우가 아니면 이 기능을 사용하지 않는 것이 좋습니다. 네트워크와의 기능 호환성을 확인하려면 Cisco TAC에 문의하십시오. 다음 제한을 참조하십시오. • Cisco IPsec 및 AnyConnect 클라이언트만 지원합니다. • NAT 정책과 VPN 정책이 적용될 수 있도록, 공개 IP 주소로 반환되는 트래픽을 ASA로 다시 라우팅해야 합니다. • 부하 균형을 지원하지 않습니다(라우팅 문제 때문). • 로밍을 지원하지 않습니다(공개 IP 변경). 추가된 명령: **nat-assigned-to-public-ip** *interface*(tunnel-group general-attributes 구성 모드).
NAT에서 IPv6 지원	9.0(1)	NAT는 이제 IPv6 트래픽은 물론 IPv4 및 IPv6 간 변환도 지원합니다. 투명 모드에서는 IPv4 및 IPv6 네트워크 간 변환이 지원되지 않습니다. 수정된 명령: **nat**(글로벌 컨피그레이션 모드), **show nat**, **show nat pool**, **show xlate**.
NAT에서 역 DNS 조회 지원	9.0(1)	NAT 규칙용 DNS 검사를 활성화하여 IPv4 NAT, IPv6 NAT 및 NAT64를 사용할 경우 NAT는 이제 역 DNS 조회를 위한 DNS PTR 레코드의 변환을 지원합니다.

표 6-1 Twice NAT의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
Per-Session PAT	9.0(1)	Per-Session PAT 기능은 PAT의 확장성을 개선하며, 클러스터링의 경우 각 멤버 유닛이 PAT 연결을 소유하도록 허용합니다. Multi-Session PAT 연결은 마스터 유닛에서 전달 및 소유해야 합니다. Per-Session PAT 세션이 끝날 무렵 ASA는 재설정을 전송하고 xlate를 즉시 제거합니다. 재설정을 통해 종료 노드에서 연결을 즉시 해제하므로 TIME_WAIT 상태를 피할 수 있습니다. 반면 다중 세션 PAT는 PAT 시간 제한을 사용합니다(기본값 30초). "hit-and-run" 트래픽(예: HTTP 또는 HTTPS)의 경우 Per-Session 기능은 한 주소에 의해 지원되는 연결 속도를 극적으로 높일 수 있습니다. Per-Session 기능을 사용하지 않으면 IP 프로토콜에 대한 한 주소의 최대 연결 속도는 약 초당 2000입니다. Per-Session 기능을 사용하면 IP 프로토콜에 대한 한 주소의 연결 속도는 65535/*average-lifetime*입니다. 기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽은 Per-Session PAT xlate를 사용합니다. Multi-Session PAT가 필요한 트래픽(예: H.323, SIP 또는 Skinny)의 경우 Per-Session 거부 규칙을 만들어 Per-Session PAT를 비활성화할 수 있습니다. 추가된 명령: **xlate per-session**, **show nat pool**.
NAT 규칙 엔진에 대한 트랜잭션 커밋 모델	9.3(1)	활성화할 경우 규칙 편집이 완료된 후 NAT 규칙 업데이트가 적용되며, 규칙 일치 성능에 영향을 미치지 않습니다. 다음 명령에 **nat** 키워드가 추가됨: **asp rule-engine transactional-commit**, **show running-config asp rule-engine transactional-commit**, **clear configure asp rule-engine transactional-commit**.

파 트 3

애플리케이션 검사

애플리케이션 계층 프로토콜 검사 시작

다음 항목에서는 애플리케이션 계층 프로토콜 검사를 구성하는 방법에 대해 설명합니다.

애플리케이션 계층 프로토콜 검사

사용자 데이터 패킷에 IP 주소 지정 정보를 포함하는 서비스 또는 동적으로 할당된 포트에서 보조 채널을 여는 서비스에는 검사 엔진이 필요합니다. 이러한 프로토콜에서 ASA는 빠른 경로로 패킷을 전달하는 대신 DPI(Deep Packet Inspection)를 수행해야 합니다(빠른 경로에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드 참조). 그 결과 검사 엔진은 전반적인 처리량에 영향을 미칠 수 있습니다. 기본적으로 ASA에서는 몇 가지 일반적인 검사 엔진이 사용되지만, 네트워크에 따라 다른 엔진을 사용해야 할 수도 있습니다.

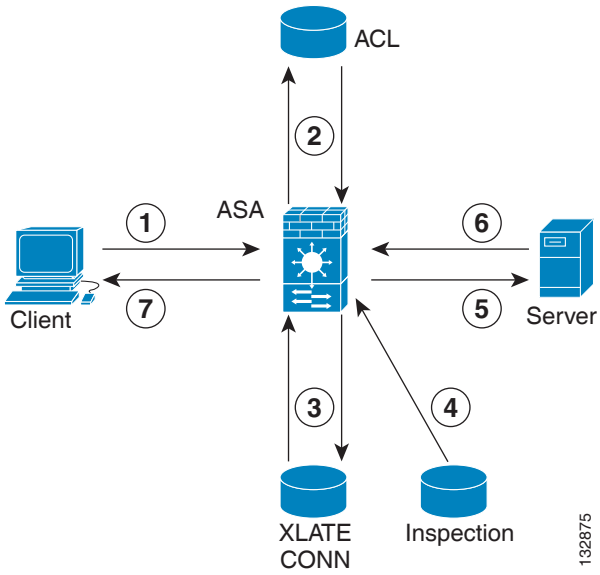
다음 항목에서는 애플리케이션 검사에 대해 좀 더 자세히 설명합니다.

검사 엔진 작동 방법

다음 그림에서 볼 수 있듯이 ASA에서는 기본 작동을 위해 세 가지 데이터베이스를 사용합니다.

- ACL - 특정 네트워크, 호스트, 서비스(TCP/UDP 포트 번호)를 기반으로 연결을 인증 및 승인하는 데 사용됩니다.
- Inspections - 미리 정의된 고정인 애플리케이션 수준 검사 기능 집합을 포함합니다.
- Connections(XLATE 및 CONN 테이블) - 설정된 각 연결에 대한 상태 및 기타 정보를 유지 관리합니다. 설정된 세션 내에서 효과적으로 트래픽을 전달하기 위해 Adaptive Security Algorithm 및 컷스루 프록시에서 이 정보가 사용됩니다.

그림 7-1 검사 엔진 작동 방법



이 그림에서는 발생하는 순서대로 작업에 번호를 매겼습니다.

1. TCP SYN 패킷이 ASA에 도착하여 새 연결을 설정합니다.
2. ASA에서는 ACL 데이터베이스를 사용하여 연결이 허용되는지 확인합니다.
3. ASA에서는 연결 데이터베이스에 새 항목을 만듭니다(XLATE 및 CONN 테이블).
4. ASA에서는 Inspections 데이터베이스를 사용하여 연결에 애플리케이션 수준 검사가 필요한지 확인합니다.
5. 애플리케이션 검사 엔진이 패킷에 대해 필요한 작업을 완료하면 ASA에서는 패킷을 목적지 시스템으로 전달합니다.
6. 목적지 시스템은 초기 요청에 응답합니다.
7. ASA에서는 응답 패킷을 받고, 연결 데이터베이스에서 연결을 조회하고, 설정된 세션에 속하는 경우 패킷을 전달합니다.

ASA의 기본 컨피그레이션에는 지원되는 프로토콜을 특정 TCP 또는 UDP 포트 번호와 연결하고 특별한 처리가 필요한지를 식별하는 애플리케이션 검사 항목 집합이 포함됩니다.

애플리케이션 프로토콜 검사를 사용해야 하는 경우

사용자가 연결을 설정하면 향후 패킷이 시간 소모형 점검을 우회할 수 있도록 ASA에서는 ACL을 기준으로 패킷을 점검하고, 주소 변환을 만들고, 빠른 경로에 세션용 항목을 만듭니다. 그러나 빠른 경로는 예측 가능한 포트 번호에 의존하며 패킷 내에서 주소 변환을 수행하지 않습니다.

많은 프로토콜이 보조 TCP 또는 UDP 포트를 엽니다. 동적으로 할당된 포트 번호를 협상하기 위해 잘 알려진 포트의 초기 세션이 사용됩니다.

다른 애플리케이션은 일반적으로 ASA를 통과할 때 변환되는 소스 주소와 일치해야 하는 IP 주소를 패킷에 포함합니다.

이러한 애플리케이션을 사용하는 경우 애플리케이션 검사를 활성화해야 합니다.

IP 주소를 포함하는 서비스에 대해 애플리케이션 검사를 활성화하면 ASA에서는 포함된 주소를 변환하고 변환의 영향을 받는 체크섬이나 기타 필드를 업데이트합니다.

동적으로 할당된 포트를 사용하는 서비스에 대해 애플리케이션 검사를 활성화하면 ASA에서는 동적 포트 할당을 식별하고 특정 세션 기간 중에 이러한 포트에서 데이터 교환을 허용하기 위해 세션을 모니터링합니다.

검사 정책 맵

*검사 정책 맵*을 사용하여 많은 애플리케이션 검사를 위한 특별한 작업을 구성할 수 있습니다. 이러한 맵은 선택 사항입니다. 검사 정책 맵을 지원하는 프로토콜에 대해 맵을 구성하지 않은 채 검사를 활성화할 수 있습니다. 기본 검사 작업 이외의 작업을 원하는 경우에만 이러한 맵이 필요합니다.

검사 정책 맵을 지원하는 애플리케이션 리스트는 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

검사 정책 맵은 다음과 같은 요소 중 하나 이상으로 구성됩니다. 검사 정책 맵에 사용할 수 있는 정확한 옵션은 애플리케이션에 따라 다릅니다.

- Traffic matching criteria - 애플리케이션 트래픽을 애플리케이션에 해당하는 기준(예: URL 문자열)으로 확인한 다음 작업을 활성화합니다.

  일부 트래픽 매칭 기준의 경우 패킷 내부의 텍스트를 확인하기 위해 정규식을 사용합니다. 정책 맵을 구성하기 전에, 단독으로 또는 정규식 클래스 맵에서 그룹으로 정규식을 만들고 테스트해야 합니다.

- Inspection class map - 일부 검사 정책 맵에서는 검사 클래스 맵을 사용하여 다중 트래픽 매칭 기준을 포함할 수 있습니다. 그러면 검사 정책 맵에서 검사 클래스 맵을 식별하고 해당 클래스에 대해 전체적으로 작업을 활성화할 수 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다. 그러나 서로 다른 일치에 대해 서로 다른 작업을 설정할 수는 없습니다.

- Parameters - 검사 엔진의 동작에 영향을 미칩니다.

다음 항목에서 자세한 내용을 제공합니다.

- 7-3 페이지의 사용 중인 검사 정책 맵 교체
- 7-4 페이지의 다중 트래픽 클래스 처리 방법

사용 중인 검사 정책 맵 교체

서비스 정책에서 이미 사용 중인 검사 정책 맵을 교체해야 하는 경우 다음 방법을 사용합니다.

- 모든 검사 정책 맵 - 사용 중인 검사 정책 맵을 다른 맵 이름으로 교체하려면 **inspect** *protocol map* 명령을 제거한 후 새 맵으로 다시 추가해야 합니다. 예:

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

- HTTP 검사 정책 맵 - 사용 중인 HTTP 검사 정책 맵을 수정하려는 경우(**policy-map type inspect http**), 변경 사항을 적용하려면 **inspect http** *map* 작업을 제거한 후 다시 적용해야 합니다. 예를 들어 "http-map" 검사 정책 맵을 수정하려면 Layer 3/4 정책에서 **inspect http http-map** 명령을 제거한 후 다시 추가해야 합니다.

```
hostname(config)# policy-map test
hostname(config-pmap)# class http
hostname(config-pmap-c)# no inspect http http-map
hostname(config-pmap-c)# inspect http http-map
```

다중 트래픽 클래스 처리 방법

여러 검사 클래스 맵을 지정할 수도 있고 검사 정책 맵의 일치 항목을 전달할 수도 있습니다.

패킷이 서로 다른여러 **match** 또는 **class** 명령과 일치하는 경우 ASA에서 작업을 적용하는 순서는 내부 ASA 규칙에 의해 결정되며, 검사 정책 맵에 추가된 순서에 의해 결정되지 않습니다. 내부 규칙은 애플리케이션 유형 및 패킷 분석의 논리적 진행에 의해 결정되며, 사용자가 구성할 수 없습니다. 예를 들어 HTTP 트래픽의 경우, Request Method 필드 분석이 Header Host Length 필드 분석을 선행합니다. Header Host Length 필드에 대한 작업이 수행되기 전에 Request Method 필드에 대한 작업이 수행됩니다. 예를 들어 다음의 일치 명령을 임의의 순서로 입력할 수 있지만 **match request method get** 명령이 가장 먼저 적용됩니다.

```
match request header host length gt 100
  reset
match request method get
  log
```

작업에서 패킷을 삭제하는 경우 검사 정책 맵에서 추가 작업이 수행되지 않습니다. 예를 들어, 첫 번째 작업에서 연결을 재설정하면 추가 일치 기준이 적용되지 않습니다. 첫 번째 작업에서 패킷을 기록하면, 두 번째 작업(예: 연결 재설정)이 발생할 수 있습니다.

패킷에 동일한 여러 **match** 또는 **class** 명령이 있는 경우 논리 맵에 나타나는 순서대로 적용됩니다. 예를 들어, 헤더 길이가 1001인 패킷의 경우 아래의 첫 번째 명령이 적용되고, 기록되고, 두 번째 명령이 적용된 후 재설정됩니다. 두 **match** 명령의 순서를 바꾸면, 두 번째 **match** 명령이 적용되기 전에 패킷이 삭제되고 연결이 재설정됩니다. 따라서 기록이 진행되지 않습니다.

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

클래스 맵은 클래스 맵 내 최저 우선 순위 **match** 명령을 기준으로 다른 클래스 맵 또는 **match** 명령과 동일한 유형으로 확인됩니다(우선 순위는 내부 규칙을 기반으로 함). 한 클래스 맵에 다른 클래스 맵과 동일한 유형의 최저 우선 순위 **match** 명령이 있으면, 정책 맵에 추가된 순서대로 클래스 맵이 적용됩니다. 각 클래스 맵의 최저 우선 순위 일치가 다른 경우, 더 높은 우선 순위 **match** 명령의 클래스 맵이 먼저 적용됩니다. 예를 들어 다음 3개의 클래스 맵에는 두 가지 유형의 **match** 명령, 즉 **match request-cmd**(더 높은 우선 순위) 및 **match filename**(더 낮은 우선 순위)이 포함되어 있습니다. ftp3 클래스 맵에는 두 명령이 모두 포함되어 있지만, 우선 순위가 가장 낮은 명령인 **match filename**으로 순위가 지정됩니다. ftp1 클래스 맵에는 우선 순위가 가장 높은 명령이 포함되어 있으므로, 정책 맵에서의 순서와 상관없이 가장 먼저 적용됩니다. ftp3 클래스 맵은 역시 **match filename** 명령이 포함된 ftp2 클래스 맵과 동일한 우선 순위가 지정됩니다. 이 둘은 정책 맵의 순서에 따라 적용됩니다(ftp3 -> ftp2).

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

애플리케이션 검사 지침

장애 조치 지침

검사가 필요한 멀티미디어 세션에 대한 상태 정보는 상태 기반 시스템 대체 작동을 위한 상태 링크로 전달되지 않습니다. 상태 링크를 통해 복제되는 SIP 및 GTP는 예외입니다.

IPv6 지침

다음 검사에 대해 IPv6을 지원합니다.

- DNS
- FTP
- HTTP
- ICMP
- SCCP(Skinny)
- SIP
- SMTP
- IPsec pass-through
- IPv6

다음 검사에 대해 NAT64를 지원합니다.

- DNS
- FTP
- HTTP
- ICMP

추가 지침 및 제한

- 일부 검사 엔진은 PAT, NAT, 외부 NAT 또는 동일한 보안 인터페이스 간 NAT를 지원하지 않습니다. NAT 지원에 대한 자세한 내용은 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오.
- 모든 애플리케이션 검사에서 ASA는 동시 활성 데이터 연결 수를 200개로 제한합니다. 예를 들어, FTP 클라이언트가 여러 보조 연결을 열면 FTP 검사 엔진은 200개의 활성 연결만 허용합니다. 따라서 201번째 연결은 삭제되며 ASA(Adaptive Security Appliance)는 시스템 오류 메시지를 생성합니다.
- 검사된 프로토콜은 고급 TCP 상태 추적 대상이 될 수 있으며, 이러한 연결의 TCP 상태는 자동으로 복제되지 않습니다. 이러한 연결은 대기 유닛으로 복제되는 한편, BE(Best Effort) 시도에서는 TCP 상태의 재설정을 시도합니다.
- ASA(인터페이스)로 전달된 TCP/UDP 트래픽은 기본적으로 검사됩니다. 그러나 인터페이스로 전달된 ICMP 트래픽은 ICMP 검사를 활성화하는 경우에도 검사되지 않습니다. 따라서 ASA가 백업 기본 경로를 통해 도달할 수 있는 소스에서 에코 요청이 오는 경우 등의 특정 상황에서는 인터페이스에 대한 ping(에코 요청)이 실패할 수 있습니다.

애플리케이션 검사를 위한 기본값

다음 항목에서는 애플리케이션 검사를 위한 기본 작업에 대해 설명합니다.

기본 검사 및 NAT 제한

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며, 모든 인터페이스의 트래픽에 검사가 적용됩니다(글로벌 정책). 기본 애플리케이션 검사 트래픽에는 각 프로토콜의 기본 포트에 대한 트래픽이 포함됩니다. 글로벌 정책은 하나만 적용할 수 있습니다. 따라서 글로벌 정책을 변경하려면(예: 검사를 비표준 포트에 적용하거나 기본적으로 사용되지 않는 검사 추가) 기본 정책을 편집해야 하거나, 비활성화한 후 새 정책을 적용해야 합니다.

다음 표에는 지원되는 모든 검사, 기본 클래스 맵에서 사용되는 기본 포트, 기본적으로 설정된 검사 엔진(굵은 글꼴로 표시)이 나열되어 있습니다. 또한 NAT 제한도 포함되어 있습니다. 이 표에서:

- 기본 포트에서 기본적으로 활성화된 검사 엔진은 굵은 글꼴로 표시됩니다.
- ASA는 표시된 표준과 호환되지만, 검사 대상 패킷에 규정준수를 적용하지는 않습니다. 예를 들어 FTP 명령은 특정 순서로 되어 있어야 하지만, ASA는 순서를 적용하지 않습니다.

표 7-1 지원되는 애플리케이션 검사 엔진

애플리케이션	기본 포트	NAT 제한	표준	설명
CTIQBE	TCP/2748	확장 PAT 없음. NAT64 없음. (클러스터링) 고정 PAT 없음.	—	—
DCERPC	TCP/135	NAT64 없음.	—	—
DNS over UDP	UDP/53	WINS를 통한 이름 확인에 NAT 지원을 이용할 수 없음.	RFC 1123	—
FTP	TCP/21	(클러스터링) 고정 PAT 없음.	RFC 959	—
GTP	UDP/3386 UDP/2123	확장 PAT 없음. NAT 없음.	—	특별 라이센스가 필요합니다.
H.323 H.225 및 **RAS**	TCP/1720 UDP/1718 UDP(RAS) 1718-1719	동적 NAT 또는 PAT 없음. 고정 PAT가 작동하지 않을 수 있음. (클러스터링) 고정 PAT 없음. 확장 PAT 없음. Per-Session PAT 없음. 동일한 보안 인터페이스에 NAT 없음. NAT64 없음.	ITU-T H.323, H.245, H225.0, Q.931, Q.932	—

표 7-1 지원되는 애플리케이션 검사 엔진 (계속)

애플리케이션	기본 포트	NAT 제한	표준	설명
HTTP	TCP/80	—	RFC 2616	ActiveX 및 Java를 제거하는 MTU 제한에 유의하십시오. MTU가 너무 작아 Java 또는 ActiveX 태그를 한 패킷에 포함할 수 없는 경우, 제거가 발생하지 않을 수 있습니다.
ICMP	—	—	—	ASA 인터페이스로 전달된 ICMP 트래픽은 검사되지 않습니다.
ICMP ERROR	—	—	—	—
ILS(LDAP)	TCP/389	확장 PAT 없음. NAT64 없음.	—	—
IM(Instant Messaging)	클라이언트에 따라 다름	확장 PAT 없음. NAT64 없음.	RFC 3860	—
IP Options	—	NAT64 없음.	RFC 791, RFC 2113	—
IPsec Pass Through	UDP/500	PAT 없음. NAT64 없음.	—	—
IPv6	—	NAT64 없음.	RFC 2460	—
MGCP	UDP/2427, 2727	확장 PAT 없음. NAT64 없음. (클러스터링) 고정 PAT 없음.	RFC 2705bis-05	—
MMP	TCP 5443	확장 PAT 없음. NAT64 없음.	—	—
NetBIOS Name Server over IP	UDP/137, 138(소스 포트)	확장 PAT 없음. NAT64 없음.	—	NBNS UDP 포트 137 및 NBDS UDP 포트 138에 대해 패킷의 NAT를 수행함으로써 NetBIOS가 지원됩니다.
PPTP	TCP/1723	NAT64 없음. (클러스터링) 고정 PAT 없음.	RFC 2637	—
RADIUS Accounting	1646	NAT64 없음.	RFC 2865	—
RSH	TCP/514	PAT 없음. NAT64 없음. (클러스터링) 고정 PAT 없음.	Berkeley UNIX	—
RTSP	TCP/554	확장 PAT 없음. NAT64 없음. (클러스터링) 고정 PAT 없음.	RFC 2326, 2327, 1889	HTTP 클로킹을 처리하지 않습니다.
ScanSafe(Cloud Web Security)	TCP/80 TCP/413	—	—	이러한 포트는 ScanSafe 검사를 위한 default-inspection-traffic 클래스에 포함되지 않습니다.

표 7-1 지원되는 애플리케이션 검사 엔진 (계속)

애플리케이션	기본 포트	NAT 제한	표준	설명
SIP	TCP/5060 UDP/5060	동일한 보안 인터페이스에 NAT 없음. 확장 PAT 없음. Per-Session PAT 없음. NAT64 또는 NAT46 없음. (클러스터링) 고정 PAT 없음.	RFC 2543	특정 상황에서는 TFTP에 업로드된 Cisco IP Phone 컨피그레이션을 처리하지 않습니다.
SKINNY(SCCP)	TCP/2000	동일한 보안 인터페이스에 NAT 없음. 확장 PAT 없음. Per-Session PAT 없음. NAT64, NAT46 또는 NAT66 없음. (클러스터링) 고정 PAT 없음.	—	특정 상황에서는 TFTP에 업로드된 Cisco IP Phone 컨피그레이션을 처리하지 않습니다.
SMTP 및 **ESMTP**	TCP/25	NAT64 없음.	RFC 821, 1123	—
SNMP	UDP/161, 162	NAT 또는 PAT 없음.	RFC 1155, 1157, 1212, 1213, 1215	v.2 RFC 1902-1908; v.3 RFC 2570-2580.
SQL*Net	TCP/1521	확장 PAT 없음. NAT64 없음. (클러스터링) 고정 PAT 없음.	—	v.1 및 v.2.
Sun RPC over UDP 및 TCP	UDP/111	확장 PAT 없음. NAT64 없음.	—	기본 규칙에는 UDP 포트 111이 포함됩니다. TCP 포트 111에 대해 Sun RPC 검사를 활성화하려면 TCP 포트 111과 맞춰보고 Sun RPC 검사를 수행하는 새 규칙을 만들어야 합니다.
TFTP	UDP/69	NAT64 없음. (클러스터링) 고정 PAT 없음.	RFC 1350	페이로드 IP 주소는 변환되지 않습니다.
WAAS	TCP/1-65535	확장 PAT 없음. NAT64 없음.	—	—
XDMCP	UDP/177	확장 PAT 없음. NAT64 없음. (클러스터링) 고정 PAT 없음.	—	—

기본 정책 컨피그레이션에는 다음 명령이 포함됩니다.

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
```

```
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

기본 검사 정책 맵

일부 검사 유형에서는 숨겨진 기본 정책 맵을 사용합니다. 예를 들어, 맵을 지정하지 않고 ESMTP 검사를 활성화하는 경우 _default_esmtp_map이 사용됩니다.

기본 검사는 각 검사 유형을 설명하는 섹션에 설명되어 있습니다. **show running-config all policy-map** 명령을 사용하거나를 사용하여 이러한 기본 맵을 볼 수 있습니다.

DNS 검사는 명시적으로 구성된 기본 맵인 preset_dns_map을 사용하는 유일한 검사입니다.

애플리케이션 계층 프로토콜 검사 구성

애플리케이션 검사는 서비스 정책에서 구성합니다. 서비스 정책은 ASA 기능을 구성하기 위한 일관되고 유연한 방법을 제공합니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 컨피그레이션을 만드는 서비스 정책을 사용할 수 있습니다. 일부 애플리케이션의 경우 검사를 활성화할 때 특별한 작업을 수행할 수 있습니다. 일반적인 서비스 정책에 대해 알아보려면 1 장, “Modular Policy Framework를 사용하는 서비스 정책”을 참조하십시오.

일부 애플리케이션에 대해서는 기본적으로 검사가 활성화됩니다. 자세한 내용은 7-6 페이지의 기본 검사 및 NAT 제한 섹션을 참조하십시오. 검사 정책을 수정하려면 이 섹션을 사용하십시오.

절차

1단계 기존 클래스 맵에 검사를 추가하지 않을 경우, 통과 트래픽 또는 관리 트래픽에 대해 Layer 3/4 클래스 맵의 검사를 적용할 트래픽을 확인합니다.

자세한 내용은 1-13 페이지의 통과 트래픽용 Layer 3/4 클래스 맵 만들기 및 1-15 페이지의 관리 트래픽용 Layer 3/4 클래스 맵 만들기를 참조하십시오. 관리 Layer 3/4 클래스 맵은 RADIUS 어카운팅 검사에서만 사용할 수 있습니다.

클래스 맵 선택에는 중요한 의미가 있습니다. inspection_default 클래스에만 둘 이상의 검사를 포함할 수 있으며, 단순히 검사 기본값을 적용하는 기존 글로벌 정책을 편집할 수도 있습니다. 선택할 클래스 맵에 대한 자세한 내용은 7-13 페이지의 검사를 위한 올바른 트래픽 클래스 선택을 참조하십시오.

2단계 (선택 사항) 일부 검사 엔진에서는 트래픽에 검사를 적용할 때 추가 매개변수를 제어할 수 있습니다. 이 절차의 뒷부분에 나오는 표에서는 구성 방법에 대한 참조 정보와 함께 검사 정책 맵을 허용하는 프로토콜을 보여줍니다.

3단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 Layer 3/4 정책 맵을 추가하거나 편집합니다.

```
hostname(config)# policy-map name
hostname(config-pmap)#
```

기본 정책 맵은 "global_policy"라고 합니다. 이 정책 맵에는 7-6 페이지의 기본 검사 및 NAT 제한에 나열된 기본 검사가 포함됩니다. 기본 정책을 수정하려면(예: 검사를 추가 또는 삭제하거나 작업을 위한 추가 클래스 맵 지정) 이름으로 **global_policy**를 입력하십시오.

4단계 작업을 할당할 클래스 맵을 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

기본 정책 맵을 편집하는 경우 inspection_default 클래스 맵이 포함됩니다. 이름으로 **inspection_default**를 입력하여 이 클래스에 대한 작업을 편집할 수 있습니다. 이 정책 맵에 클래스 맵을 추가하려면 다른 이름을 지정하십시오.

원하는 경우 여러 클래스 맵을 동일한 정책에 결합하여, 특정 트래픽에 적용할 클래스 맵과 다른 트래픽에 적용할 클래스 맵을 별도로 만들 수 있습니다. 그러나 트래픽이 검사 명령을 포함하는 클래스 맵과 일치하고 역시 검사 명령을 포함하는 또 다른 클래스 맵과도 일치하는 경우, 첫 번째 일치 클래스만 사용됩니다. 예를 들어, SNMP는 inspection_default 클래스 맵과 일치합니다. SNMP 검사를 활성화하려면 기본 클래스에 대해 SNMP 검사를 활성화하십시오. SNMP와 일치하는 다른 클래스를 추가하지 마십시오.

5단계 애플리케이션 검사를 활성화합니다.

```
hostname(config-pmap-c)# inspect protocol
```

*protocol*은 다음 값 중 하나입니다.

표 7-2 프로토콜 키워드

키워드	참고
ctiqbe	9-1 페이지의 CTIQBE 검사 섹션을 참조하십시오.
dcerpc [*map_name*]	11-1 페이지의 DCERPC 검사 섹션을 참조하십시오. 11-2 페이지의 DCERPC 검사 정책 맵 구성에 따라 DCERPC 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
dns [*map_name*] [**dynamic-filter-snoop**]	8-1 페이지의 DNS 검사 섹션을 참조하십시오. 8-3 페이지의 DNS 검사 정책 맵 구성에 따라 DNS 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오. 기본 DNS 검사 정책 맵 이름은 "preset_dns_map"입니다. 봇네트(botnet) 트래픽 필터에 대해 DNS 스누핑을 활성화하려면 **dynamic-filter-snoop** 키워드를 입력합니다.
esmtp [*map_name*]	8-39 페이지의 SMTP 및 Extended SMTP 검사 섹션을 참조하십시오. 8-41 페이지의 ESMTP 검사 정책 맵 구성에 따라 ESMTP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.

표 7-2 프로토콜 키워드

키워드	참고
ftp [**strict** [*map_name*]]	8-8 페이지의 FTP 검사 섹션을 참조하십시오. 보호되는 네트워크의 보안을 강화하려면 웹 브라우저가 FTP 요청에 포함된 명령을 전송하지 못하게 하여 **엄격한** 키워드를 사용하십시오. 자세한 내용은 8-9 페이지의 엄격한 FTP 섹션을 참조하십시오. 8-10 페이지의 FTP 검사 정책 맵 구성에 따라 FTP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
gtp [*map_name*]	11-4 페이지의 GTP 검사 섹션을 참조하십시오. 11-6 페이지의 GTP 검사 정책 맵 구성에 따라 GTP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
h323 h225 [*map_name*]	9-3 페이지의 H.323 검사 섹션을 참조하십시오. 9-6 페이지의 H.323 검사 정책 맵 구성에 따라 H323 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
h323 ras [*map_name*]	9-3 페이지의 H.323 검사 섹션을 참조하십시오. 9-6 페이지의 H.323 검사 정책 맵 구성에 따라 H323 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
http [*map_name*]	8-14 페이지의 HTTP 검사 섹션을 참조하십시오. 8-15 페이지의 HTTP 검사 정책 맵 구성에 따라 HTTP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
icmp	8-20 페이지의 ICMP 검사 섹션을 참조하십시오.
icmp error	8-20 페이지의 ICMP 오류 검사 섹션을 참조하십시오.
ils	10-1 페이지의 ILS 검사 섹션을 참조하십시오.
im [*map_name*]	8-21 페이지의 IM(Instant Messaging) 검사 섹션을 참조하십시오. 8-21 페이지의 IM 검사 정책 맵 구성에 따라 Instant Messaging 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
ip-options [*map_name*]	8-25 페이지의 IP Options 검사 섹션을 참조하십시오. 8-27 페이지의 IP Options 검사 정책 맵 구성에 따라 IP Options 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
ipsec-pass-thru [*map_name*]	8-29 페이지의 IPsec Pass Through 검사 섹션을 참조하십시오. 8-29 페이지의 IPsec Pass Through 검사에 따라 IPsec Pass Through 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
ipv6 [*map_name*]	8-32 페이지의 IPv6 검사 섹션을 참조하십시오. 8-33 페이지의 IPv6 검사 정책 맵 구성에 따라 IPv6 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.

표 7-2 프로토콜 키워드

키워드	참고
mgcp [*map_name*]	9-12 페이지의 MGCP 검사 섹션을 참조하십시오. 9-14 페이지의 추가 검사 제어를 위한 MGCP 검사 정책 맵 구성에 따라 MGCP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
netbios [*map_name*]	8-36 페이지의 NetBIOS 검사 섹션을 참조하십시오. 8-36 페이지의 추가 검사 제어를 위한 NetBIOS 검사 정책 맵 구성에 따라 NetBIOS 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
pptp	8-38 페이지의 PPTP 검사 섹션을 참조하십시오.
radius-accounting *map_name*	11-11 페이지의 RADIUS 어카운팅 검사 섹션을 참조하십시오. **radius-accounting** 키워드는 관리 클래스 맵에만 사용할 수 있습니다. RADIUS 어카운팅 검사 정책 맵을 지정해야 합니다. 11-12 페이지의 RADIUS 어카운팅 검사 정책 맵 구성을 참조하십시오.
rsh	11-14 페이지의 RSH 검사 섹션을 참조하십시오.
rtsp [*map_name*]	9-17 페이지의 RTSP 검사 섹션을 참조하십시오. 9-18 페이지의 RTSP 검사 정책 맵 구성에 따라 RTSP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
scansafe [*map_name*] [**fail-open** | **fail-closed**]	ScanSafe(Cloud Web Security)를 사용하려면 이 절차보다는 15-9 페이지의 Cloud Web Security로 트래픽을 전송하도록 서비스 정책 구성 항목에서 설명하는 절차를 사용하십시오. 해당 절차에서는 정책 검사 맵 컨피그레이션 방법을 비롯한 전체 정책 컨피그레이션에 대해 설명합니다.
sip [*map_name*] [**tls-proxy** *proxy_name*]	9-22 페이지의 SIP 검사 섹션을 참조하십시오. 9-25 페이지의 SIP 검사 정책 맵 구성에 따라 SIP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오. 암호화된 트래픽의 검사를 활성화하려면 TLS 프록시를 지정하십시오.
skinny [*map_name*] [**tls-proxy** *proxy_name*]	9-30 페이지의 Skinny(SCCP) 검사 섹션을 참조하십시오. 9-32 페이지의 추가 검사 제어를 위한 Skinny(SCCP) 검사 정책 맵 구성에 따라 Skinny 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오. 암호화된 트래픽의 검사를 활성화하려면 TLS 프록시를 지정하십시오.
snmp [*map_name*]	11-15 페이지의 SNMP 검사 섹션을 참조하십시오. SNMP 검사 정책 맵을 추가한 경우 이 명령에서 맵 이름을 확인하십시오.
sqlnet	10-2 페이지의 SQL*Net 검사 섹션을 참조하십시오.

표 7-2 프로토콜 키워드

키워드	참고
sunrpc	10-3 페이지의 Sun RPC 검사 섹션을 참조하십시오. 기본 클래스 맵은 UDP 포트 111을 포함합니다. TCP 포트 111에 대해 Sun RPC 검사를 활성화하려면 TCP 포트 111과 일치하는 새 클래스 맵을 만들고, 정책에 클래스를 추가한 다음, 해당 클래스에 **inspect sunrpc** 명령을 적용하십시오.
tftp	8-45 페이지의 TFTP 검사 섹션을 참조하십시오.
waas	TCP option 33 parsing을 활성화합니다. Cisco WAAS(Wide Area Application Services) 제품을 배포할 때 사용하십시오.
xdmcp	11-16 페이지의 XDMCP 검사 섹션을 참조하십시오.

참고 다른 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect** *protocol* 명령을 사용해 이전 검사를 제거한 다음 새 검사 정책 맵 이름으로 다시 추가해야 합니다.

6단계 하나 이상의 인터페이스에 대한 정책 맵을 활성화하려면 다음 명령을 입력합니다.

```
hostname(config)# service-policy policymap_name {global | interface interface_name}
```

여기서 **global**은 모든 인터페이스에서 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 기본적으로 기본 정책 맵 "global_policy"는 전체적으로 적용됩니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

검사를 위한 올바른 트래픽 클래스 선택

통과 트래픽을 위한 기본 Layer 3/4 클래스 맵은 "inspection_default"입니다. 이 클래스 맵은 각 애플리케이션 프로토콜에 대해 기본 포트를 확인하기 위해 특수한 **match** 명령인 **match default-inspection-traffic**을 사용합니다. 이 트래픽 클래스는(검사에 일반적으로 사용되지 않는 **match any**와 함께) IPv6을 지원하는 검사에 대해 IPv4와 IPv6 트래픽을 모두 확인합니다. IPv6 지원 검사 리스트는 7-5 페이지의 애플리케이션 검사 지침을 참조하십시오.

일치하는 트래픽을 특정 IP 주소로 좁히려면 **match access-list** 명령과 **match default-inspection-traffic** 명령을 함께 지정할 수 있습니다. **match default-inspection-traffic** 명령은 확인할 포트를 지정하므로 ACL의 포트는 모두 무시됩니다.

팁 애플리케이션 트래픽이 예상되는 포트에 대해서만 트래픽을 검사하는 것이 좋습니다. 예를 들어 **match any**를 사용하여 모든 트래픽을 검사하는 경우 ASA 성능이 저하될 수 있습니다.

비표준 포트를 검사하려면 비표준 포트에 대한 새 클래스 맵을 만듭니다. 각 검사 엔진에 대한 표준 포트는 7-6 페이지의 기본 검사 및 NAT 제한을 참조하십시오. 원하는 경우 여러 클래스 맵을 동일한 정책에 결합하여, 특정 트래픽에 적용할 클래스 맵과 다른 트래픽에 적용할 클래스 맵을 별도로 만들 수 있습니다. 그러나 트래픽이 검사 명령을 포함하는 클래스 맵과 일치하고 역시 검사 명령을 포함하는 또 다른 클래스 맵과도 일치하는 경우, 첫 번째 일치 클래스만 사용됩니다. 예를 들어 SNMP는 inspection_default 클래스를 확인합니다. SNMP 검사를 사용하려면 기본 클래스에 대해 SNMP 검사를 활성화하십시오. SNMP와 일치하는 다른 클래스를 추가하지 마십시오.

예를 들어 기본 클래스 맵을 사용하여 10.1.1.0에서 오는 트래픽에 대한 검사를 192.168.1.0으로 제한하려면 다음 명령을 입력합니다.

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

전체 클래스 맵을 보려면 다음 명령을 사용합니다.

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

포트 21과 1056(비표준 포트)에서 FTP 트래픽을 검사하려면 포트를 지정하는 ACL을 만들어 새 클래스 맵에 할당합니다.

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

정규식 구성

정규식은 텍스트 문자열을 확인하는 패턴을 정의합니다. URL 또는 특별 헤더 필드의 내용을 기반으로 일부 프로토콜 검사 맵에서 정규식을 사용하여 패킷을 일치시킬 수 있습니다.

정규식 만들기

정규식은 있는 그대로의 정확한 문자열로서 텍스트 문자열을 확인하거나, *메타 문자*를 사용하여 텍스트 문자열의 다양한 변형을 확인합니다. 특정 애플리케이션 트래픽의 내용을 확인하기 위해 정규식을 사용할 수 있습니다. 예를 들면 HTTP 패킷 내에서 URL 문자열을 확인할 수 있습니다.

시작하기 전에

물음표(?)나 탭 등 CLI의 모든 특수 문자를 이스케이프하려면 **Ctrl+V**를 사용하십시오. 예를 들면 **d[Ctrl+V]?g**를 입력하여 컨피그레이션에 **d?g**를 추가합니다.

패킷에 정규식을 적용할 때 성능에 미치는 영향을 보려면 명령 참조의 **regex** 명령을 참조하십시오. 일반적으로 일치 확인 대상이 긴 입력 문자열이거나 다수의 정규식인 경우 시스템 성능이 저하됩니다.

참고 최적화를 위해 ASA는 애매함이 제거된(deobfuscated) URL에서 검색합니다. 애매함 제거 방식(Deobfuscation)에서는 여러 슬래시(/)를 단일 슬래시로 압축합니다. "http://"와 같이 일반적으로 이중 슬래시를 사용하는 문자열의 경우 "http:/"를 대신 검색해야 합니다.

다음 표에는 특별한 의미를 지닌 메타 문자가 나열되어 있습니다.

표 7-3 정규식 메타 문자

문자	설명	참고
.	점	단일 문자와 일치합니다. 예를 들어 **d.g**는 dog, dag, dtg 및 그러한 문자가 포함된 단어(예: doggonnit)와 일치합니다.
(*exp***)**	하위 식	하위 식은 문자를 주변 문자와 분리하므로, 하위 식에서 기타 메타 문자를 사용할 수 있습니다. 예를 들어, **d(o|a)g**는 dog 및 dag와 일치하지만, **do|ag**는 do 및 ag와 일치합니다. 하위 식을 반복 한정자와 함께 사용하면 반복을 의미하는 문자를 구분할 수 있습니다. 예를 들어 **ab(xy){3}z**는 abxyxyxyz와 같습니다.
|	대안	구분하는 두 가지 식 중 하나와 일치합니다. 예를 들어 **dog|cat**은 dog 또는 cat과 일치합니다.
?	물음표	이전 식이 0 또는 1회 반복됨을 나타내는 한정자입니다. 예를 들어 **lo?se**는 lse 또는 lose와 일치합니다.
*	별표	이전 식이 0, 1 또는 임의의 숫자만큼 반복됨을 나타내는 한정자입니다. 예를 들어 **lo*se**는 lse, lose, loose 등과 일치합니다.
+	Plus	이전 식이 1회 이상 반복됨을 나타내는 한정자입니다. 예를 들어 **lo+se**는 lose 및 loose와 일치하지만 lse와는 일치하지 않습니다.
{*x*} 또는 {*x*,}	최소 반복 한정자	최소 *x*회 반복됩니다. 예를 들어 **ab(xy){2,}z**는 abxyxyz, abxyxyxyz 등과 일치합니다.
[*abc***]**	문자 클래스	괄호 안에 있는 모든 문자와 일치합니다. 예를 들어 **[abc]**는 a, b 또는 c와 일치합니다.
[^*abc***]**	부정 문자 클래스	괄호에 포함되지 않은 단일 문자와 일치합니다. 예를 들어 **[^abc]**는 a, b 또는 c 이외의 모든 문자와 일치합니다. **[^A-Z]**는 대문자가 아닌 모든 단일 문자와 일치합니다.
[*a-c***]**	문자 범위 클래스	범위에 있는 모든 문자와 일치합니다. **[a-z]**는 모든 소문자와 일치합니다. 문자 및 범위를 혼합할 수 있습니다. **[abcq-z]**는 a, b, c, q, r, s, t, u, v, w, x, y, z와 일치하며 **[a-cq-z]**도 마찬가지입니다. 대시(-) 문자는 괄호 안의 마지막 문자 또는 첫 번째 문자인 경우에만 리터럴입니다(예: **[abc-]** 또는 **[-abc]**).
“”	따옴표	문자열에 있는 선행 또는 후행 공백을 유지합니다. 예를 들어 **" test"**는 일치 항목을 찾을 때 선행 공백을 유지합니다.
^	캐럿	줄의 시작을 지정합니다.

표 7-3 정규식 메타 문자 (계속)

문자	설명	참고
\	이스케이프 문자	메타 문자와 함께 사용할 경우 리터럴 문자와 일치합니다. 예를 들어 **\[**는 왼쪽 각괄호와 일치합니다.
char	문자	문자가 메타 문자가 아닐 경우 리터럴 문자와 일치합니다.
\r	캐리지 리턴	캐리지 리턴 0x0d와 일치합니다.
\n	새 줄	새 줄 0x0a와 일치합니다.
\t	탭	탭 0x09와 일치합니다.
\f	폼피드	폼피드 0x0c와 일치합니다.
\x*NN*	이스케이프된 16진수 숫자	16진수(정확히 두 자릿수)를 사용하는 ASCII 문자와 일치합니다.
\NNN	이스케이프된 8진수 숫자	8진수(정확히 세 자릿수)를 사용하는 ASCII 문자와 일치합니다. 예를 들어, 문자 040은 공백을 나타냅니다.

절차

1단계 정규식을 테스트하여 원하는 내용과 일치하는지 확인합니다.

```
hostname(config)# test regex input_text regular_expression
```

여기서 *input_text* 인수는 정규식을 사용하여 확인하려는 문자열이며 길이는 최대 201자입니다.

regular_expression 인수의 길이는 최대 100자입니다.

CLI의 모든 특수 문자를 이스케이프하려면 **Ctrl+V**를 사용하십시오. 예를 들어 **test regex** 명령의 입력 텍스트에 탭을 입력하려면 **test regex "test[Ctrl+V Tab]" "test\t"**를 입력해야 합니다.

정규식이 입력 텍스트와 일치하면 다음 메시지가 표시됩니다.

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

정규식이 입력 텍스트와 일치하지 않으면 다음 메시지가 표시됩니다.

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

2단계 테스트 후 정규식을 추가하려면 다음 명령을 사용합니다.

```
hostname(config)# regex name regular_expression
```

여기서 *name* 인수의 길이는 최대 40자입니다.

regular_expression 인수의 길이는 최대 100자입니다.

예

다음 예에서는 검사 정책 맵에서 사용할 정규식 2개를 만듭니다.

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

정규식 클래스 맵 만들기

정규식 클래스 맵은 하나 이상의 정규식을 식별합니다. 이 맵은 정규식 객체 모음입니다. 정규식 객체 대신 많은 경우 정규식 클래스 맵을 사용할 수 있습니다.

절차

1단계 정규식 클래스 맵을 만듭니다.

```
hostname(config)# class-map type regex match-any class_map_name
hostname(config-cmap)#
```

여기서 *class_map_name*은 길이가 최대 40자인 문자열입니다. "class-default"는 예약된 이름입니다. 모든 유형의 클래스 맵은 동일한 네임스페이스를 사용하므로, 다른 클래스 맵 유형에서 사용된 이름을 재사용할 수 없습니다.

match-any 키워드는 트래픽이 하나 이상의 정규식과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다.

2단계 (선택 사항) 클래스 맵에 설명을 추가합니다.

```
hostname(config-cmap)# description string
```

3단계 각 정규식에 다음 명령을 입력함으로써 포함하고자 하는 정규식을 식별합니다.

```
hostname(config-cmap)# match regex regex_name
```

예

다음 예에서는 정규식 2개를 만들어 정규식 클래스 맵에 추가합니다. "example.com" 또는 "example2.com" 문자열이 포함되어 있으면 트래픽이 클래스 맵과 일치합니다.

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

애플리케이션 검사 기록

기능 이름	릴리스	설명
검사 정책 맵	7.2(1)	검사 정책 맵이 추가되었습니다. 추가된 명령: **class-map type inspect**.
정규식 및 정책 맵	7.2(1)	검사 정책 맵에서 사용할 수 있도록 정규식과 정책 맵이 추가되었습니다. 추가된 명령: **class-map type regex**, **regex**, **match regex**.
검사 정책 맵을 위한 Match any	8.0(2)	검사 정책 맵과 사용할 수 있도록 **match any** 키워드가 추가되었습니다. 트래픽이 하나 이상의 기준을 충족하면 클래스 맵과 일치합니다. 전에는 **match all**만 사용 가능했습니다.

8 장

기본 인터넷 프로토콜 검사

다음 항목에서는 기본 인터넷 프로토콜에 대한 애플리케이션 검사에 대해 설명합니다. 특정 프로토콜에 대해 검사를 사용해야 하는 이유 및 검사 적용을 위한 전반적인 방법에 대해 자세히 알아보려면 7-1 페이지의 애플리케이션 계층 프로토콜 검사 시작을 참조하십시오.

DNS 검사

다음 섹션에서는 DNS 애플리케이션 검사에 대해 설명합니다.

DNS 검사 작업

DNS 검사는 기본적으로 사용됩니다. 많은 작업을 수행할 수 있도록 DNS 검사를 사용자 지정할 수 있습니다.

- NAT 컨피그레이션을 기반으로 DNS 레코드를 변환합니다. 자세한 내용은 4-32 페이지의 DNS 및 NAT 섹션을 참조하십시오.
- 메시지 길이, 도메인 이름 길이 및 레이블 길이를 적용합니다.
- DNS 메시지에서 압축 포인터가 발견되는 경우 포인터에서 참조하는 도메인 이름의 무결성을 확인합니다.
- 압축 포인터 루프가 존재하는지 확인합니다.
- DNS 헤더, 유형, 클래스 등을 기반으로 패킷을 검사합니다.

DNS 검사를 위한 기본값

DNS 검사는 preset_dns_map 검사 클래스 맵을 사용하여 기본적으로 활성화됩니다.

- 최대 DNS 메시지 길이는 512바이트입니다.
- 최대 클라이언트 DNS 메시지 길이는 자동으로 리소스 레코드에 맞게 설정됩니다.
- DNS Guard가 사용되므로 ASA에 의해 DNS 회신이 전달되자마자 ASA에서 DNS 쿼리와 관련된 DNS 세션을 해제합니다. ASA는 또한 DNS 회신의 ID가 DNS 쿼리의 ID와 일치하는지 확인하기 위해 메시지 교환을 모니터링합니다.
- NAT 컨피그레이션으로 기반으로 하는 DNS 레코드의 변환이 활성화됩니다.
- 프로토콜 적용이 활성화되고, 이에 따라 DNS 메시지 형식 확인이 활성화됩니다. 여기에는 도메인 이름 길이 최대 255자, 레이블 길이 63자, 압축 및 반복되는 포인터 확인 등이 포함됩니다.

다음의 기본 DNS 검사 명령을 참조하십시오.

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
! ...
service-policy global_policy global
```

DNS 검사 구성

DNS 검사는 기본적으로 사용됩니다. 기본 이외의 프로세싱을 원하는 경우에만 구성해야 합니다. DNS 검사를 사용자 지정하려면 다음 프로세스를 사용합니다.

절차

1단계 8-3 페이지의 DNS 검사 정책 맵 구성.

2단계 8-6 페이지의 DNS 검사 서비스 정책 구성.

DNS 검사 정책 맵 구성

네트워크에서 기본 검사 동작만으로 충분하지 않은 경우 DNS 검사 정책 맵을 만들어 DNS 검사 작업을 사용자 지정할 수 있습니다.

트래픽 매칭 기준을 정의할 때 클래스 맵을 만들 수도 있고, 정책 맵에 일치 명령문을 직접 포함할 수도 있습니다. 다음 절차에서는 두 가지 방법을 모두 설명합니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 (선택 사항) 다음 단계를 수행하여 DNS 검사 클래스 맵을 만듭니다.

클래스 맵은 여러 트래픽 일치를 그룹화합니다. 대신 정책 맵에서 **match** 명령을 직접 지정할 수도 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.

클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다.

이 클래스 맵에서 식별하는 트래픽에 대해 수행할 작업을 검사 정책 맵에서 지정할 수 있습니다.

각 **match** 명령에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

a. 다음 명령을 입력하여 클래스 맵을 만듭니다.

```
hostname(config)# class-map type inspect dns [match-all | match-any] class_map_name
hostname(config-cmap)#
```

여기에서 *class_map_name*은 클래스 맵의 이름입니다. **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. match-any 키워드는 트래픽이 하나 이상의 **match** 문과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

b. (선택 사항) 클래스 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-cmap)# description string
```

여기서 *string*은 클래스 맵에 대한 설명입니다(최대 200자).

c. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **header-flag** [**eq**] {*f_name* [*f_name*...] | *f_value*} - DNS 플래그를 확인합니다. *f_name* 인수는 DNS 플래그 이름이며 **AA**(Authoritative Answer), **QR**(Query), **RA**(Recursion Available), **RD**(Recursion Desired), **TC**(Truncation) 중 하나입니다. *f_value* 인수는 0x로 시작하는 16진수의 16비트 값입니다(0x0~0xffff). **eq** 키워드는 정확한 일치(match all)를 지정합니다. **eq** 키워드가 없으면 패킷은 지정된 헤더 중 하나와만 일치하면 됩니다(match any). 예: **match header-flag AA QR**.
- **match** [**not**] **dns-type** {**eq** {*t_name* | *t_value*} | **range** *t_value1 t_value2*} - DNS 유형을 확인합니다. *t_name* 인수는 DNS 유형 이름이며 **A**(IPv4 address), **AXFR**(full zone transfer), **CNAME**(canonical name), **IXFR**(incremental zone transfer), **NS**(authoritative name server), **SOA**(start of a zone of authority) 또는 **TSIG**(transaction signature) 중 하나입니다. *t_value* 인수는 DNS Type 필드에서 지정하는 임의의 값입니다(0-65535). **range** 키워드는 범위를 지정하고 **eq** 키워드는 정확한 일치를 지정합니다. 예: **match dns-type eq A**.
- **match** [**not**] **dns-class** {**eq** {**in** | *c_value*} | **range** *c_value1 c_value2*} - DNS 클래스를 확인합니다. 클래스는 **in**(Internet) 또는 *c_value,* 즉 DNS Class 필드에서 지정하는 임의의 값입니다(0-65535). **range** 키워드는 범위를 지정하고 **eq** 키워드는 정확한 일치를 지정합니다. 예: **match dns-class eq in**.
- **match** [**not**] {**question** | **resource-record** {**answer** | **authority** | **additional**}} - DNS 질문 또는 리소스 레코드를 확인합니다. **question** 키워드는 DNS 메시지의 질문 부분을 지정합니다. **resource-record** 키워드는 리소스 레코드의 **answer**, **authority** 또는 **additional** 섹션 중 하나를 지정합니다. 예: **match resource-record answer**.
- **match** [**not**] **domain-name regex** {*regex_name* | **class** *class_name*} - DNS 메시지 도메인 이름 리스트를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.

d. 클래스 맵 컨피그레이션 모드를 종료하려면 **exit**를 입력합니다.

2단계 DNS 검사 정책 맵을 만들고 다음 명령을 입력합니다.

```
hostname(config)# policy-map type inspect dns policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

3단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

4단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.

- DNS 클래스 맵을 만든 경우 다음 명령을 입력하여 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- DNS 클래스 맵에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {drop [log] | drop-connection [log] |
enforce-tsig {[drop] [log]} | mask [log] | log}
```

각 **match** 또는 **class** 명령에서 모든 옵션을 사용할 수 있는 것은 아닙니다. 사용 가능한 정확한 옵션은 CLI 도움말 또는 명령 참조에서 확인할 수 있습니다.

drop 키워드는 일치하는 모든 패킷을 삭제합니다.

drop-connection 키워드는 패킷을 삭제하고 연결을 닫습니다.

mask 키워드는 패킷에서 일치하는 부분을 마스크 처리합니다. 이 작업은 헤더 플래그 일치에만 사용할 수 있습니다.

단독으로 또는 기타 키워드와 함께 사용할 수 있는 **log** 키워드는 시스템 로그 메시지를 전송합니다.

enforce-tsig {[**drop**] [**log**]} 키워드는 메시지에 있는 TSIG 리소스 레코드의 프레즌스를 적용합니다. TSIG 리소스 레코드 없이 패킷을 삭제하거나, 기록하거나, 삭제하고 기록할 수 있습니다. 헤더 플래그 일치에 대한 마스크 작업과 함께 이 옵션을 사용할 수 있습니다. 그렇게 하지 않으면 이 작업은 다른 작업과 별도로 적용됩니다.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다. **class** 및 **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

예:

```
hostname(config)# policy-map type inspect dns dns-map
hostname(config-pmap)# class dns-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match header-flag eq aa
hostname(config-pmap-c)# drop log
```

5단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **dns-guard** - DNS Guard를 활성화합니다. ASA에 의해 DNS 회신이 전달되자마자 ASA에서 DNS 쿼리와 관련된 DNS 세션을 해제합니다. ASA는 또한 DNS 회신의 ID가 DNS 쿼리의 ID와 일치하는지 확인하기 위해 메시지 교환을 모니터링합니다.
- **id-mismatch count** *number* **duration** *seconds* **action log** - 과도한 DNS ID 불일치의 기록을 활성화합니다. 여기서 **count** *number* **duration** *seconds* 인수는 시스템 메시지 기록이 전송되기 전 초당 최대 불일치 인스턴스 수를 지정합니다.
- **id-randomization** - DNS 쿼리에 대한 DNS 식별자를 임의로 지정합니다.
- **message-length maximum** {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}} - 최대 DNS 메시지 길이를 지정합니다(512~65535바이트). 클라이언트 또는 서버 메시지의 최대 길이도 설정할 수 있습니다. **auto** 키워드는 최대 길이를 Resource Record의 값으로 설정합니다.
- **nat-rewrite** - NAT 컨피그레이션을 기반으로 DNS 레코드를 변환합니다.
- **protocol-enforcement** - DNS 메시지 형식 확인이 활성화됩니다. 여기에는 도메인 이름 길이 최대 255자, 레이블 길이 63자, 압축 및 반복되는 포인터 확인 등이 포함됩니다.
- **tsig enforced action** {[**drop**] [**log**]} - TSIG 리소스 레코드가 있어야 합니다. 일치하지 않는 패킷을 삭제(**drop**)하거나, 기록(**log**)하거나, 삭제하고 기록할 수 있습니다.

예:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

예

다음 예는 DNS 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
regex domain_example "example\.com"
regex domain_foo "foo\.com"

! define the domain names that the server serves
class-map type inspect regex match-any my_domains
    match regex domain_example
    match regex domain_foo

! Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
    match not header-flag QR
    match question
    match not domain-name regex class my_domains

policy-map type inspect dns new_dns_map
    class pub_server_map
        drop log
    match header-flag RD
        mask log
    parameters
        message-length maximum client auto
        message-length maximum 512
        dns-guard
        protocol-enforcement
        nat-rewrite
```

DNS 검사 서비스 정책 구성

기본 ASA 컨피그레이션에는 모든 인터페이스에 전체적으로 적용되는 기본 포트에 대한 DNS 검사가 포함됩니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 DNS 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 DNS 검사를 구성합니다.

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

여기서 각 항목은 다음을 나타냅니다.

- *dns_policy_map*은 선택적인 DNS 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. DNS 검사 정책 맵 생성에 대한 자세한 내용은 8-3 페이지의 DNS 검사 정책 맵 구성을 참조하십시오.
- **dynamic-filter-snoop**는 Botnet Traffic Filter에서만 사용되는 동적 필터 스누핑을 활성화합니다. Botnet Traffic Filtering을 사용하는 경우에만 이 키워드를 포함하십시오. 외부 DNS 요청이 이동하는 인터페이스에서만 DNS 스누핑을 활성화하는 것이 좋습니다. 내부 DNS 서버로 이동하는 트래픽을 포함하여 모든 UDP DNS 트래픽에서 DNS 스누핑을 활성화하면 ASA에 불필요한 부하가 발생합니다.

예:

```
hostname(config-class)# no inspect dns
hostname(config-class)# inspect dns dns-map
```

참고 다른 DNS 검사 정책 맵(예: 기본 preset_dns_map을 교체)을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect dns** 명령을 사용해 DNS 검사를 제거한 다음 새 DNS 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

예

다음 예는 글로벌 기본 컨피그레이션에서 새로운 검사 정책 맵을 사용하는 방법을 보여줍니다.

```
policy-map global_policy
 class inspection_default
  no inspect dns preset_dns_map
  inspect dns new_dns_map
service-policy global_policy global
```

DNS 검사 모니터링

현재 DNS 연결에 대한 정보를 보려면 를 사용합니다.

```
hostname# show conn
```

DNS 서버를 사용하는 연결에 대해, 연결의 소스 포트를 show conn 명령 출력에 있는 DNS 서버의 IP 주소와 교체할 수 있습니다.

여러 DNS 세션이 동일한 두 호스트 사이에 있는 한, 이러한 세션에 대해 단일 연결이 생성되며 동일한 5개 튜플(source/destination IP address, source/destination port 및 protocol)이 적용됩니다. DNS 식별은 app_id에 의해 추적되며, 각 app_id의 유휴 타이머는 독립적으로 실행됩니다.

app_id는 독립적으로 만료되므로, 정상적인 DNS 응답만이 제한된 기간 내에 보안 어플라이언스를 통과할 수 있으며 리소스 빌드업은 없습니다. 그러나 **show conn** 명령을 입력하면 DNS 연결의 유휴 타이머가 새로운 DNS 세션에 의해 재설정되는 것을 확인할 수 있습니다. 이는 공유 DNS 연결의 본질 때문이며 의도적인 설정입니다.

DNS 애플리케이션 검사의 통계를 표시하려면 **show service-policy** 명령을 입력합니다. 다음은 **show service-policy** 명령의 샘플 출력입니다.

```
hostname# show service-policy
Interface outside:
  Service-policy: sample_policy
    Class-map: dns_port
      Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

FTP 검사

다음 섹션에서는 FTP 검사 엔진에 대해 설명합니다.

FTP 검사 개요

FTP 애플리케이션 검사는 FTP 세션을 검사하고 4가지 작업을 수행합니다.

- 동적 보조 데이터 연결 준비
- FTP 명령-응답 시퀀스 추적

- 감사 추적 생성
- 포함된 IP 주소 변환

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

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

엄격한 FTP

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

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

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

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

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

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

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

FTP 검사 구성

FTP 검사는 기본적으로 사용됩니다. 기본 이외의 프로세싱을 원하는 경우에만 구성해야 합니다. FTP 검사를 사용자 지정하려면 다음 프로세스를 사용합니다.

절차

1단계 8-10 페이지의 FTP 검사 정책 맵 구성.

2단계 8-12 페이지의 Configure the FTP Inspection Service Policy.

FTP 검사 정책 맵 구성

보안 및 제어 기능 향상을 위해 FTP 명령 필터링 및 보안 점검은 엄격한 FTP 검사를 사용해 제공됩니다. 프로토콜 준수 항목에는 패킷 길이 점검, 구분 기호 및 패킷 형식 점검, 명령 종결자 점검, 명령 검증 등이 포함됩니다.

사용자 값을 기반으로 하는 FTP 차단도 지원되므로 FTP 사이트에 다운로드할 파일을 게시할 수 있지만 특정 사용자의 액세스는 제한됩니다. 파일 형식, 서버 이름 및 기타 특성을 기반으로 FTP 연결을 차단할 수 있습니다. 검사 후 FTP 연결이 거부되면 시스템 메시지 로그가 생성됩니다.

FTP 검사에서 FTP 서버가 시스템 유형을 FTP 클라이언트에 공개하도록 허용하고 허용되는 FTP 명령을 제한하려면 FTP 검사 정책 맵을 만들고 구성하십시오. 그러면 FTP 검사를 사용할 때 맵을 적용할 수 있습니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 (선택 사항) 다음 단계를 수행하여 FTP 검사 클래스 맵을 만듭니다.

클래스 맵은 여러 트래픽 일치를 그룹화합니다. 대신 정책 맵에서 **match** 명령을 직접 지정할 수도 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.

클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다.

이 클래스 맵에서 식별하는 트래픽에 대해 수행할 작업을 검사 정책 맵에서 지정할 수 있습니다.

각 **match** 명령에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

a. 다음 명령을 입력하여 클래스 맵을 만듭니다.

```
hostname(config)# class-map type inspect ftp [match-all | match-any] class_map_name
hostname(config-cmap)#
```

여기에서 *class_map_name*은 클래스 맵의 이름입니다. **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. match-any 키워드는 트래픽이 하나 이상의 **match** 문과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

b. (선택 사항) 클래스 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-cmap)# description string
```

여기서 *string*은 클래스 맵에 대한 설명입니다(최대 200자).

c. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*} - FTP 전송의 파일 이름을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **filetype regex** {*regex_name* | **class** *class_name*} - FTP 전송의 파일 형식을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **request-command** *ftp_command* [*ftp_command...*] - 하나 이상의 다음과 같은 FTP 명령을 확인합니다.

  APPE - 파일에 추가합니다.

  CDUP - 현재 작업 디렉토리의 상위 디렉토리로 변경합니다.

  DELE - 서버의 파일을 삭제합니다.

  GET - 서버에서 파일을 가져옵니다.

  HELP - 도움말 정보를 제공합니다.

  MKD - 서버에 디렉토리를 만듭니다.

  PUT - 파일을 서버로 전송합니다.

  RMD - 서버에서 디렉토리를 삭제합니다.

  RNFR - "rename-from" 파일 이름을 지정합니다.

  RNTO - "rename-to" 파일 이름을 지정합니다.

  SITE - 서버 전용 명령을 지정하는 데 사용됩니다. 주로 원격 관리에 사용됩니다.

  STOU - 고유한 파일 이름을 사용하여 파일을 저장합니다.

- **match** [**not**] **server regex** {*regex_name* | **class** *class_name*} - FTP 서버 이름을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **username regex** {*regex_name* | **class** *class_name*} - FTP 사용자 이름을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.

d. 클래스 맵 컨피그레이션 모드를 종료하려면 **exit**를 입력합니다.

2단계 FTP 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect ftp policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

3단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

4단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.

- FTP 클래스 맵을 만든 경우 다음 명령을 입력하여 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- FTP 클래스 맵에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# reset [log]
```

reset 키워드는 패킷을 삭제하고, 연결을 닫고, TCP 재설정을 서버 또는 클라이언트로 전송합니다. 시스템 로그 메시지를 전송하려면 **log** 키워드를 추가합니다.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다. **class** 및 **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

5단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **mask-banner** - FTP 서버의 인사 배너를 마스크 처리합니다.
- **mask-syst-reply** - **syst** 명령에 대한 회신을 마스크 처리합니다.

예

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

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

hostname(config)# service-policy ftp-policy interface inside
```

Configure the FTP Inspection Service Policy

기본 ASA 컨피그레이션에는 모든 인터페이스에 전체적으로 적용되는 기본 포트에 대한 FTP 검사가 포함됩니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map ftp_class_map
hostname(config-cmap)# match access-list ftp
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 FTP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

```
class name
```

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 FTP 검사를 구성합니다.

```
inspect ftp [strict [ftp_policy_map]]
```

여기서 각 항목은 다음을 나타냅니다.

- **strict**는 엄격한 FTP를 구현합니다. FTP 검사 정책 맵을 지정하려면 엄격한 FTP를 사용해야 합니다.
- *ftp_policy_map*은 선택적인 FTP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. FTP 검사 정책 맵 생성에 대한 자세한 내용은 8-10 페이지의 FTP 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect ftp
hostname(config-class)# inspect ftp strict ftp-map
```

참고 다른 FTP 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect ftp** 명령을 사용해 FTP 검사를 제거한 다음 새 FTP 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

FTP 검사 확인 및 모니터링

FTP 애플리케이션 검사는 다음 로그 메시지를 생성합니다.

- 검색하거나 업로드하는 각 파일에 대해 감사 레코드 303002가 생성됩니다.
- FTP 명령이 RETR 또는 STOR인지를 확인하고, retrieve 및 store 명령이 기록됩니다.
- IP 주소를 제공하는 테이블을 조회하여 사용자 이름을 가져옵니다.
- 사용자 이름, 소스 IP 주소, 수신 IP 주소, NAT 주소 및 파일 작업이 기록됩니다.
- 메모리가 부족하여 보조 동적 채널 준비가 실패하면 감사 레코드 201005가 생성됩니다.

FTP 애플리케이션 검사는 NAT와 함께 애플리케이션 페이로드 내에서 IP 주소를 변환합니다. 이 내용은 RFC 959에 자세히 설명되어 있습니다.

HTTP 검사

다음 섹션에서는 HTTP 검사 엔진에 대해 설명합니다.

- 8-14 페이지의 HTTP 검사 개요
- 8-15 페이지의 HTTP 검사 구성

HTTP 검사 개요

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

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

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

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

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

고급 HTTP 검사는 모든 HTTP 메시지에서 다음을 확인합니다.

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

HTTP 검사 구성

HTTP 검사는 기본적으로 사용되지 않습니다. HTTP 검사 및 애플리케이션 필터링에 특수 모듈(예: ASA CX 또는 ASA FirePOWER)을 사용하지 않는 경우 다음 프로세스를 사용하여 ASA에서 HTTP 검사를 수동으로 구성할 수 있습니다.

팁 서비스 모듈과 ASA 모두에서 HTTP 검사를 구성하지 마십시오. 두 검사는 호환되지 않습니다.

절차

1단계 8-15 페이지의 HTTP 검사 정책 맵 구성.

2단계 8-19 페이지의 HTTP 검사 서비스 정책 구성.

HTTP 검사 정책 맵 구성

메시지가 매개변수를 위반하는 경우의 작업을 지정하려면 HTTP 검사 정책 맵을 만듭니다. 그러면 HTTP 검사를 사용할 때 검사 정책 맵을 적용할 수 있습니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 (선택 사항) 다음 단계를 수행하여 HTTP 검사 클래스 맵을 만듭니다.

클래스 맵은 여러 트래픽 일치를 그룹화합니다. 대신 정책 맵에서 **match** 명령을 직접 지정할 수도 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.

클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다.

이 클래스 맵에서 식별하는 트래픽에 대해 수행할 작업을 검사 정책 맵에서 지정할 수 있습니다.

각 **match** 명령에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

a. 다음 명령을 입력하여 클래스 맵을 만듭니다.

```
hostname(config)# class-map type inspect http [match-all | match-any] class_map_name
hostname(config-cmap)#
```

여기에서 *class_map_name*은 클래스 맵의 이름입니다. **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. match-any 키워드는 트래픽이 하나 이상의 **match** 문과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

b. (선택 사항) 클래스 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-cmap)# description string
```

여기서 *string*은 클래스 맵에 대한 설명입니다(최대 200자).

c. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **req-resp content-type mismatch** - HTTP 응답의 content-type 필드가 해당 HTTP 요청 메시지의 accept 필드와 일치하지 않는 경우 트래픽을 확인합니다.
- **match** [**not**] **request args regex** {*regex_name* | **class** *class_name*} - HTTP 요청 메시지 인수에 있는 텍스트를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **request body** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*} - HTTP 요청 메시지 본문에 있는 텍스트를 지정된 정규식 또는 정규식 클래스와 맞춰보거나, 요청 본문이 지정된 길이보다 큰 경우 메시지와 맞춰봅니다.
- **match** [**not**] **request header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*} - HTTP 요청 메시지 헤더에 있는 필드의 내용을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다. 필드 이름을 정확히 지정할 수도 있고 정규식을 이용할 수도 있습니다. 필드 이름: accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.
- **match** [**not**] **request header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*} - HTTP 요청 메시지 헤더에 있는 지정된 필드의 길이 또는 전체 필드 수(count)를 확인합니다. 필드 이름을 정확히 지정할 수도 있고 정규식 또는 정규식 클래스를 이용할 수도 있습니다. 필드 이름은 바로 위에 나열되어 있습니다.
- **match** [**not**] **request header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**} - HTTP 요청 메시지 헤더의 전체 길이, 헤더에 있는 전체 필드 수(count) 또는 비 ASCII 문자가 있는 헤더를 확인합니다.
- **match** [**not**] **request method** {*method* | **regex** {*regex_name* | **class** *class_name*}} - HTTP 요청 메서드를 확인합니다. 메서드를 정확히 지정할 수도 있고 메서드를 정규식 또는 정규식 클래스와 맞춰볼 수도 있습니다. 메서드: bcopy, bdelete, bmove, bpropfind, bproppatch, connect, copy, delete, edit, get, getattribute, getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, revlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.

- **match** [**not**] **request uri** {**regex** {*regex_name* | **class** *class_name*} | **length gt** *bytes*} - HTTP 요청 메시지 URI에 있는 텍스트를 지정된 정규식 또는 정규식 클래스와 맞춰보거나, 요청 URI가 지정된 길이보다 큰 메시지를 확인합니다.
- **match** [**not**] **response body** {**active-x** | **java-applet** | **regex** {*regex_name* | **class** *class_name*}} - HTTP 응답 메시지 본문에 있는 텍스트를 지정된 정규식 또는 정규식 클래스와 맞춰보거나, 필터링을 위해 Java 애플릿 및 Active X 객체 태그를 주석 처리합니다.
- **match** [**not**] **response body length gt** *bytes* - 본문이 지정된 길이보다 긴 HTTP 응답 메시지를 확인합니다.
- **match** [**not**] **response header** {*field* | **regex** *regex_name*} **regex** {*regex_name* | **class** *class_name*} - HTTP 응답 메시지 헤더에 있는 필드의 내용을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다. 필드 이름을 정확히 지정할 수도 있고 정규식을 이용할 수도 있습니다. 필드 이름: accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.
- **match** [**not**] **response header** {*field* | **regex** {*regex_name* | **class** *class_name*}} {**length gt** *bytes* | **count gt** *number*} - HTTP 응답 메시지 헤더에 있는 지정된 필드의 길이 또는 전체 필드 수(count)를 확인합니다. 필드 이름을 정확히 지정할 수도 있고 정규식 또는 정규식 클래스를 이용할 수도 있습니다. 필드 이름은 바로 위에 나열되어 있습니다.
- **match** [**not**] **response header** {**length gt** *bytes* | **count gt** *number* | **non-ascii**} - HTTP 응답 메시지 헤더의 전체 길이, 헤더에 있는 전체 필드 수(count) 또는 비 ASCII 문자가 있는 헤더를 확인합니다.
- **match** [**not**] **response status-line regex** {*regex_name* | **class** *class_name*} - HTTP 응답 메시지 상태 줄에 있는 텍스트를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.

d. 클래스 맵 컨피그레이션 모드를 종료하려면 **exit**를 입력합니다.

2단계 HTTP 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect http policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

3단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

4단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.

- HTTP 클래스 맵을 만든 경우 다음 명령을 입력하여 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- HTTP 클래스 맵에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {drop-connection [log]| reset [log] | log}
```

drop-connection 키워드는 패킷을 삭제하고 연결을 닫습니다.

reset 키워드는 패킷을 삭제하고, 연결을 닫고, TCP 재설정을 서버 또는 클라이언트로 전송합니다.

단독으로 또는 기타 키워드와 함께 사용할 수 있는 **log** 키워드는 시스템 로그 메시지를 전송합니다.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다. **class** 및 **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

5단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **body-match-maximum** *number* - 본문 일치에서 검색 가능한 HTTP 메시지 본문의 최대 문자 수를 설정합니다. 기본값은 200바이트입니다. 숫자가 커지면 성능에 큰 영향을 미치게 됩니다.
- **protocol-violation action** {**drop-connection** [**log**] | **reset** [**log**] | **log**} - 본문 일치에서 검색 가능한 HTTP 메시지 본문의 최대 문자 수를 설정합니다. 기본값은 200바이트입니다. 숫자가 커지면 HTTP 프로토콜 위반에 대한 performance.xxxChecks에 큰 영향을 미치게 됩니다. 위반에 대해 수행할 작업(패킷 삭제, 연결 해제, 재설정, 기록 등) 및 기록의 사용 여부도 선택해야 합니다.
- **spoof-server** *string* - 서버 헤더 필드의 문자열을 대체합니다. WebVPN 스트림은 **spoof-server** 명령의 영향을 받지 않습니다.

예

다음 예는 "GET" 또는 "PUT" 메서드로 "www\.xyz.com/.*\.asp" 또는 "www\.xyz[0-9][0-9]\.com"에 액세스를 시도하는 HTTP 연결을 허용하고 기록할 HTTP 검사 정책 맵을 정의하는 방법을 보여줍니다. 다른 모든 URL/메서드 조합은 자동으로 허용됩니다.

```
hostname(config)# regex url1 “www\.xyz.com/.*\.asp”
hostname(config)# regex url2 “www\.xyz[0-9][0-9]\.com”
hostname(config)# regex get “GET”
hostname(config)# regex put “PUT”

hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit

hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit

hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit

hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

HTTP 검사 서비스 정책 구성

HTTP 검사는 기본 검사 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. 그러나 기본 검사 클래스에는 기본 HTTP 포트가 포함되어 있지 않으므로, 기본 글로벌 검사 정책을 편집하여 HTTP 검사를 추가하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map http_class_map
hostname(config-cmap)# match access-list http
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 HTTP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

```
class name
```

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 HTTP 검사를 구성합니다.

```
inspect http [http_policy_map]
```

여기서 *http_policy_map*은 선택적인 HTTP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. HTTP 검사 정책 맵 생성에 대한 자세한 내용은 8-15 페이지의 HTTP 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect http
hostname(config-class)# inspect http http-map
```

참고 다른 HTTP 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect http** 명령을 사용해 HTTP 검사를 제거한 다음 새 HTTP 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

ICMP 검사

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

그러나 ASA 인터페이스로 전달된 ICMP 트래픽은 ICMP 검사를 활성화하는 경우에도 검사되지 않습니다. 따라서 ASA가 백업 기본 경로를 통해 도달할 수 있는 소스에서 에코 요청이 오는 경우 등의 특정 상황에서는 인터페이스에 대한 ping(에코 요청)이 실패할 수 있습니다.

ICMP 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

ICMP 오류 검사

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

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

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

- IP 헤더 - 매핑된 IP가 실제 IP(수신 주소)로 변경되고 IP 체크섬이 수정됩니다.
- ICMP 헤더 - ICMP 패킷의 변경으로 인해 ICMP 체크섬이 수정됩니다.

- 페이로드 변경 사항:
  - 원래 패킷의 매핑된 IP가 실제 IP로 변경됨
  - 원래 패킷의 매핑된 포트가 실제 포트로 변경됨
  - 원래 패킷 IP 체크섬이 다시 계산됨

ICMP 오류 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

IM(Instant Messaging) 검사

IM 검사 엔진을 사용하면 IM의 네트워크 사용량을 제어할 수 있으며 기밀 데이터 유출, 웜의 전파 및 기업 네트워크에 대한 기타 위협을 막을 수 있습니다.

IM 검사는 기본적으로 사용되지 않습니다. IM 검사를 사용하려면 구성해야 합니다.

절차

1단계 8-21 페이지의 IM 검사 정책 맵 구성.

2단계 8-24 페이지의 IM 검사 서비스 정책 구성.

IM 검사 정책 맵 구성

메시지가 매개변수를 위반하는 경우의 작업을 지정하려면 IM 검사 정책 맵을 만듭니다. 그러면 IM 검사를 사용할 때 검사 정책 맵을 적용할 수 있습니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 (선택 사항) 다음 단계를 수행하여 IM 검사 클래스 맵을 만듭니다.

클래스 맵은 여러 트래픽 일치를 그룹화합니다. 대신 정책 맵에서 **match** 명령을 직접 지정할 수도 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.

클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다.

이 클래스 맵에서 식별하는 트래픽에 대해 수행할 작업을 검사 정책 맵에서 지정할 수 있습니다.

각 **match** 명령에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

a. 다음 명령을 입력하여 클래스 맵을 만듭니다.

```
hostname(config)# class-map type inspect im [match-all | match-any] class_map_name
hostname(config-cmap)#
```

여기에서 *class_map_name*은 클래스 맵의 이름입니다. **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. match-any 키워드는 트래픽이 하나 이상의 **match** 문과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

b. (선택 사항) 클래스 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-cmap)# description string
```

여기서 *string*은 클래스 맵에 대한 설명입니다(최대 200자).

c. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **protocol {im-yahoo | im-msn}** - 특정 IM 프로토콜(Yahoo 또는 MSN)을 확인합니다.
- **match** [**not**] **service {chat | file-transfer | webcam | voice-chat | conference | games}** - 특정 IM 서비스를 확인합니다.
- **match** [**not**] **login-name regex** {*regex_name* | **class** *class_name*} - IM 메시지의 소스 클라이언트 로그인 이름을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **peer-login-name regex** {*regex_name* | **class** *class_name*} - IM 메시지의 목적지 피어 로그인 이름을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **ip-address** *ip_address mask*} - 소스 IP 주소 및 IM 메시지의 마스크를 확인합니다.
- **match** [**not**] **peer-ip-address** *ip_address mask*} - 수신 IP 주소 및 IM 메시지의 마스크를 확인합니다.
- **match** [**not**] **version regex** {*regex_name* | **class** *class_name*} - IM 메시지의 버전을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **filename regex** {*regex_name* | **class** *class_name*} - IM 메시지의 파일 이름을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다. MSN IM 프로토콜에서는 이 일치가 지원되지 않습니다.

d. 클래스 맵 컨피그레이션 모드를 종료하려면 **exit**를 입력합니다.

2단계 IM 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect im policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

3단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

4단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.

- IM 클래스 맵을 만든 경우 다음 명령을 입력하여 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- IM 클래스 맵에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {drop-connection [log]| reset [log] | log}
```

drop-connection 키워드는 패킷을 삭제하고 연결을 닫습니다.

reset 키워드는 패킷을 삭제하고, 연결을 닫고, TCP 재설정을 서버 또는 클라이언트로 전송합니다.

단독으로 또는 기타 키워드와 함께 사용할 수 있는 **log** 키워드는 시스템 로그 메시지를 전송합니다.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다. **class** 및 **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

예

다음 예는 IM 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname4 "darshant\@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\.0"
hostname(config)# regex gif_files ".*\.gif"
hostname(config)# regex exe_files ".*\.exe"

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

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

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

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

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

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

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

IM 검사 서비스 정책 구성

IM 검사는 기본 검사 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. 그러나 기본 검사 클래스에는 기본 IM 포트가 포함되어 있지 않으므로, 기본 글로벌 검사 정책을 편집하여 IM 검사를 추가하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map im_class_map
hostname(config-cmap)# match access-list im
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 IM 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

```
class name
```

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 IM 검사를 구성합니다.

```
inspect im [im_policy_map]
```

여기서 *im_policy_map*은 선택적인 IM 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. IM 검사 정책 맵 생성에 대한 자세한 내용은 8-21 페이지의 IM 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect im
hostname(config-class)# inspect im im-map
```

참고 다른 IM 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect im** 명령을 사용해 IM 검사를 제거한 다음 새 IM 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

```
service-policy policymap_name {global | interface interface_name}
```

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

IP Options 검사

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

다음 섹션에서는 IP Options 검사 엔진에 대해 설명합니다.

- 8-25 페이지의 IP Options 검사 개요
- 8-26 페이지의 IP 옵션 검사를 위한 기본값
- 8-27 페이지의 IP Options 검사 구성
- 8-29 페이지의 IP Options 검사 모니터링

IP Options 검사 개요

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

IP 옵션의 리스트 및 관련 RFC에 대한 참조 사항은 IANA 페이지, http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml을 참조하십시오.

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

옵션을 지울 경우

IP Options 검사 정책 맵을 구성할 때, 각 옵션 유형을 허용할지 아니면 지울지를 지정할 수 있습니다. 옵션 유형을 지정하지 않으면 해당 옵션을 포함한 패킷이 삭제됩니다.

옵션을 허용하면 해당 옵션을 포함한 패킷은 변경되지 않은 채 통과됩니다.

IP 헤더에서 옵션을 지우도록 지정하면 IP 헤더가 다음과 같이 변경됩니다.

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

검사가 지원되는 IP Options

IP Options 검사는 패킷에서 다음 IP 옵션을 검사할 수 있습니다. IP 헤더에 아래 옵션 이외의 옵션이 포함된 경우, 이러한 옵션을 허용하도록 ASA를 구성했는지 여부와 상관없이, ASA는 패킷을 삭제합니다.

- EOOL(End of Options List) 또는 IP Option 0 - 단일 0바이트만을 포함하는 이 옵션은 모든 옵션의 끝에 나타나며 옵션 리스트의 끝을 마스크 처리합니다. 이것은 헤더 길이에 따른 헤더의 끝과 일치하지 않을 수 있습니다.
- NOP(No Operation) 또는 IP Option 1 - IP 헤더의 Options 필드는 0개, 1개 또는 그 이상의 옵션을 포함할 수 있습니다. 그러나 IP 헤더는 32비트의 배수여야 합니다. 모든 옵션의 비트 수가 32비트의 배수가 아니면 32비트 경계에 옵션을 맞추기 위해 NOP 옵션이 "internal padding"으로 사용됩니다.
- RTRALT(Router Alert) 또는 IP Option 20 - 이 옵션은 트랜싯 라우터에 패킷의 내용을 검사하도록 알립니다(패킷의 목적지가 해당 라우터가 아닌 경우에도). 이 검사는 RSVP 및 패킷의 배달 경로에 있는 라우터에서 비교적 복잡한 프로세싱을 수행하도록 요구하는 유사 프로토콜을 구현할 때 매우 유용합니다. Router Alert 옵션이 포함된 RSVP 패킷을 삭제하면 VoIP 구현 시 문제가 발생할 수 있습니다.

IP 옵션 검사를 위한 기본값

IP Options 검사는 _default_ip_options_map 검사 정책 맵을 사용하여 기본적으로 활성화됩니다.

- Router Alert 옵션은 허용됩니다.
- 기타 옵션이 포함된 패킷은 삭제됩니다. 여기에는 지원되지 않는 옵션을 포함하는 패킷이 포함됩니다.

다음은 정책 맵 컨피그레이션입니다.

```
policy-map type inspect ip-options _default_ip_options_map
 description Default IP-OPTIONS policy-map
 parameters
  router-alert action allow
```

IP Options 검사 구성

IP Options 검사는 기본적으로 사용됩니다. 기본 맵에서 허용하는 것보다 더 많은 옵션을 허용하려는 경우에만 구성해야 합니다.

절차

1단계 8-27 페이지의 IP Options 검사 정책 맵 구성.

2단계 8-28 페이지의 IP Options 검사 서비스 정책 구성.

IP Options 검사 정책 맵 구성

기본 IP Options 검사 이외의 검사를 수행하려면 IP Options 검사 정책 맵을 만들고 지원되는 각 옵션 유형의 처리 방법을 지정하십시오.

절차

1단계 IP Options 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect ip-options policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

3단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다. 모든 경우에, **allow** 작업은 옵션이 포함된 패킷을 수정 없이 허용하고 **clear** 작업은 패킷을 허용하되 헤더에서 옵션을 제거합니다. 사용자가 맵에 포함하지 않은 옵션을 포함하고 있는 패킷은 삭제됩니다. 옵션에 대한 자세한 설명은 8-26 페이지의 검사가 지원되는 IP Options를 참조하십시오.

- **eool action** {**allow** | **clear**} - End of Options List 옵션을 허용하거나 지웁니다.
- **nop action** {**allow** | **clear**} - No Operation 옵션을 허용하거나 지웁니다.
- **router-alert action** {**allow** | **clear**} - RTRALT(Router Alert) 옵션을 허용하거나 지웁니다.

IP Options 검사 서비스 정책 구성

기본 ASA 컨피그레이션에는 모든 인터페이스에서 전체적으로 적용되는 IP Options 검사가 포함되어 있습니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map ip_options_class_map
hostname(config-cmap)# match access-list ipoptions
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 IP Options 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 IP Options 검사를 구성합니다.

inspect ip-options [*ip_options_policy_map*]

여기서 *ip_options_policy_map*은 선택적인 IP Options 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. IP Options 검사 정책 맵 생성에 대한 자세한 내용은 8-27 페이지의 IP Options 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect ip-options
hostname(config-class)# inspect ip-options ip-options-map
```

참고 다른 IP Options 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect ip-options** 명령을 사용해 IP Options 검사를 제거한 다음 새 IP Options 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

IP Options 검사 모니터링

IP Options 검사의 결과를 모니터링하려면 다음과 같은 방법을 사용할 수 있습니다.

- 검사 때문에 패킷이 삭제될 때마다 syslog 106012가 생성됩니다. 메시지에는 삭제를 일으킨 옵션이 표시됩니다.
- 각 옵션의 통계를 표시하려면 **show service-policy inspect ip-options** 명령을 사용합니다.

IPsec Pass Through 검사

다음 섹션에서는 IPsec Pass Through 검사 엔진에 대해 설명합니다.

- 8-29 페이지의 IPsec Pass Through 검사 개요
- 8-30 페이지의 IPsec Pass Through 검사 구성

IPsec Pass Through 검사 개요

IPsec(Internet Protocol Security)은 데이터 스트림의 각 IP 패킷을 인증 및 암호화하여 IP 통신을 보호하기 위한 프로토콜 모음입니다. IPsec에는 세션을 시작할 때 에이전트 간 상호 인증을 설정하기 위한 프로토콜 및 세션 중에 사용할 암호화 키의 협상을 위한 프로토콜도 포함됩니다. IPsec은 호스트 쌍(예: 컴퓨터 사용자 또는 서버) 사이, 보안 게이트웨이 쌍(예: 라우터 또는 방화벽) 사이 또는 보안 게이트웨이와 호스트 사이의 데이터 흐름을 보호하는 데 사용할 수 있습니다.

IPsec Pass Through 애플리케이션 검사를 사용하면 IKE UDP 포트 500으로 연결된 ESP(IP 프로토콜 50) 및 AH(IP 프로토콜 51) 트래픽의 통과를 편리하게 관리할 수 있습니다. 이 검사에서는 ESP 및 AH 트래픽 허용을 위해 긴 ACL 컨피그레이션을 피하며, 시간 제한 및 최대 연결 수를 사용하여 보안을 제공합니다.

ESP 또는 AH 트래픽에 대한 제한을 지정하려면 IPsec Pass Through용 정책 맵을 구성하십시오. 클라이언트당 최대 연결 수 및 유휴 시간 제한을 설정할 수 있습니다.

NAT 및 비 NAT 트래픽은 허용되지만, PAT는 지원되지 않습니다.

IPsec Pass Through 검사 구성

IPsec Pass Through 검사는 기본적으로 사용되지 않습니다. IPsec Pass Through 검사를 사용하려면 구성해야 합니다.

절차

1단계 8-30 페이지의 IPsec Pass Through 검사 정책 맵 구성.

2단계 8-31 페이지의 IPsec Pass Through 검사 서비스 정책 구성.

IPsec Pass Through 검사 정책 맵 구성

IPsec Pass Through 맵을 사용하면 IPsec Pass Through 애플리케이션 검사에 사용된 기본 컨피그레이션값을 변경할 수 있습니다. ACL을 사용하지 않은 채 특정 흐름을 허용하려면 IPsec Pass Through 맵을 사용할 수 있습니다.

컨피그레이션에는 클라이언트당 ESP 최대 연결 수의 제한을 설정하지 않으며 ESP 유휴 시간 제한을 10분으로 설정하는 기본 맵인 _default_ipsec_passthru_map이 포함됩니다. 다른 값을 원하는 경우 또는 AH 값을 설정하려는 경우에만 검사 정책 맵을 구성해야 합니다.

절차

1단계 IPsec Pass Through 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect ipsec-pass-thru policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

3단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **esp per-client-max** *number* **timeout** *time* - ESP 터널을 허용하며 클라이언트당 허용되는 최대 연결 수 및 유휴 시간 제한(hh:mm:ss 형식)을 설정합니다. 무제한 연결을 허용하려면 number를 0으로 지정합니다.
- **ah per-client-max** *number* **timeout** *time* - AH 터널을 허용합니다. 매개변수의 의미는 esp 명령과 동일합니다.

예

다음 예는 ACL을 사용하여 IKE 트래픽을 식별하고, IPsec Pass Thru 매개변수 맵을 정의하고, 정책을 정의하고, 외부 인터페이스에 정책을 적용하는 방법을 보여줍니다.

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

IPsec Pass Through 검사 서비스 정책 구성

IPsec Pass Through 검사는 기본 검사 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. 그러나 기본 검사 클래스에는 기본 IPsec 포트가 포함되어 있지 않으므로, 기본 글로벌 검사 정책을 편집하여 IPsec 검사를 추가하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map ipsec_class_map
hostname(config-cmap)# match access-list ipsec
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 IPsec Pass Through 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 IPsec Pass Through 검사를 구성합니다.

```
inspect ipsec-pass-thru [ipsec_policy_map]
```

여기서 *ipsec_policy_map*은 선택적인 IPsec Pass Through 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. 검사 정책 맵 생성에 대한 자세한 내용은 8-30 페이지의 IPsec Pass Through 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect ipsec-pass-thru
hostname(config-class)# inspect ipsec-pass-thru ipsec-map
```

참고 다른 IPsec Pass Through 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect ipsec-pass-thru** 명령을 사용해 IPsec Pass Through 검사를 제거한 다음 새 IPsec Pass Through 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

```
service-policy policymap_name {global | interface interface_name}
```

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

IPv6 검사

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

IPv6 검사를 위한 기본값

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

- 알려진 IPv6 확장 헤더만 허용됩니다. 적합하지 않은 패킷은 삭제되고 기록됩니다.
- IPv6 확장 헤더의 순서가 RFC 2460 사양에 정의된 대로 적용됩니다. 적합하지 않은 패킷은 삭제되고 기록됩니다.

- 라우팅 유형(routing type) 헤더가 포함된 패킷은 삭제됩니다.

다음은 정책 맵 컨피그레이션입니다.

```
policy-map type inspect ipv6 _default_ipv6_map
 description Default IPV6 policy-map
 parameters
  verify-header type
  verify-header order
 match header routing-type range 0 255
  drop log
```

IPv6 검사 구성

IPv6 검사는 기본적으로 사용되지 않습니다. IPv6 검사를 사용하려면 구성해야 합니다.

절차

1단계 8-33 페이지의 IPv6 검사 정책 맵 구성.

2단계 8-35 페이지의 IPv6 검사 서비스 정책 구성.

IPv6 검사 정책 맵 구성

삭제 또는 기록할 확장 헤더를 식별하거나 패킷 확인을 비활성화하려면 서비스 정책에서 사용할 IPv6 검사 정책 맵을 만드십시오.

절차

1단계 IPv6 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect ipv6 policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가합니다.

```
hostname(config-pmap)# description string
```

3단계 (선택 사항) IPv6 메시지의 헤더를 기반으로 트래픽을 삭제 또는 기록합니다.

a. IPv6 헤더를 기반으로 트래픽을 식별합니다.

```
hostname(config-pmap)# match header type
```

여기서 type은 다음 중 하나입니다.

- **ah** - IPv6 Authentication 확장 헤더를 확인합니다.
- **count gt** *number* - IPv6 확장 헤더의 최대 수를 지정합니다(0~255).
- **destination-option** - IPv6 destination-option 확장 헤더를 확인합니다.
- **esp** - IPv6 ESP(Encapsulation Security Payload) 확장 헤더를 확인합니다.

- **fragment** - IPv6 fragment 확장 헤더를 확인합니다.
- **hop-by-hop** - IPv6 hop-by-hop 확장 헤더를 확인합니다.
- **routing-address count gt** *number* - IPv6 라우팅 헤더 유형 0 주소의 최대 수를 지정합니다(0~255).
- **routing-type** {**eq** | **range**} *number* - IPv6 라우팅 헤더 유형을 확인합니다(0~255). 범위를 지정할 경우 공백으로 구분합니다(예: **30 40**).

b. 일치하는 패킷에 대해 수행할 작업을 지정합니다. 패킷을 삭제하고 선택적으로 기록하거나, 기록만 할 수도 있습니다. 작업을 입력하지 않으면 패킷이 기록됩니다.

```
hostname(config-pmap)# {drop [log] | log}
```

c. 삭제 또는 기록할 모든 헤더를 확인할 때까지 이 과정을 반복합니다.

4단계 검사 엔진에 영향을 미치는 매개변수를 구성합니다.

a. 매개변수 컨피그레이션 모드로 들어갑니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **verify-header type** - 알려진 IPv6 확장 헤더를 허용합니다.
- **verify-header order** - IPv6 확장 헤더의 순서를 RFC 2460에 정의된 대로 적용합니다.

예

다음 예는 hop-by-hop, destination-option, routing-address 및 routing type 0 헤더의 모든 IPv6 패킷을 삭제하고 기록할 검사 정책 맵을 만듭니다. 또한 헤더 순서와 유형을 적용합니다.

```
policy-map type inspect ipv6 ipv6-pm
 parameters
  verify-header type
  verify-header order
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
 match header routing-type eq 0
  drop log

policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

IPv6 검사 서비스 정책 구성

IPv6 검사는 기본 검사 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. IPv6 검사를 추가하려면 기본 글로벌 검사 정책을 편집하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map ipv6_class_map
hostname(config-cmap)# match access-list ipv6
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 IPv6 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 IPv6 검사를 구성합니다.

inspect ipv6 [*ipv6_policy_map*]

여기서 *ipv6_policy_map*은 선택적인 IPv6 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. 검사 정책 맵 생성에 대한 자세한 내용은 8-33 페이지의 IPv6 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect ipv6
hostname(config-class)# inspect ipv6 ipv6-map
```

참고 다른 IPv6 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect ipv6** 명령을 사용해 IPv6 검사를 제거한 다음 새 IPv6 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

```
service-policy policymap_name {global | interface interface_name}
```

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

NetBIOS 검사

NetBIOS 검사는 기본적으로 사용됩니다. NetBIOS 검사 엔진은 ASA NAT 컨피그레이션에 따라 NBNS(NetBIOS Name Service) 패킷에서 IP 주소를 변환합니다. NetBIOS 프로토콜 위반 시 삭제 또는 기록하기 위한 정책 맵을 선택적으로 만들 수 있습니다.

절차

1단계 8-36 페이지의 추가 검사 제어를 위한 NetBIOS 검사 정책 맵 구성.

2단계 8-37 페이지의 NetBIOS 검사 서비스 정책 구성.

추가 검사 제어를 위한 NetBIOS 검사 정책 맵 구성

프로토콜 위반 시 수행할 작업을 지정하려면 NETBIOS 검사 정책 맵을 만드십시오. 그러면 NETBIOS 검사를 사용할 때 검사 정책 맵을 적용할 수 있습니다.

절차

1단계 NetBIOS 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect netbios policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

3단계 매개변수 컨피그레이션 모드로 들어갑니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

4단계 NETBIOS 프로토콜 위반 시 수행할 작업을 지정합니다.

```
hostname(config-pmap-p)# protocol-violation action {drop [log] | log}
```

여기서 **drop** 작업은 패킷을 삭제합니다. 이 정책 맵이 트래픽과 일치할 경우 **log** 작업은 시스템 로그 메시지를 전송합니다.

예

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

hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect netbios netbios_map
```

NetBIOS 검사 서비스 정책 구성

NetBIOS 애플리케이션 검사는 NetBIOS 이름 서비스 패킷 및 NetBIOS 데이터그램 서비스 패킷에 포함된 IP 주소에 대해 NAT를 수행합니다. 또한 프로토콜 적합성을 적용하여 다양한 개수 및 길이 필드에서 일관성을 확인합니다.

기본 ASA 컨피그레이션에는 모든 인터페이스에 전체적으로 적용되는 기본 포트에 대한 NetBIOS 검사가 포함됩니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map netbios_class_map
hostname(config-cmap)# match access-list netbios
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 NetBIOS 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 NetBIOS 검사를 구성합니다.

inspect netbios [*netbios_policy_map*]

여기서 *netbios_policy_map*은 선택적인 NetBIOS 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. NetBIOS 검사 정책 맵 생성에 대한 자세한 내용은 8-36 페이지의 추가 검사 제어를 위한 NetBIOS 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect netbios
hostname(config-class)# inspect netbios netbios-map
```

참고 다른 NetBIOS 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect skinny** 명령을 사용해 NetBIOS 검사를 제거한 다음 새 NetBIOS 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

PPTP 검사

PPTP 터널링 PPP 트래픽용 프로토콜입니다. PPTP 세션은 TCP 채널 1개 및 대개 PPTP GRE 터널 2개로 구성됩니다. TCP 채널은 PPTP GRE 터널의 협상 및 관리에 사용되는 제어 채널입니다. GRE 터널은 두 호스트 간 PPP 세션을 연결합니다.

활성화 시 PPTP 애플리케이션 검사는 PPTP 프로토콜 패킷을 검사하고, PPTP 트래픽 허용에 필요한 GRE 연결 및 xlate를 동적으로 만듭니다.

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

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

PPTP 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

SMTP 및 Extended SMTP 검사

ESMTP 검사는 스팸, 피싱, 형식이 잘못된 메시지 공격, 버퍼 오버플로/언더플로 공격 등의 공격을 감지합니다. 또한 애플리케이션 보안 및 프로토콜 적합성에 대한 지원을 제공하여 ESMTP 메시지의 온전성을 적용하는 것은 물론 여러 공격을 감지하고, 발신자/수신자를 차단하고, 메일 릴레이를 차단합니다.

다음 섹션에서는 ESMTP 검사 엔진에 대해 설명합니다.

SMTP 및 ESMTP 검사 개요

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

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

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

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

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

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

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

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

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

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

ESMTP 검사를 위한 기본값

ESMTP 검사는 _default_esmtp_map 검사 정책 맵을 사용하여 기본적으로 활성화됩니다.

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

다음은 정책 맵 컨피그레이션입니다.

```
policy-map type inspect esmtp _default_esmtp_map
 description Default ESMTP policy-map
 parameters
  mask-banner
  no mail-relay
  no special-character
  no allow-tls
 match cmd line length gt 512
  drop-connection log
 match cmd RCPT count gt 100
  drop-connection log
 match body line length gt 998
  log
```

```
match header line length gt 998
 drop-connection log
match sender-address length gt 320
 drop-connection log
match MIME filename length gt 255
 drop-connection log
match ehlo-reply-parameter others
 mask
```

ESMTP 검사 구성

ESMTP 검사는 기본적으로 사용됩니다. 기본 검사 맵에서 제공하는 것과 다른 프로세스를 원하는 경우에만 구성해야 합니다.

절차

1단계 8-41 페이지의 ESMTP 검사 정책 맵 구성.

2단계 8-43 페이지의 ESMTP 검사 서비스 정책 구성.

ESMTP 검사 정책 맵 구성

메시지가 매개변수를 위반하는 경우의 작업을 지정하려면 ESMTP 검사 정책 맵을 만듭니다. 그러면 ESMTP 검사를 사용할 때 검사 정책 맵을 적용할 수 있습니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 ESMTP 검사 정책 맵을 만들고 다음 명령을 입력합니다.

```
hostname(config)# policy-map type inspect esmtp policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

3단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **body** {**length** | **line length**} **gt** *bytes* - ESMTP 본문 메시지의 길이 또는 줄 길이가 지정된 바이트 수보다 큰 경우 메시지를 확인합니다.
- **match** [**not**] **cmd verb** *verb1* [*verb2...*] - 메시지의 명령 동사를 확인합니다. 명령 auth, data, ehlo, etrn, helo, help, mail, noop, quit, rcpt, rset, saml, soml, vrfy 중 하나 이상을 지정할 수 있습니다.

- **match** [**not**] **cmd line length gt** *bytes* - 명령 동사의 줄 길이가 지정된 바이트 수보다 큰 경우 메시지를 확인합니다.
- **match** [**not**] **cmd rcpt count gt** *count* - 수신자의 숫자가 지정된 수보다 큰 경우 메시지를 확인합니다.
- **match** [**not**] **ehlo-reply-parameter** *parameter* [*parameter2...*] - ESMTP EHLO 회신 매개변수를 확인합니다. 매개변수 8bitmime, auth, binaryname, checkpoint, dsn, etrn, others, pipelining, size, vrfy 중 하나 이상을 지정할 수 있습니다.
- **match** [**not**] **header** {**length** | **line length**} **gt** *bytes* - ESMTP 헤더의 길이 또는 줄 길이가 지정된 바이트 수보다 큰 경우 메시지를 확인합니다.
- **match** [**not**] **header to-fields count gt** *count* - 헤더에 있는 To 필드의 숫자가 지정된 수보다 큰 경우 메시지를 확인합니다.
- **match** [**not**] **invalid-recipients count gt** *number* - 잘못된 수신자의 숫자가 지정된 수보다 큰 경우 메시지를 확인합니다.
- **match** [**not**] **mime filetype regex** {*regex_name* | **class** *class_name*} - MIME 또는 미디어 파일 형식을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **mime filename length gt** *bytes* - 파일 이름이 지정된 바이트 수보다 긴 경우 메시지를 확인합니다.
- **match** [**not**] **mime encoding** *type* [*type2...*] - MIME 인코딩 유형을 확인합니다. 유형 7bit, 8bit, base64, binary, others, quoted-printable 중 하나 이상을 지정할 수 있습니다.
- **match** [**not**] **sender-address regex** {*regex_name* | **class** *class_name*} - 발신자 이메일 주소를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **sender-address length gt** *bytes* - 발신자 주소가 지정된 바이트 수보다 큰 경우 메시지를 확인합니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {drop-connection [log] | mask [log] | reset [log] | log |
rate-limit message_rate}
```

각 **match** 명령에서 모든 옵션을 사용할 수 있는 것은 아닙니다. 사용 가능한 정확한 옵션은 CLI 도움말 또는 명령 참조에서 확인할 수 있습니다.

- **drop-connection** 키워드는 패킷을 삭제하고 연결을 닫습니다.
- **mask** 키워드는 패킷에서 일치하는 부분을 마스크 처리합니다. 이 작업은 **ehlo-reply-parameter** 및 **cmd verb**에만 이용할 수 있습니다.
- **reset** 키워드는 패킷을 삭제하고, 연결을 닫고, TCP 재설정을 서버 및/또는 클라이언트로 전송합니다.
- 단독으로 또는 기타 키워드와 함께 사용할 수 있는 **log** 키워드는 시스템 로그 메시지를 전송합니다.
- **rate-limit** *message_rate* 인수는 메시지의 속도를 제한합니다. 이 옵션은 **cmd verb**에만 이용할 수 있습니다. 이것을 유일한 작업으로 사용할 수도 있고 **mask** 작업과 함께 사용할 수도 있습니다.

정책 맵에서 여러 **match** 명령을 지정할 수 있습니다. **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

4단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **mail-relay** *domain-name* **action** {**drop-connection** [**log**] | **log**} - 메일 릴레이의 도메인 이름을 식별합니다. 연결을 삭제하고 선택적으로 기록할 수도 있고, 기록만 할 수도 있습니다.
- **mask-banner** - ESMTP 서버의 배너를 마스크 처리합니다.
- **special-character action** {**drop-connection** [**log**] | **log**} - 발신자 또는 수신자 이메일 주소에 파이프(|), 역따옴표, NUL 등의 특수 문자가 포함된 메시지에 대해 수행할 작업을 식별합니다. 연결을 삭제하고 선택적으로 기록할 수도 있고, 기록만 할 수도 있습니다.
- **allow-tls** [**action log**] - 검사 없이 ESMTP over TLS(암호화된 연결)를 허용할지 여부를 설정합니다. 암호화된 연결을 선택적으로 기록할 수 있습니다.

예

다음 예는 ESMTP 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
hostname(config)# regex user1 "user1@cisco.com"
hostname(config)# regex user2 "user2@cisco.com"
hostname(config)# regex user3 "user3@cisco.com"
hostname (config) # class-map type Regex senders_black_list
hostname(config-cmap)# description "Regular expressions to filter out undesired senders"
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map

hostname(config)# service-policy outside_policy interface outside
```

ESMTP 검사 서비스 정책 구성

기본 ASA 컨피그레이션에는 모든 인터페이스에서 전체적으로 적용되는 ESMTP 검사가 포함되어 있습니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map esmtp_class_map
hostname(config-cmap)# match access-list esmtp
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 IP Options 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 ESMTP 검사를 구성합니다.

inspect esmtp [*esmtp_policy_map*]

여기서 *esmtp_policy_map*은 선택적인 ESMTP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. ESMTP 검사 정책 맵 생성에 대한 자세한 내용은 8-43 페이지의 ESMTP 검사 서비스 정책 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect esmtp
hostname(config-class)# inspect esmtp esmtp-map
```

참고 다른 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect esmtp** 명령을 사용해 ESMTP 검사를 제거한 다음 새 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

TFTP 검사

TFTP 검사는 기본적으로 사용됩니다.

RFC 1350에 기술되어 있는 TFTP는 TFTP 서버와 클라이언트 간에 파일을 읽고 쓰기 위한 간단한 프로토콜입니다.

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

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

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

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

TFTP 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

9 장

음성 및 비디오 프로토콜에 대한 검사

다음 항목에서는 음성 및 비디오 프로토콜에 대한 애플리케이션 검사에 대해 설명합니다. 특정 프로토콜에 대해 검사를 사용해야 하는 이유 및 검사 적용을 위한 전반적인 방법에 대해 알아보려면 7-1 페이지의 애플리케이션 계층 프로토콜 검사 시작을 참조하십시오.

CTIQBE 검사

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

TAPI 및 JTAPI는 여러 Cisco VoIP 애플리케이션에서 사용됩니다. Cisco TSP는 Cisco CallManager와 통신하기 위해 CTIQBE를 사용합니다.

CTIQBE 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

CTIQBE 검사의 제한

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

- CTIQBE 애플리케이션 검사는 **alias** 명령을 이용한 컨피그레이션을 지원하지 않습니다.
- CTIQBE 통화의 상태 저장 장애 조치는 지원되지 않습니다.

- **debug ctiqbe** command를 입력하면 메시지 전송이 지연될 수 있으며, 이는 실시간 환경에 성능 영향을 미칠 수 있습니다. 이 디버깅 또는 기록을 활성화한 경우 Cisco IP SoftPhone에서 ASA를 통해 통화 설정을 완료하지 못할 것 같으면 Cisco IP SoftPhone을 실행하는 시스템의 Cisco TSP 설정에서 시간 제한 값을 늘리십시오.

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

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

CTIQBE 검사 확인 및 모니터링

show ctiqbe 명령은 ASA 전체에 설정된 CTIQBE 세션에 대한 정보를 표시합니다. 이는 CTIQBE 검사 엔진에 의해 할당된 미디어 연결에 대한 정보입니다.

다음은 **show ctiqbe** 명령의 샘플 출력입니다(다음과 같은 조건에서 사용). ASA 전체에 활성 CTIQBE 세션이 하나만 설정되어 있습니다. 로컬 주소 10.0.0.99의 내부 CTI 디바이스(예: Cisco IP SoftPhone)와 외부 Cisco CallManager at 172.29.1.77 간에 설정됩니다. 여기서 TCP 포트 2748은 Cisco CallManager입니다. 세션에 대한 하트비트 간격은 120초입니다.

```
hostname# # show ctiqbe

Total: 1
        LOCAL            FOREIGN          STATE   HEARTBEAT
-----------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ------------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        ------------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        ------------------------------------------------
```

CTI 디바이스는 CallManager로 이미 등록되었습니다. 디바이스 내부 주소 및 RTP 수신 대기 포트는 172.29.1.99 UDP 포트 1028에서 PAT 처리됩니다. RTCP 수신 대기 포트는 UDP 1029로 PAT 처리됩니다.

내부 CTI 디바이스가 외부 CallManager로 등록되었고 CTI 디바이스 주소와 포트가 해당 외부 인터페이스로 PAT 처리되는 경우에만 `RTP/RTCP: PAT xlates:`로 시작되는 줄이 나타납니다. CallManager가 내부 인터페이스에 있거나 내부 CTI 디바이스 주소와 포트가 CallManager에서 사용하는 것과 동일한 외부 인터페이스로 변환되는 경우에는 이 줄이 나타나지 않습니다.

위 출력에서는 172.29.1.88에서 이 CTI 디바이스와 다른 전화기 사이에 통화가 설정되었음을 나타냅니다. 다른 전화기의 RTP 및 RTCP 수신 대기 포트는 UDP 26822 및 26823입니다. ASA에서 두 번째 전화기 및 CallManager와 연결된 CTIQBE 세션 레코드를 유지 관리하지 않으므로 다른 전화기는 CallManager와 동일한 인터페이스에 있는 것입니다. CTI 디바이스의 활성 통화 구간은 Device ID 27 및 Call ID 0으로 식별할 수 있습니다.

다음은 이러한 CTIBQE 연결에 대한 **show xlate debug** 명령의 샘플 출력입니다.

```
hostname# show xlate debug
3 in use, 3 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

show conn state ctiqbe 명령은 CTIQBE 연결의 상태를 표시합니다. 출력에서 CTIQBE 검사 엔진에 의해 할당된 미디어 연결은 'C' 플래그로 표시됩니다. 다음은 **show conn state ctiqbe** 명령의 샘플 출력입니다.

```
hostname# show conn state ctiqbe
1 in use, 10 most used
hostname# show conn state ctiqbe detail
1 in use, 10 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, k - Skinny media,
       M - SMTP data, m - SIP media, O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
```

H.323 검사

다음 섹션에서는 H.323 애플리케이션 검사에 대해 설명합니다.

H.323 검사 개요

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

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

H.323 검사의 중요한 두 가지 기능은 다음과 같습니다.

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

H.323 작동 방식

H.323 프로토콜 모음은 모두 합하여 최대 2개의 TCP 연결 및 4~8개의 UDP 연결을 사용할 수 있습니다. FastConnect는 TCP 연결을 하나만 사용하고, RAS는 등록, 허가 및 상태에 단일 UDP 연결을 사용합니다.

초기에 H.323 클라이언트는 Q.931 통화 설정을 요청하기 위해 TCP 포트 1720을 사용하여 H.323 서버에 대해 TCP 연결을 설정할 수 있습니다. 통화 설정 과정 중에 H.323 터미널은 H.245 TCP 연결에 사용할 수 있도록 클라이언트에 포트 번호를 제공합니다. H.323 게이트키퍼가 사용 중인 환경에서는 초기 패킷이 UDP를 사용하여 전송됩니다.

H.323 검사는 Q.931 TCP 연결을 모니터링하여 H.245 포트 번호를 확인합니다. H.323 터미널이 FastConnect를 사용하지 않으면 ASA는 H.225 메시지의 검사를 기반으로 H.245 연결을 동적으로 할당합니다.

참고 RAS를 사용할 경우 H.225 연결도 동적으로 할당됩니다.

각 H.245 메시지에서 H.323 엔드포인트는 후속 UDP 데이터 스트림에 사용할 포트 번호를 교환합니다. H.323 검사는 H.245 메시지를 검사하여 이러한 포트를 식별하고 미디어 교환을 위한 연결을 동적으로 생성합니다. RTP는 협상된 포트 번호를 사용하는 반면 RTCP는 그다음으로 높은 포트 번호를 사용합니다.

H.323 제어 채널은 H.225, H.245 및 H.323 RAS를 처리합니다. H.323 검사는 다음과 같은 포트를 사용합니다.

- 1718 - Gate Keeper Discovery UDP 포트
- 1719 - RAS UDP 포트
- 1720 - TCP 제어 포트

잘 알려진 RAS 신호용 H.323 포트 1719에 대한 트래픽을 허용해야 합니다. 또한 잘 알려진 H.225 통화 신호용 H.323 포트 1720에 대한 트래픽도 허용해야 합니다. 그러나 H.245 신호 포트는 H.225 신호에서 엔드포인트 간에 협상됩니다. H.323 게이트키퍼가 사용되는 경우 ASA는 ACF 및 RCF 메시지 검사를 기반으로 H.225 연결을 엽니다.

H.225 메시지 검사 후 ASA는 H.245 채널을 연 다음, H.245 채널을 통해 전송된 트래픽도 검사합니다. ASA를 통과하는 모든 H.245 메시지는 H.245 애플리케이션 검사를 거칩니다. 이 과정에서 포함된 IP 주소가 변환되고 H.245 메시지에서 협상된 미디어 채널이 열립니다.

H.323 ITU 표준에서는, 신뢰할 수 있는 연결로 전달되기 전에 메시지 길이를 정의하는 TPKT 헤더가 H.225 및 H.245보다 먼저 와야 합니다. TPKT 헤더를 H.225 및 H.245 메시지와 동일한 TCP 패킷에서 전송해야 할 필요는 없으므로 ASA에서는 메시지를 올바르게 처리하고 디코딩하기 위해 TPKT 길이를 기억해야 합니다. 각 연결에서 ASA는 다음 예상 메시지에 대한 TPKT 길이를 포함하는 레코드를 유지합니다.

메시지의 IP 주소에 대해 NAT를 수행해야 하는 경우 ASA는 체크섬, UUIE 길이 및 TPKT(H.225 메시지와 함께 TCP 패킷에 포함된 경우)를 변경합니다. TPKT가 별도의 TCP 패킷에서 전송되는 경우 ASA는 해당 TPKT를 프록시 ACK 처리하고 새 TPKT를 새 길이로 H.245 메시지에 추가합니다.

참고 ASA는 TPKT용 프록시 ACK에서 TCP 옵션을 지원하지 않습니다.

H.323 검사를 통과하는 패킷과의 각 UDP 연결은 H.323 연결로 표시되며, **timeout** 명령으로 구성한 H.323 시간 제한의 적용을 받습니다.

참고 게이트키퍼가 네트워크 내부에 있는 경우 H.323 엔드포인트 간의 통화 설정을 활성화할 수 있습니다. ASA에는 RRQ/RCF(RegistrationRequest/RegistrationConfirm) 메시지를 기반으로 통화에 대한 핀홀을 열기 위한 옵션이 포함되어 있습니다. 이러한 RRQ/RCF 메시지는 게이트키퍼에서 보내고 받으므로, 통화 엔드포인트의 IP 주소는 알 수 없으며 ASA에서는 소스 IP 주소/포트 0/0을 통해 핀홀을 엽니다. 기본적으로 이 옵션은 사용되지 않습니다. H.323 엔드포인트 간 통화 설정을 활성화하려면 매개변수 컨피그레이션 모드에서 H.323 검사 정책 맵을 만드는 동안 **ras-rcf-pinholes enable** 명령을 입력합니다. 9-6 페이지의 H.323 검사 정책 맵 구성 섹션을 참조하십시오.

H.245 메시지에서 H.239 지원

ASA는 두 개의 H.323 엔드포인트 사이에 있습니다. 두 개의 H.323 엔드포인트가 데이터 프레젠테이션(예: 스프레드시트 데이터)을 주고받을 수 있도록 텔레프레젠테이션 세션을 설정하면 ASA는 엔드포인트 간 H.239 협상이 성공적으로 이루어지도록 지원합니다.

H.239는 H.300 시리즈 엔드포인트가 신호 통화에서 추가 비디오 채널을 열 수 있는 기능을 제공하는 표준입니다. 통화에서 엔드포인트(예: 비디오 폰)는 비디오용 채널 및 데이터 프레젠테이션용 채널을 전송합니다. H.239 협상은 H.245 채널에서 발생합니다.

ASA는 추가 미디어 채널 및 미디어 제어 채널을 위한 핀홀을 엽니다. 엔드포인트는 OLC(Open Logical Channel) 메시지를 사용하여 새 채널 생성 신호를 보냅니다. 메시지 확장은 H.245 버전 13의 일부입니다.

텔레프레젠테이션의 디코딩 및 인코딩 세션은 기본적으로 사용됩니다. H.239 인코딩 및 디코딩은 ASN.1 코더에서 수행됩니다.

H.323 검사의 제한

H.323 검사는 CUCM(Cisco Unified Communications Manager) 7.0에서 테스트 및 지원됩니다. CUCM 8.0 이상에서는 지원되지 않습니다. 기타 릴리스 및 제품에서는 H.323 검사가 작동하지 않을 수 있습니다.

다음은 H.323 애플리케이션 검사 사용과 관련된 몇 가지 알려진 문제 및 제한 사항입니다.

- 고정 NAT만 완전히 지원됩니다. 고정 PAT는 H.323 메시지 내의 선택적 필드에 포함된 IP 주소를 제대로 변환하지 못할 수 있습니다. 이러한 종류의 문제가 발생하면 H.323에서 고정 PAT를 사용하지 마십시오.
- 동적 NAT 또는 PAT는 지원되지 않습니다.
- 확장 PAT는 지원되지 않습니다.
- 동일한 보안 수준 인터페이스 간 NAT는 지원되지 않습니다.
- 외부 NAT는 지원되지 않습니다.
- NAT64는 지원되지 않습니다.

- H.323 게이트키퍼로 등록된 NetMeeting 클라이언트가 역시 H.323 게이트키퍼로 등록된 H.323 게이트웨이로 통화를 시도하면 연결이 설정되지만 어떤 방향으로도 음성이 들리지 않습니다. 이 문제는 ASA와 관련이 없습니다.
- 네트워크 고정 주소가 타사 넷마스크 및 주소와 동일한 경우 네트워크 고정 주소를 구성하면 아웃바운드 H.323 연결이 실패합니다.

H.323 검사 구성

H.323 검사는 RAS, H.225 및 H.245를 지원하며, 포함된 모든 IP 주소 및 포트를 변환하는 기능을 제공합니다. 또한 정적 추적과 필터링을 수행하며 연속적인 검사 기능 활성화를 수행할 수 있습니다. H.323 검사는 전화번호 필터링, 동적 T.120 제어, H.245 터널링 제어, HSI 그룹, 프로토콜 상태 추적, H.323 통화 기간 적용, 오디오/비디오 제어를 지원합니다.

H.323 검사는 기본적으로 사용됩니다. 기본 이외의 프로세싱을 원하는 경우에만 구성해야 합니다. H.323 검사를 사용자 지정하려면 다음 프로세스를 사용합니다.

절차

1단계 9-6 페이지의 H.323 검사 정책 맵 구성

2단계 9-9 페이지의 Configure the H.323 Inspection Service Policy

H.323 검사 정책 맵 구성

네트워크에서 기본 검사 동작만으로 충분하지 않은 경우 H.323 검사 정책 맵을 만들어 H.323 검사 작업을 사용자 지정할 수 있습니다.

트래픽 매칭 기준을 정의할 때 클래스 맵을 만들 수도 있고, 정책 맵에 일치 명령문을 직접 포함할 수도 있습니다. 다음 절차에서는 두 가지 방법을 모두 설명합니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 (선택 사항) 다음 단계를 수행하여 H.323 검사 클래스 맵을 만듭니다.

클래스 맵은 여러 트래픽 일치를 그룹화합니다. 대신 정책 맵에서 **match** 명령을 직접 지정할 수도 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.

클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다.

이 클래스 맵에서 식별하는 트래픽에 대해 수행할 작업을 검사 정책 맵에서 지정할 수 있습니다.

각 **match** 명령에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

a. 다음 명령을 입력하여 클래스 맵을 만듭니다.

```
hostname(config)# class-map type inspect h323 [match-all | match-any] class_map_name
hostname(config-cmap)#
```

여기서 *class_map_name*은 클래스 맵의 이름입니다. **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. **match-any** 키워드는 트래픽이 하나 이상의 기준과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

b. (선택 사항) 클래스 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-cmap)# description string
```

여기서 *string*은 클래스 맵에 대한 설명입니다(최대 200자).

c. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} - 수신자를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} - 발신자를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **media-type** {**audio** | **data** | **video**} - 미디어 유형을 확인합니다.

2단계 H.323 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect h323 policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

3단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

4단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다. **class** 및 **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

a. 다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.

- H.323 클래스 맵을 만든 경우 다음 명령을 입력하여 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- H.323 클래스 맵에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {drop [log] | drop-connection | reset}
```

drop 키워드는 패킷을 삭제합니다. 미디어 유형 확인을 위해 **log** 키워드를 포함하여 시스템 로그 메시지를 전송할 수 있습니다.

drop-connection 키워드는 패킷을 삭제하고 연결을 닫습니다. 이 옵션은 수신자 또는 발신자 확인에 사용할 수 있습니다.

reset 키워드는 패킷을 삭제하고, 연결을 닫고, TCP 재설정을 서버 및/또는 클라이언트로 전송합니다. 이 옵션은 수신자 또는 발신자 확인에 사용할 수 있습니다.

5단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **ras-rcf-pinholes enable** - H.323 엔드포인트 간 통화 설정을 활성화합니다. 게이트키퍼가 네트워크 내부에 있는 경우 H.323 엔드포인트 간의 통화 설정을 활성화할 수 있습니다. RRQ/RCF(RegistrationRequest/RegistrationConfirm) 메시지를 기반으로 통화에 대한 핀홀을 열려면 이 옵션을 사용합니다. 이러한 RRQ/RCF 메시지는 게이트키퍼에서 보내고 받으므로, 통화 엔드포인트의 IP 주소는 알 수 없으며 ASA에서는 소스 IP 주소/포트 0/0을 통해 핀홀을 엽니다. 기본적으로 이 옵션은 사용되지 않습니다.
- **timeout users** *time* - 통화 기간 제한을 설정합니다(hh:mm:ss 형식). 시간 제한을 없애려면 숫자에 00:00:00을 지정합니다. 범위는 0:0:0~1193:0:0입니다.
- **call-party-number** - 통화 설정 중에 통화자 번호 전송을 적용합니다.
- **h245-tunnel-block action {drop-connection | log}** - H.245 터널 차단을 적용합니다. 연결을 삭제할지 단순히 기록할지를 지정합니다.
- **rtp-conformance [enforce-payloadtype]** - 핀홀에서 흐르는 RTP 패킷에 대해 프로토콜 적합성을 확인합니다. 선택적인 **enforce-payloadtype** 키워드는 신호 교환을 기반으로 오디오 또는 비디오에 페이로드 유형을 적용합니다.
- **state-checking {h225 | ras}** - 상태 확인 검증을 활성화합니다. 상태 확인 활성화를 위한 명령을 H.225 및 RAS에 대해 별도로 입력할 수 있습니다.

6단계 아직 매개변수 컨피그레이션 모드에 있을 때 원하는 경우 HSI 그룹을 구성할 수 있습니다.

a. HSI 그룹을 정의하고 HSI 그룹 컨피그레이션 모드로 들어갑니다.

```
hostname(config-pmap-p)# hsi-group id
```

여기서 *id*는 HSI 그룹 ID입니다. 범위는 0~2147483647입니다.

b. IP 주소를 사용하여 HSI를 HSI 그룹에 추가합니다. HSI 그룹당 최대 5개의 호스트를 추가할 수 있습니다.

```
hostname(config-h225-map-hsi-grp)# hsi ip_address
```

c. HSI 그룹에 엔드포인트를 추가합니다.

```
hostname(config-h225-map-hsi-grp)# endpoint ip_address if_name
```

여기서 *ip_address*는 추가할 엔드포인트이며 *if_name*은 엔드포인트를 ASA에 연결할 인터페이스입니다. HSI 그룹당 최대 10개의 엔드포인트를 추가할 수 있습니다.

예

다음 예는 전화번호 필터링 구성 방법을 보여줍니다.

```
hostname(config)# regex caller 1 "5551234567"
hostname(config)# regex caller 2 "5552345678"
hostname(config)# regex caller 3 "5553456789"
```

```
hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

Configure the H.323 Inspection Service Policy

기본 ASA 컨피그레이션에는 모든 인터페이스에 전체적으로 적용되는 기본 포트에 대한 H.323 H.255 및 RAS 검사가 포함됩니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map h323_class_map
hostname(config-cmap)# match access-list h323
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 H.323 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 H.323 검사를 구성합니다.

inspect h323 {**h255** | **ras**} [*h323_policy_map*]

여기서 *h323_policy_map*은 선택적인 H.323 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. H.323 검사 정책 맵 생성에 대한 자세한 내용은 9-6 페이지의 H.323 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect h323 h225
hostname(config-class)# no inspect h323 ras
hostname(config-class)# inspect h255 h323-map
hostname(config-class)# inspect ras h323-map
```

참고 다른 H.323 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect h323** 명령을 사용해 H.323 검사를 제거한 다음 새 H.323 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

H.323 및 H.225 시간 제한 값 구성

Configuration > Firewall > Advanced > Global Timeouts 페이지에서 H.323/H.255 글로벌 시간 제한 값을 구성할 수 있습니다. H.255 신호 연결이 닫히기까지의 비활성 간격(기본값 1시간) 또는 H.323 제어 연결이 닫히기까지의 비활성 간격(기본값 5분)을 설정할 수 있습니다.

H.225 신호 연결이 닫히기까지의 유휴 시간을 구성하려면 **timeout h225** 명령을 사용하십시오. H.225 시간 제한의 기본값은 1시간입니다.

H.323 제어 연결이 닫히기까지의 유휴 시간을 구성하려면 **timeout h323** 명령을 사용하십시오. 기본값은 5분입니다.

H.323 검사 확인 및 모니터링

다음 섹션에서는 H.323 세션에 대한 정보를 표시하는 방법에 대해 설명합니다.

- 9-11 페이지의 H.225 세션 모니터링
- 9-11 페이지의 H.245 세션 모니터링
- 9-12 페이지의 H.323 RAS 세션 모니터링

H.225 세션 모니터링

show h225 명령은 ASA 전반에 걸쳐 설정된 H.225 세션에 대한 정보를 표시합니다. **debug h323 h225 event**, **debug h323 h245 event** 및 **show local-host** 명령과 함께 이 명령은 H.323 검사 엔진의 문제를 해결하는 데 사용됩니다.

연결 수가 비정상적으로 많은 경우 세션의 시간 제한이 기본 시간 제한 값 또는 자신이 설정한 값을 기반으로 적용되고 있는지 확인하십시오. 그렇지 않은 경우 조사해야 할 문제가 있는 것입니다.

다음은 **show h225** 명령의 샘플 출력입니다.

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

위 출력은 로컬 엔드포인트 10.130.56.3과 외부 호스트 172.30.254.203 사이에서 ASA를 통과하는 활성 H.323 통화가 1개 있고, 이러한 특별한 엔드포인트 간에 동시 통화가 1개 있으며 해당 통화의 CRV는 9861임을 나타냅니다.

로컬 엔드포인트 10.130.56.4와 외부 호스트 172.30.254.205에는 동시 통화가 0개 있습니다. 이는 H.225 세션이 아직 존재하더라도 두 엔드포인트 간에 활성 통화가 없음을 나타냅니다. **show h225** 명령을 사용한 시점에 통화가 이미 종료됐지만 H.225 세션이 아직 삭제되지 않은 경우 이러한 현상이 발생할 수 있습니다. 또는 "maintainConnection"이 TRUE로 설정되어 두 엔드포인트 간에 아직 TCP 연결이 열려 있음을 의미할 수 있습니다. "maintainConnection"을 다시 FALSE로 설정할 때까지 또는 컨피그레이션의 H.225 시간 제한 값을 기반으로 세션의 시간이 초과될 때까지 세션이 계속 열려 있게 됩니다.

H.245 세션 모니터링

show h245 명령은 ASA 전반에 걸쳐 느린 시작을 사용하여 엔드포인트에 의해 설정된 H.245 세션에 대한 정보를 표시합니다. 느린 시작은 통화의 두 엔드포인트가 H.245에 대해 또 다른 TCP 제어 채널을 열 때 발생합니다. 빠른 시작은 H.225 제어 채널에서 H.245 메시지가 H.225 메시지의 일부로서 교환될 때 발생합니다.

다음은 **show h245** 명령의 샘플 출력입니다.

```
hostname# show h245
Total: 1
        LOCAL            TPKT    FOREIGN          TPKT
1       10.130.56.3/1041         0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

현재 ASA 전체에 활성 상태의 H.245 제어 세션이 하나 있습니다. 로컬 엔드포인트는 10.130.56.3이며, TPKT 값이 0이므로 이 엔드포인트의 다음 패킷에는 TPKT 헤더가 있을 것으로 예상됩니다. TKTP 헤더는 각 H.225/H.245 메시지 앞에 오는 4바이트 헤더입니다. 메시지의 길이에 4바이트의 헤더가 포함됩니다. 외부 호스트 엔드포인트는 172.30.254.203이며, TPKT 값이 0이므로 이 엔드포인트의 다음 패킷에는 TPKT 헤더가 있을 것으로 예상됩니다.

이러한 엔드포인트 간에 협상된 미디어의 경우 LCN이 258, 외부 RTP IP 주소/포트 쌍이 172.30.254.203/49608, RTCP IP 주소/포트가 172.30.254.203/49609, 로컬 RTP IP 주소/포트 쌍이 10.130.56.3/49608, RTCP 포트가 49609입니다.

두 번째 LCN 259는 외부 RTP IP 주소/포트 쌍이 172.30.254.203/49606, RTCP IP 주소/포트 쌍이 172.30.254.203/49607, 로컬 RTP IP 주소/포트 쌍이 10.130.56.3/49606, RTCP 포트가 49607입니다.

H.323 RAS 세션 모니터링

show h323-ras 명령은 ASA 전체에서 게이트키퍼와 H.323 엔드포인트 간에 설정된 H.323 RAS 세션에 대한 연결 정보를 표시합니다. **debug h323 ras event** 및 **show local-host** 명령과 함께 이 명령은 H.323 RAS 검사 엔진의 문제를 해결하는 데 사용됩니다.

다음은 **show h323-ras** 명령의 샘플 출력입니다.

```
hostname# show h323-ras
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

위 출력은 게이트키퍼 172.30.254.214 및 해당 클라이언트 10.130.56.14 간에 활성 등록이 1개 있음을 보여줍니다.

MGCP 검사

다음 섹션에서는 MGCP 애플리케이션 검사에 대해 설명합니다.

- 9-12 페이지의 MGCP 검사 개요
- 9-13 페이지의 MGCP 검사 구성
- 9-16 페이지의 MGCP 시간 제한 값 구성
- 9-16 페이지의 MGCP 검사 확인 및 모니터링

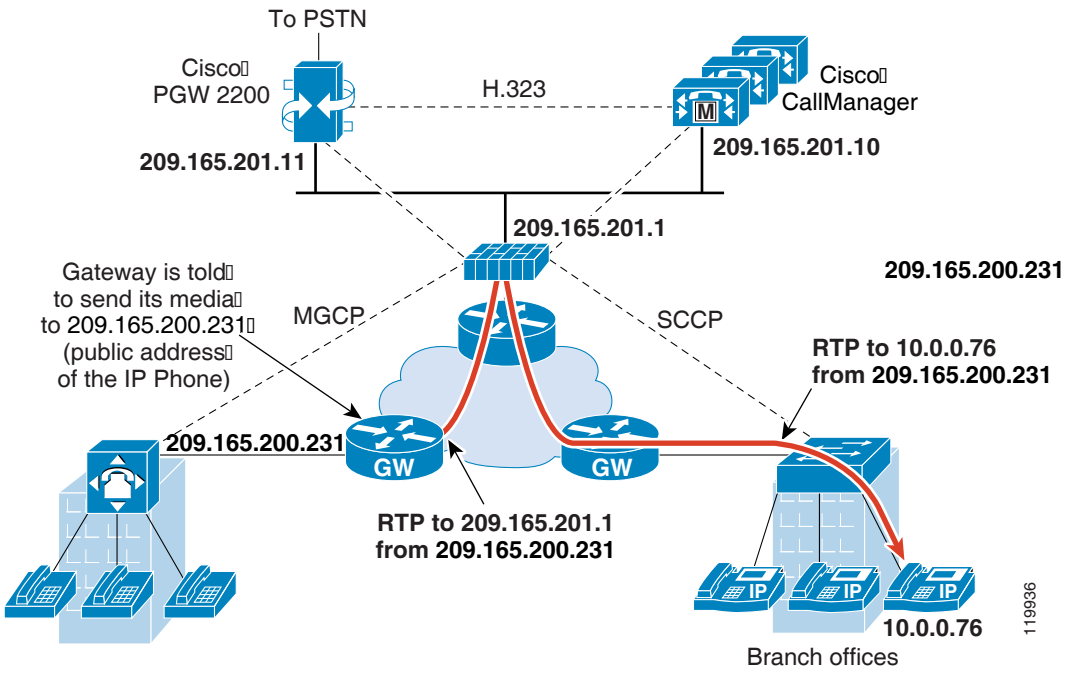
MGCP 검사 개요

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

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

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

그림 9-1 MGCP와 함께 NAT 사용



MGCP 엔드포인트는 데이터의 물리적/가상 소스 및 대상입니다. 미디어 게이트웨이는 기타 멀티미디어 엔드포인트와의 미디어 세션을 설정하고 제어하기 위해 통화 에이전트가 연결을 생성, 수정 및 삭제할 수 있는 엔드포인트를 포함합니다. 통화 에이전트는 특정 이벤트를 감지하여 신호를 생성하도록 엔드포인트에 지시할 수 있습니다. 엔드포인트는 서비스 상태의 변경 사항을 통화 에이전트에 자동으로 전달합니다.

- 게이트웨이는 일반적으로 통화 에이전트의 명령을 수신하기 위해 UDP 포트 2427에서 수신 대기합니다.
- 통화 에이전트는 게이트웨이에서 오는 명령을 이 포트에서 수신합니다. 통화 에이전트는 일반적으로 게이트웨이의 명령을 수신하기 위해 UDP 포트 2727에서 수신 대기합니다.

참고 MGCP 검사에서는 MGCP 신호 및 RTP 데이터에 서로 다른 IP 주소를 사용하는 것을 지원하지 않습니다. 일반적인 권장 방식은 복원력이 있는 IP 주소(예: 루프백 또는 가상 IP 주소)에서 RTP 데이터를 전송하는 것입니다. 그러나 ASA의 요구 사항은 RTP 데이터가 MGCP 신호와 동일한 주소에서 오는 것입니다.

MGCP 검사 구성

MGCP 검사를 활성화하려면 다음 과정을 사용합니다.

절차

1단계 9-14 페이지의 추가 검사 제어를 위한 MGCP 검사 정책 맵 구성.

2단계 9-15 페이지의 MGCP 검사 서비스 정책 구성.

추가 검사 제어를 위한 MGCP 검사 정책 맵 구성

네트워크에 ASA에서 핀홀을 열어야 하는 여러 통화 에이전트 및 게이트웨이가 있는 경우 MGCP 맵을 만듭니다. 그러면 MGCP 검사를 사용할 때 MGCP 맵을 적용할 수 있습니다.

절차

1단계 MGCP 검사 정책 맵을 만들고 다음 명령을 입력합니다.

```
hostname(config)# policy-map type inspect mgcp map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

3단계 매개변수 컨피그레이션 모드로 들어갑니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

4단계 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **call-agent** *ip_address group_id* - 하나 이상의 게이트웨이를 관리할 수 있는 통화 에이전트 그룹을 구성합니다. 모든 통화 에이전트에서 응답을 보낼 수 있도록, 그룹(게이트웨이가 명령을 전송하는 그룹 제외)의 통화 에이전트에 대한 연결을 여는 데 통화 에이전트 그룹 정보가 사용됩니다. 동일한 *group_id*의 통화 에이전트는 동일한 그룹에 속합니다. 통화 에이전트 하나가 여러 그룹에 속할 수 있습니다. *group_id* 옵션은 0~4294967295 사이의 숫자입니다. *ip_address* 옵션은 통화 에이전트의 IP 주소를 지정합니다.

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

- **gateway** *ip_address group_id* - 통화 에이전트 그룹이 특정 게이트웨이를 관리하는지 확인합니다. 게이트웨이의 IP 주소는 *ip_address* 옵션으로 지정합니다. *group_id* 옵션은 게이트웨이를 관리하는 통화 에이전트의 *group_id*와 일치해야 하는 0~4294967295 사이의 숫자입니다. 게이트웨이는 하나의 그룹에만 속할 수 있습니다.
- **command-queue** *command_limit* - MGCP 명령 큐에 허용되는 최대 명령 수를 설정합니다(1~2147483647). 기본값은 200입니다.

예

다음 예는 MGCP 맵을 정의하는 방법을 보여줍니다.

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
```

```
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

MGCP 검사 서비스 정책 구성

MGCP 검사는 기본 검사 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. 그러나 기본 검사 클래스에는 기본 MGCP 포트가 포함되어 있지 않으므로, 기본 글로벌 검사 정책을 편집하여 MGCP 검사를 추가하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map mgcp_class_map
hostname(config-cmap)# match access-list mgcp
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 MGCP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

```
class name
```

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 MGCP 검사를 구성합니다.

```
inspect mgcp [mgcp_policy_map]
```

여기서 *mgcp_policy_map*은 선택적인 MGCP 검사 정책 맵입니다. MGCP 검사 정책 맵 생성에 대한 자세한 내용은 9-14 페이지의 추가 검사 제어를 위한 MGCP 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect mgcp
hostname(config-class)# inspect mgcp mgcp-map
```

참고 다른 MGCP 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect mgcp** 명령을 사용해 MGCP 검사를 제거한 다음 새 MGCP 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

MGCP 시간 제한 값 구성

Configuration > Firewall > Advanced > Global Timeouts 페이지에서 MGCP 글로벌 시간 제한 값을 구성할 수 있습니다. MGCP 미디어 연결이 닫히기까지의 비활성 간격을 설정합니다(기본값은 5분). PAT xlate(30 초)에 대한 시간 제한도 설정할 수 있습니다.

timeout mgcp 명령을 이용해 MGCP 미디어 연결이 닫히기까지의 비활성 간격을 설정할 수 있습니다. 기본값은 5분입니다.

timeout mgcp-pat 명령을 이용해 PAT xlate에 대한 시간 제한을 설정할 수 있습니다. MGCP에는 킵얼라이브 메커니즘이 없기 때문에, 비 Cisco MGCP 게이트웨이(통화 에이전트)를 사용하는 경우 기본 시간 제한 간격(30초)이 지나면 PAT xlate가 해제됩니다.

MGCP 검사 확인 및 모니터링

show mgcp 명령은 명령 큐에 있는 MGCP 명령의 수를 표시합니다. **show mgcp sessions** 명령은 기존 MGCP 세션의 수를 표시합니다. **detail** 옵션은 출력에 있는 각 명령(또는 세션)에 대한 추가 정보를 표시합니다. 다음은 **show mgcp commands** 명령의 샘플 출력입니다.

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
```

다음은 **show mgcp detail** 명령의 샘플 출력입니다.

```
hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP      host-pc-2
        Transaction ID  2052
        Endpoint name   aaln/1
        Call ID         9876543210abcdef
        Connection ID
        Media IP        192.168.5.7
        Media port      6058
```

다음은 **show mgcp sessions** 명령의 샘플 출력입니다.

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
```

다음은 **show mgcp sessions detail** 명령의 샘플 출력입니다.

```
hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP      host-pc-2
        Call ID         9876543210abcdef
        Connection ID   6789af54c9
        Endpoint name   aaln/1
        Media lcl port  6166
        Media rmt IP    192.168.5.7
        Media rmt port  6058
```

RTSP 검사

다음 섹션에서는 RTSP 애플리케이션 검사에 대해 설명합니다.

RTSP 검사 개요

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

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

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

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

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

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

RTSP 검사는 PAT 또는 이중 NAT를 지원하지 않습니다. 또한 ASA는 RTSP 메시지가 HTTP 메시지에 숨겨지는 HTTP 클로킹을 인식할 수 없습니다.

RealPlayer 컨피그레이션 요구 사항

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

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

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

RSTP 검사의 제한

RSTP 검사에는 다음과 같은 제한이 적용됩니다.

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

RTSP 검사 구성

RTSP 검사는 기본적으로 사용됩니다. 기본 이외의 프로세싱을 원하는 경우에만 구성해야 합니다. RTSP 검사를 사용자 지정하려면 다음 프로세스를 사용합니다.

절차

1단계 9-18 페이지의 RTSP 검사 정책 맵 구성

2단계 9-21 페이지의 RTSP 검사 서비스 정책 구성

RTSP 검사 정책 맵 구성

네트워크에서 기본 검사 동작만으로 충분하지 않은 경우 RTSP 검사 정책 맵을 만들어 RTSP 검사 작업을 사용자 지정할 수 있습니다.

트래픽 매칭 기준을 정의할 때 클래스 맵을 만들 수도 있고, 정책 맵에 일치 명령문을 직접 포함할 수도 있습니다. 다음 절차에서는 두 가지 방법을 모두 설명합니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 (선택 사항) 다음 단계를 수행하여 RTSP 검사 클래스 맵을 만듭니다.

클래스 맵은 여러 트래픽 일치를 그룹화합니다. 대신 정책 맵에서 **match** 명령을 직접 지정할 수도 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.

클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다.

이 클래스 맵에서 식별하는 트래픽에 대해 수행할 작업을 검사 정책 맵에서 지정할 수 있습니다.

각 **match** 명령에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

a. 다음 명령을 입력하여 클래스 맵을 만듭니다.

```
hostname(config)# class-map type inspect rtsp [match-all | match-any] class_map_name
hostname(config-cmap)#
```

여기서 *class_map_name*은 클래스 맵의 이름입니다. **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. **match-any** 키워드는 트래픽이 하나 이상의 기준과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

b. (선택 사항) 클래스 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-cmap)# description string
```

c. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **request-method** *method* - RTSP 요청 메서드를 확인합니다. 메서드에는 announce, describe, get_parameter, options, pause, play, record, redirect, setup, set_parameter, teardown이 있습니다.
- **match** [**not**] **url-filter regex** {*regex_name* | **class** *class_name*} - URL을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.

2단계 RTSP 검사 정책 맵을 만들고 다음 명령을 입력합니다.

```
hostname(config)# policy-map type inspect rtsp policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

3단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

4단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.

- RTSP 클래스 맵을 만든 경우 다음 명령을 입력하여 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- RTSP 클래스 맵에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {drop-connection [log] | log | rate-limit message_rate}
```

drop-connection 키워드는 패킷을 삭제하고 연결을 닫습니다. 이 옵션은 URL 매칭에만 사용할 수 있습니다.

단독으로 또는 **drop-connection**과 함께 사용할 수 있는 **log** 키워드는 시스템 로그 메시지를 전송합니다.

rate-limit *message_rate* 인수는 초당 메시지의 속도를 제한합니다. 이 옵션은 요청 메서드 매칭에 사용할 수 있습니다.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다. **class** 및 **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

5단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **reserve-port-protect** - 미디어 협상 중에 예약 포트의 사용을 제한합니다.
- **url-length-limit** *bytes* - 메시지에서 사용할 수 있는 URL 길이의 제한을 설정합니다(0~6000 바이트).

예

다음 예는 RTSP 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic
```

```
hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

RTSP 검사 서비스 정책 구성

기본 ASA 컨피그레이션에는 모든 인터페이스에 전체적으로 적용되는 기본 포트에 대한 RAS 검사가 포함됩니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map rtsp_class_map
hostname(config-cmap)# match access-list rtsp
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 RTSP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 RTSP 검사를 구성합니다.

inspect rtsp [*rtsp_policy_map*]

여기서 *rtsp_policy_map*은 선택적인 RTSP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. RTSP 검사 정책 맵 생성에 대한 자세한 내용은 9-18 페이지의 RTSP 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect rtsp
hostname(config-class)# inspect rtsp rtsp-map
```

참고 다른 RTSP 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect rtsp** 명령을 사용해 RTSP 검사를 제거한 다음 새 RTSP 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

SIP 검사

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

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

SIP 검사는 기본적으로 사용됩니다. 기본 이외의 프로세싱을 원하는 경우 또는 암호화된 트래픽 검사를 활성화하기 위해 TLS 프록시를 식별하고자 하는 경우에만 구성해야 합니다. 다음 항목에서는 SIP 검사에 대해 좀 더 자세히 설명합니다.

SIP 검사 개요

IETF에 정의된 대로 SIP는 통화 처리 세션, 특히 양자간 오디오 컨퍼런스 또는 "통화"를 활성화합니다. SIP는 통화 신호에 대해 SDP와 작동합니다. SDP는 미디어 스트림용 포트를 지정합니다. SIP를 사용하여 ASA는 SIP VoIP 게이트웨이 및 VoIP 프록시 서버를 지원할 수 있습니다. SIP 및 SDP는 다음 RFC에 정의되어 있습니다.

- SIP: Session Initiation Protocol, RFC 3261
- SDP: Session Description Protocol, RFC 2327

SIP 통화가 ASA를 통과하도록 지원하려면 미디어 연결 주소, 미디어 포트 및 미디어의 미발달 연결에 대한 신호 메시지를 검사해야 합니다. 잘 알려진 목적지 포트(UDP/TCP 5060)를 통해 신호가 전송되는 동안 미디어 스트림이 동적으로 할당되기 때문입니다. 또한 SIP는 IP 패킷의 사용자 데이터 부분에 IP 주소를 포함합니다. ASA에서 지원하는 SIP Request URI의 최대 길이는 255입니다.

SIP 검사의 제한

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

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

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

SIP 인스턴트 메시징

인스턴트 메시징은 사용자 간 메시지를 거의 실시간으로 전송합니다. SIP는 Windows Messenger RTC Client 버전 4.7.0105를 사용하는 경우에만 Windows XP의 채팅 기능을 지원합니다. 다음 RFC에 정의된 대로 IM을 지원하기 위해 MESSAGE/INFO 메서드 및 202 Accept 응답이 사용됩니다.

- SIP(Session Initiation Protocol)-Specific Event Notification, RFC 3265
- SIP(Session Initiation Protocol) Extension for Instant Messaging, RFC 3428

MESSAGE/INFO 요청은 등록/서브스크립션 후 언제든 올 수 있습니다. 예를 들어, 사용자 2명이 언제든 온라인 상태일 수 있지만 수 시간 동안 채팅할 수는 없습니다. 따라서 SIP 검사 엔진은 구성된 SIP 시간 제한 값에 따라 시간이 초과되는 핀홀을 엽니다. 이 값은 서브스크립션 기간보다 길게 최소 5분으로 구성해야 합니다. 서브스크립션 기간은 Contact Expires 값에서 정의하며 일반적으로 30분입니다.

MESSAGE/INFO 요청은 대개 동적으로 할당된 포트(5060 이외의 포트)를 사용하여 전송되므로 SIP 검사 엔진을 통과해야 합니다.

참고 채팅 기능만 지원됩니다. 화이트보드, 파일 전송 및 애플리케이션 공유 기능은 지원되지 않습니다. RTC Client 5.0은 지원되지 않습니다.

SIP 검사는 SIP 텍스트 기반 메시지를 변환하고, 메시지 SDP 부분의 콘텐츠 길이를 다시 계산하고, 패킷 길이 및 체크섬을 다시 계산합니다. 또한 메시지 SDP 부분에 지정된 포트에 대한 미디어 연결을 엔드포인트가 수신 대기해야 할 주소/포트로서 동적으로 엽니다.

SIP 검사에는 SIP 페이로드의 CALL_ID/FROM/TO 인덱스가 포함된 데이터베이스가 있습니다. 이러한 인덱스는 통화, 소스 및 대상을 식별합니다. 이 데이터베이스에는 SDP 미디어 정보 필드의 미디어 주소와 미디어 포트 및 미디어 유형이 포함되어 있습니다. 한 세션에 여러 개의 미디어 주소 및 포트가 있을 수 있습니다. ASA는 이러한 미디어 주소/포트를 사용해 두 엔드포인트 간 RTP/RTCP 연결을 엽니다.

잘 알려진 포트 5060은 초기 통화 설정(INVITE) 메시지에 사용해야 합니다. 그러나 이후 메시지에는 이 포트 번호가 없을 수 있습니다. SIP 검사 엔진은 신호 연결 핀홀을 열고, 이러한 연결을 SIP 연결로 표시합니다. 이 작업은 SIP 애플리케이션에 도달하고 변환되는 메시지에 대해 수행됩니다.

통화가 설정되면, 수신자 엔드포인트에서 수신 대기하는 RTP 포트를 나타내는 Response 메시지의 수신자 엔드포인트에서 미디어 주소와 미디어 포트를 받을 때까지 SIP 세션은 "transient" 상태에 있게 됩니다. 1분 내에 응답 메시지를 받지 못하면 신호 연결이 해제됩니다.

최종 핸드셰이크가 만들어지면 통화는 활성 상태로 전환되며 BYE 메시지를 수신할 때까지 신호 연결이 유지됩니다.

내부 엔드포인트가 외부 엔드포인트에 대한 통화를 시작하면 RTP/RTCP UDP 패킷이 내부 엔드포인트 미디어 주소 및 내부 엔드포인트의 INVITE 메시지에 지정된 미디어 포트로 들어올 수 있도록 외부 인터페이스에 대해 미디어 홀이 열립니다. ASA 컨피그레이션에서 명확하게 허용하지 않는 한 내부 인터페이스에 대해 요청되지 않은 RTP/RTCP UDP 패킷은 ASA를 통과하지 못합니다.

기본 SIP 검사

SIP 검사는 다음과 같은 기본 검사 맵을 사용하여 기본적으로 활성화됩니다.

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

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

SIP 검사 구성

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

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

절차

1단계 9-25 페이지의 SIP 검사 정책 맵 구성

2단계 9-28 페이지의 SIP 검사 서비스 정책 구성

SIP 검사 정책 맵 구성

네트워크에서 기본 검사 동작만으로 충분하지 않은 경우 SIP 검사 정책 맵을 만들어 SIP 검사 작업을 사용자 지정할 수 있습니다.

트래픽 매칭 기준을 정의할 때 클래스 맵을 만들 수도 있고, 정책 맵에 일치 명령문을 직접 포함할 수도 있습니다. 다음 절차에서는 두 가지 방법을 모두 설명합니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 (선택 사항) 다음 단계를 수행하여 SIP 검사 클래스 맵을 만듭니다.

클래스 맵은 여러 트래픽 일치를 그룹화합니다. 대신 정책 맵에서 **match** 명령을 직접 지정할 수도 있습니다. 클래스 맵을 만드는 것과 검사 정책 맵에서 직접 트래픽 일치를 정의하는 것의 차이는, 클래스 맵에서는 좀 더 복잡한 일치 기준을 만들 수 있으며 클래스 맵을 재사용할 수 있다는 점입니다.

클래스 맵과 일치해서는 안 되는 트래픽을 지정하려면 **match not** 명령을 사용합니다. 예를 들어 **match not** 명령에서 "example.com" 문자열을 지정하면 "example.com"을 포함하는 모든 트래픽은 클래스 맵과 일치하지 않게 됩니다.

이 클래스 맵에서 식별하는 트래픽에 대해 수행할 작업을 검사 정책 맵에서 지정할 수 있습니다.

각 **match** 명령에 대해 서로 다른 작업을 수행하려면 정책 맵에서 직접 트래픽을 식별해야 합니다.

a. 다음 명령을 입력하여 클래스 맵을 만듭니다.

```
hostname(config)# class-map type inspect sip [match-all | match-any] class_map_name
hostname(config-cmap)#
```

여기에서 *class_map_name*은 클래스 맵의 이름입니다. **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. match-any 키워드는 트래픽이 하나 이상의 **match** 문과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.

b. (선택 사항) 클래스 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-cmap)# description string
```

여기서 *string*은 클래스 맵에 대한 설명입니다(최대 200자).

c. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*} - To 헤더에 지정된 대로 수신자를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*} - From 헤더에 지정된 대로 발신자를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **content length gt** *bytes* - SIP 헤더의 콘텐츠 길이가 지정된 바이트 수(0~65536)보다 큰지 확인합니다.
- **match** [**not**] **content type** {**sdp** | **regex** {*regex_name* | **class** *class_name*} - 콘텐츠 유형을 SDP로서 또는 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **im-subscriber regex** {*regex_name* | **class** *class_name*} - SIP IM 가입자를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **message-path regex** {*regex_name* | **class** *class_name*} - 헤더를 통해 SIP를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **request-method** *method* - SIP 요청 메서드(ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update)를 확인합니다.
- **match** [**not**] **third-party-registration regex** {*regex_name* | **class** *class_name*} - 타사 등록의 요청자를 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **uri {sip | tel} length gt** *bytes* - 선택한 유형(SIP or TEL)의 SIP 헤더에 있는 URI의 길이가 지정된 값(0~65536)보다 큰지 확인합니다.

d. 클래스 맵 컨피그레이션 모드를 종료하려면 **exit**를 입력합니다.

2단계 SIP 검사 정책 맵을 만들고 다음 명령을 입력합니다.

```
hostname(config)# policy-map type inspect sip policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

3단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

4단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음 방법 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다.

- SIP 클래스 맵을 만든 경우 다음 명령을 입력하여 지정합니다.

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- SIP 클래스 맵에 대해 설명한 **match** 명령 중 하나를 사용하여 정책 맵에서 직접 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {[drop | drop-connection | reset] [log] |
rate-limit message_rate}
```

각 **match** 또는 **class** 명령에서 모든 옵션을 사용할 수 있는 것은 아닙니다. 사용 가능한 정확한 옵션은 CLI 도움말 또는 명령 참조에서 확인할 수 있습니다.

drop 키워드는 일치하는 모든 패킷을 삭제합니다.

drop-connection 키워드는 패킷을 삭제하고 연결을 닫습니다.

reset 키워드는 패킷을 삭제하고, 연결을 닫고, TCP 재설정을 서버 및/또는 클라이언트로 전송합니다.

단독으로 또는 기타 키워드와 함께 사용할 수 있는 **log** 키워드는 시스템 로그 메시지를 전송합니다.

rate-limit *message_rate* 인수는 메시지의 속도를 제한합니다. 요청 메서드가 "invite" 및 "register"와 일치하는 경우에만 속도 제한을 사용할 수 있습니다.

정책 맵에서 여러 **class** 또는 **match** 명령을 지정할 수 있습니다. **class** 및 **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

5단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **im** - 인스턴트 메시징을 활성화합니다.
- **ip-address-privacy** - 서버 및 엔드포인트 IP 주소를 숨기는 IP 주소 비공개를 활성화합니다.
- **max-forwards-validation action {drop | drop-connection | reset | log} [log]** - Max-Forwards 헤더의 값을 확인합니다. 이 값은 목적지에 도달하기 전에는 0이 될 수 없습니다. 적합하지 않은 트래픽에 대해 수행할 작업(패킷 삭제, 연결 해제, 재설정, 기록 등) 및 기록의 사용 여부를 선택해야 합니다.
- **rtp-conformance [enforce-payloadtype]** - 핀홀에서 흐르는 RTP 패킷에 대해 프로토콜 적합성을 확인합니다. 선택적인 **enforce-payloadtype** 키워드는 신호 교환을 기반으로 오디오 또는 비디오에 페이로드 유형을 적용합니다.
- **software-version action {mask [log] | log}** - Server 및 User-Agent(엔드포인트) 헤더 필드를 사용하여 소프트웨어 버전을 식별합니다. SIP 메시지에서 소프트웨어 버전을 마스크 처리하고 선택적으로 기록할 수도 있고, 단순히 기록만 할 수도 있습니다.
- **state-checking action {drop | drop-connection | reset | log} [log]** - 상태 변환 확인을 활성화합니다. 적합하지 않은 트래픽에 대해 수행할 작업(패킷 삭제, 연결 해제, 재설정, 기록 등) 및 기록의 사용 여부를 선택해야 합니다.
- **strict-header-validation action {drop | drop-connection | reset | log} [log]** - RFC 3261에 따라 SIP 메시지의 헤더 필드를 엄격하게 검증합니다. 적합하지 않은 트래픽에 대해 수행할 작업(패킷 삭제, 연결 해제, 재설정, 기록 등) 및 기록의 사용 여부를 선택해야 합니다.
- **traffic-non-sip** - 잘 알려진 SIP 신호 포트에서 비 SIP 트래픽을 허용합니다.
- **uri-non-sip action {mask [log] | log}** - Alert-Info 및 Call-Info 헤더 필드에 있는 비 SIP URI를 식별합니다. SIP 메시지에서 정보를 마스크 처리하고 선택적으로 기록할 수도 있고, 단순히 기록만 할 수도 있습니다.

예

다음 예는 SIP를 통한 인스턴트 메시징을 비활성화하는 방법을 보여줍니다.

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

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

SIP 검사 서비스 정책 구성

기본 ASA 컨피그레이션에는 모든 인터페이스에 전체적으로 적용되는 기본 포트에 대한 SIP 검사가 포함됩니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map sip_class_map
hostname(config-cmap)# match access-list sip
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 SIP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 SIP 검사를 구성합니다.

```
inspect sip [sip_policy_map] [tls-proxy proxy_name]
```

여기서 각 항목은 다음을 나타냅니다.

- *sip_policy_map*은 선택적인 SIP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. SIP 검사 정책 맵 생성에 대한 자세한 내용은 9-25 페이지의 SIP 검사 정책 맵 구성을 참조하십시오.
- **tls-proxy** *proxy_name*은 이 검사에 사용할 TLS 프록시를 식별합니다. 암호화된 트래픽의 검사를 활성화하려는 경우에만 TLS 프록시가 필요합니다.

예:

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

참고 다른 SIP 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect sip** 명령을 사용해 SIP 검사를 제거한 다음 새 SIP 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

```
service-policy policymap_name {global | interface interface_name}
```

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

SIP 시간 제한 값 구성

연결이 유휴 상태가 된 후 2분 이내에 미디어 연결이 해제됩니다. 그러나 이 시간 제한은 구성 가능하며 더 짧게 또는 더 길게 설정할 수 있습니다.

Configuration > Firewall > Advanced > Global Timeouts 페이지에서 SIP 글로벌 시간 제한 값을 구성할 수 있습니다.

SIP 제어 연결에 대한 시간 제한을 구성하려면 다음 명령을 입력합니다.

```
hostname(config)# timeout sip hh:mm:ss
```

이 명령은 SIP 제어 연결이 닫힌 후 유휴 제한 시간을 구성 합니다.

SIP 미디어 연결에 대한 시간 제한을 구성하려면 다음 명령을 입력합니다.

```
hostname(config)# timeout sip_media hh:mm:ss
```

이 명령은 SIP 미디어 연결이 닫힌 후 유휴 제한 시간을 구성 합니다.

SIP 검사 확인 및 모니터링

show sip 명령은 ASA 전반에 걸쳐 설정된 SIP 세션에 대한 정보를 표시합니다. **debug sip** 및 **show local-host** 명령과 함께 이 명령은 SIP 검사 엔진의 문제를 해결하는 데 사용됩니다.

다음은 **show sip** 명령의 샘플 출력입니다.

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
    state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
    state Active, idle 0:00:06
```

이 샘플에서는 ASA에 있는 2개의 활성 SIP 세션을 보여줍니다(Total 필드에 표시됨). 각 call-id는 통화를 나타냅니다.

첫 번째 세션(call-id c3943000-960ca-2e43-228f@10.130.56.44)은 Call Init 상태인데, 이는 세션이 아직 통화 설정 중임을 의미합니다. 통화에 대한 최종 응답을 수신하기 전에는 통화 설정이 완료되지 않습니다. 예를 들어 발신자가 이미 INVITE를 보냈고 100 Response를 수신했을 수 있지만, 200 OK가 아직 표시되지 않았으므로 통화 설정은 완료된 것이 아닙니다. 모든 non-1xx 응답 메시지가 최종 응답으로 간주됩니다. 이 세션은 1초 동안 유휴 상태였습니다.

두 번째 세션은 Active 상태인데, 이는 통화 설정이 완료되었고 엔드포인트가 미디어를 교환 중임을 의미합니다. 이 세션은 6초 동안 유휴 상태였습니다.

Skinny(SCCP) 검사

다음 섹션에서는 SCCP 애플리케이션 검사에 대해 설명합니다.

SCCP 검사 개요

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

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

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

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

Cisco IP Phone 지원

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

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

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

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

SCCP 검사의 제한

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

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

기본 SCCP 검사

SCCP 검사는 기본적으로 다음 기본값으로 사용됩니다.

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

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

SCCP(Skinny) 검사 구성

SCCP(Skinny) 애플리케이션 검사는 패킷 데이터 내에 포함된 IP 주소와 포트 번호를 변환하고 핀홀을 동적으로 엽니다. 또한 추가 프로토콜 적합성 확인 및 기본 상태 추적을 수행합니다.

SCCP 검사는 기본적으로 사용됩니다. 기본 이외의 프로세싱을 원하는 경우 또는 암호화된 트래픽 검사를 활성화하기 위해 TLS 프록시를 식별하고자 하는 경우에만 구성해야 합니다. SCCP 검사를 사용자 지정하려면 다음 프로세스를 사용합니다.

절차

1단계 9-32 페이지의 추가 검사 제어를 위한 Skinny(SCCP) 검사 정책 맵 구성

2단계 9-33 페이지의 SCCP 검사 서비스 정책 구성

추가 검사 제어를 위한 Skinny(SCCP) 검사 정책 맵 구성

메시지가 매개변수를 위반하는 경우의 작업을 지정하려면 SCCP 검사 정책 맵을 만듭니다. 그러면 SCCP 검사를 사용할 때 검사 정책 맵을 적용할 수 있습니다.

절차

1단계 SCCP 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect skinny policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가합니다.

```
hostname(config-pmap)# description string
```

3단계 (선택 사항) SCCP 메시지의 스테이션 메시지 ID 필드를 기반으로 트래픽을 삭제합니다.

a. 16진수의 스테이션 메시지 ID 값을 기반으로 트래픽을 식별합니다(0x0~0xffff). **match** [**not**] **message-id** 명령을 사용하여 단일 ID 또는 ID 범위를 지정할 수 있습니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

```
hostname(config-pmap)# match message-id value
hostname(config-pmap)# match message-id range start_value end_value
```

예:

```
hostname(config-pmap)# match message-id 0x181

hostname(config-pmap)# match message-id range 0x200 0xffff
```

b. 일치하는 패킷에 대해 수행할 작업을 지정합니다. 패킷을 삭제하고 선택적으로 기록할 수 있습니다.

```
hostname(config-pmap)# drop [log]
```

c. 삭제할 모든 메시지 ID를 확인할 때까지 이 과정을 반복합니다.

4단계 검사 엔진에 영향을 미치는 매개변수를 구성합니다.

a. 매개변수 컨피그레이션 모드로 들어갑니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **enforce-registration** - 통화를 시작하기 전에 등록을 적용합니다.
- **message-ID max** *hex_value* - 허용되는 최대 SCCP 스테이션 메시지 ID를 설정합니다. 메시지 ID는 16진수이고 기본 최대값은 0x181입니다.
- **rtp-conformance** [**enforce-payloadtype**] - 핀홀에서 흐르는 RTP 패킷에 대해 프로토콜 적합성을 확인합니다. 선택적인 **enforce-payloadtype** 키워드는 신호 교환을 기반으로 오디오 또는 비디오에 페이로드 유형을 적용합니다.
- **sccp-prefix-len** {**max** | **min**} *length* - 허용되는 최대 또는 최소 SCCP 접두사 길이를 지정합니다. 최소값과 최대값을 모두 설정하려면 명령을 두 번 입력합니다. 기본 최소값은 4이며 기본 최대값은 없습니다.
- **timeout** {**media** | **signaling**} *time* - 미디어 및 신호 연결의 시간 제한을 설정합니다 (hh:mm:ss 형식). 시간 제한을 없애려면 숫자에 0을 지정합니다. 기본 미디어 시간 제한은 5분이고 기본 신호 시간 제한은 1시간입니다.

예

다음 예는 SCCP 검사 정책 맵을 정의하는 방법을 보여줍니다.

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

SCCP 검사 서비스 정책 구성

기본 ASA 컨피그레이션에는 모든 인터페이스에 전체적으로 적용되는 기본 포트에 대한 SCCP 검사가 포함됩니다. 검사 컨피그레이션을 사용자 지정하기 위한 일반적인 방법은 기본 글로벌 정책을 사용자 지정하는 것입니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map sccp_class_map
hostname(config-cmap)# match access-list sccp
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 SCCP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 SCCP 검사를 구성합니다.

inspect skinny [*sccp_policy_map*] [**tls-proxy** *proxy_name*]

여기서 각 항목은 다음을 나타냅니다.

- *sccp_policy_map*은 선택적인 SCCP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. SCCP 검사 정책 맵 생성에 대한 자세한 내용은 9-32 페이지의 추가 검사 제어를 위한 Skinny(SCCP) 검사 정책 맵 구성을 참조하십시오.
- **tls-proxy** *proxy_name*은 이 검사에 사용할 TLS 프록시를 식별합니다. 암호화된 트래픽의 검사를 활성화하려는 경우에만 TLS 프록시가 필요합니다.

예:

```
hostname(config-class)# no inspect skinny
hostname(config-class)# inspect skinny sccp-map
```

참고 다른 SCCP 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect skinny** 명령을 사용해 SCCP 검사를 제거한 다음 새 SCCP 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

SCCP 검사 확인 및 모니터링

show Skinny 명령은 SCCP(Skinny) 검사 엔진 문제의 해결을 지원합니다. 다음 샘플 출력은 다음과 같은 조건에서 **show skinny** 명령을 사용한 결과입니다. ASA 전체에 2개의 활성 Skinny 세션이 설정됩니다. 첫 번째 세션은 내부 Cisco IP Phone(로컬 주소 10.0.0.11) 및 외부 Cisco CallManager(172.18.1.33) 간에 설정됩니다. TCP 포트 2000은 CallManager입니다. 두 번째 세션은 내부 Cisco IP Phone(로컬 호스트 10.0.0.22) 및 동일한 Cisco CallManager 간에 설정됩니다.

```
hostname# show skinny
        LOCAL                   FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

이 출력은 두 개의 내부 Cisco IP Phone 간에 통화가 설정되었음을 나타냅니다. 첫 번째 및 두 번째 전화기의 RTP 수신 대기 포트는 각각 UDP 22948 및 20798입니다.

다음은 이러한 Skinny 연결에 대한 **show xlate debug** 명령의 샘플 출력입니다.

```
hostname# show xlate debug
2 in use, 2 most used
Flags:  D - DNS, d - dump, I - identity, i - inside, n - no random,
        r - portmap, s - static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

음성 및 비디오 프로토콜 검사를 위한 기록

기능 이름	릴리스	기능 정보
SIP, SCCP 및 TLS 프록시에서 IPv6 지원	9.3(1)	이제 SIP, SCCP 및 TLS 프록시를 사용할 때 IPv6 트래픽을 검사할 수 있습니다(SIP 또는 SCCP 사용). 수정된 명령이 없습니다.

10 장

데이터베이스 및 디렉토리 프로토콜 검사

다음 항목에서는 데이터베이스 및 디렉토리 프로토콜에 대한 애플리케이션 검사에 대해 설명합니다. 특정 프로토콜에 대해 검사를 사용해야 하는 이유 및 검사 적용을 위한 전반적인 방법에 대해 자세히 알아보려면 7-1 페이지의 애플리케이션 계층 프로토콜 검사 시작을 참조하십시오.

ILS 검사

ILS 검사 엔진은 LDAP를 사용해 ILS 서버와 디렉토리 정보를 교환하는 Microsoft NetMeeting, SiteServer 및 Active Directory 제품에 NAT 지원을 제공합니다.

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

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

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

참고 ILS 트래픽(H225 통화 신호)은 보조 UDP 채널에서만 발생하므로 TCP 비활성 간격 이후 TCP 연결이 해제됩니다. 기본적으로 이 간격은 60분이며 TCP **timeout** 명령으로 조정 가능합니다. ASDM에서는 해당 명령이 **Configuration > Firewall > Advanced > Global Timeouts** 창에 있습니다.

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

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

ILS 검사는 다음 작업을 수행합니다.

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

ILS 검사에는 다음과 같은 제한이 있습니다.

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

ILS 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

SQL*Net 검사

SQL*Net 검사는 기본적으로 사용됩니다.

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

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

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

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

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

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

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

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

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

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

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

SQL*Net 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

Sun RPC 검사

이 섹션에서는 Sun RPC 애플리케이션 검사에 대해 설명합니다.

Sun RPC 검사 개요

Sun RPC 검사 엔진은 Sun RPC 프로토콜에 대한 애플리케이션 검사를 활성화 또는 비활성화합니다. NFS 및 NIS에서 Sun RPC를 사용합니다. Sun RPC 서비스는 어느 포트에서나 실행할 수 있습니다. 클라이언트가 서버의 Sun RPC 서비스에 액세스하려면 현재 서비스가 실행 중인 포트를 알아야 합니다. 이 작업은 잘 알려진 포트 111에서 포트 매퍼 프로세스(대개 rpcbind)를 쿼리하여 수행됩니다.

클라이언트는 서비스의 Sun RPC 프로그램 번호를 전송하고 포트 매퍼 프로세스는 서비스의 포트 번호로 응답합니다. 클라이언트는 포트 매퍼 프로세스로 식별된 포트를 지정하여 Sun RPC 쿼리를 서버로 전송합니다. 서버가 회신할 때 ASA는 이 패킷을 가로채고 해당 포트에서 두 개의 미발달 TCP 및 UDP 연결을 모두 엽니다.

팁 Sun RPC 검사는 기본적으로 사용됩니다. 사용자는 방화벽 통과를 허용할 서비스를 식별하기 위해 Sun RPC 서버 테이블을 관리하기만 하면 됩니다. Sun RPC 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

Sun RPC 검사에는 다음과 같은 제한이 적용됩니다.

- Sun RPC 페이로드 정보의 NAT 또는 PAT는 지원되지 않습니다.
- Sun RPC 검사는 인바운드 ACL만 지원합니다. 검사 엔진이 보조 연결 대신 동적 ACL을 사용하므로 Sun RPC 검사는 아웃바운드 ACL을 지원하지 않습니다. 동적 ACL은 항상 이그레스(egress)가 아니라 인그레스(ingress) 방향에서 추가됩니다. 따라서 이 검사 엔진은 아웃바운드 ACL을 지원하지 않습니다. ASA에 대해 구성된 동적 ACL을 보려면 **show asp table classify domain permit** 명령을 사용하십시오.

Sun RPC 서비스 관리

기존의 Sun RPC 세션을 기반으로 ASA를 통해 Sun RPC 트래픽을 제어하려면 Sun RPC 서비스 테이블을 사용하십시오. Sun RPC 서비스 테이블에서 항목을 만들려면 글로벌 컨피그레이션 모드에서 **sunrpc-server** 명령을 사용합니다.

```
hostname(config)# sunrpc-server interface_name ip_address mask service service_type
protocol {tcp | udp} port[-port] timeout hh:mm:ss
```

이 명령을 사용해 Sun RPC 애플리케이션 검사에 의해 열린 핀홀이 닫히기까지의 시간 제한을 지정할 수 있습니다. 예를 들어 IP 주소 192.168.100.2의 Sun RPC 서버에 시간 제한 30분을 지정하려면 다음 명령을 입력합니다.

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003
protocol tcp 111 timeout 00:30:00
```

이 명령은 Sun RPC 애플리케이션 검사에 의해 열린 핀홀이 30분 후에 닫히도록 지정합니다. 이 예에서 Sun RPC 서버는 TCP 포트 111을 사용하는 내부 인터페이스에 있습니다. UDP, 다른 포트 번호 또는 포트 범위를 지정할 수도 있습니다. 포트 범위를 지정하려면 범위의 시작 및 끝 포트 번호를 하이픈으로 구분합니다(예: 111-113).

서비스 유형은 특정 서비스 유형 및 서비스에 사용된 포트 번호 간 매핑을 식별합니다. 서비스 유형을 확인하려면(이 예의 경우 100003) Sun RPC 서버 시스템의 UNIX 또는 Linux 명령줄에서 **sunrpcinfo** 명령을 사용합니다.

Sun RPC 컨피그레이션을 지우려면 다음 명령을 입력합니다.

```
hostname(config)# clear configure sunrpc-server
```

그러면 **sunrpc-server** 명령을 사용하여 수행된 컨피그레이션이 제거됩니다. **sunrpc-server** 명령을 사용하면 지정된 시간 제한으로 핀홀을 생성할 수 있습니다.

활성 Sun RPC 서비스를 지우려면 다음 명령을 입력합니다.

```
hostname(config)# clear sunrpc-server active
```

그러면 NFS 또는 NIS 등 특정 서비스에 대한 Sun RPC 애플리케이션 검사에 의해 열린 핀홀이 지워집니다.

Sun RPC 검사 확인 및 모니터링

이 섹션의 샘플 출력은 내부 인터페이스에서 IP 주소가 192.168.100.2인 Sun RPC 서버 및 외부 인터페이스에서 IP 주소가 209.168.200.5인 Sun RPC 클라이언트에 대한 것입니다.

현재 Sun RPC 연결에 대한 정보를 보려면 **show conn** 명령을 입력합니다. 다음은 **show conn** 명령의 샘플 출력입니다.

```
hostname# show conn
15 in use, 21 most used
UDP out 209.165.200.5:800 in 192.168.100.2:2049 idle 0:00:04 flags -
UDP out 209.165.200.5:714 in 192.168.100.2:111 idle 0:00:04 flags -
UDP out 209.165.200.5:712 in 192.168.100.2:647 idle 0:00:05 flags -
UDP out 192.168.100.2:0 in 209.165.200.5:714 idle 0:00:05 flags i
hostname(config)#
```

Sun RPC 서비스 테이블 컨피그레이션에 대한 정보를 표시하려면 **show running-config sunrpc-server** 명령을 입력합니다. 다음은 **show running-config sunrpc-server** 명령의 샘플 출력입니다.

```
hostname(config)# show running-config sunrpc-server
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003 protocol UDP port 111
timeout 0:30:00
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100005 protocol UDP port 111
timeout 0:30:00
```

이 출력은 내부 인터페이스에서 IP 주소가 192.168.100.2인 Sun RPC 서버에 대해 UDP 포트 111에서 시간 제한 간격 30분이 구성되었음을 보여줍니다.

Sun RPC 서비스에 대해 열린 핀홀을 표시하려면 **show sunrpc-server active** 명령을 입력합니다. 다음은 **show sunrpc-server active** 명령의 샘플 출력입니다.

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL 열의 항목은 내부 인터페이스에 있는 클라이언트 또는 서버의 IP 주소를 보여주는 반면, FOREIGN 열의 값은 외부 인터페이스에 있는 클라이언트 또는 서버의 IP 주소를 보여줍니다.

Sun RPC 서버에서 실행 중인 Sun RPC 서비스에 대한 정보를 보려면 Linux 또는 UNIX 서버 명령줄에서 **rpcinfo -p** 명령을 입력합니다. 다음은 **rpcinfo -p** 명령의 샘플 출력입니다.

```
sunrpcserver:~ # rpcinfo -p
program vers proto port
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 632 status
100024 1 tcp 635 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100021 1 udp 32771 nlockmgr
100021 3 udp 32771 nlockmgr
100021 4 udp 32771 nlockmgr
100021 1 tcp 32852 nlockmgr
100021 3 tcp 32852 nlockmgr
100021 4 tcp 32852 nlockmgr
100005 1 udp 647 mountd
100005 1 tcp 650 mountd
100005 2 udp 647 mountd
100005 2 tcp 650 mountd
100005 3 udp 647 mountd
100005 3 tcp 650 mountd
```

이 출력에서 포트 647은 UDP를 통해 실행되는 mountd 데몬에 해당합니다. mountd 프로세스는 포트 32780에서 좀 더 일반적으로 사용됩니다. TCP를 통해 실행되는 mountd 프로세스는 이 예에서 포트 650을 사용합니다.

11 장 관리 애플리케이션 프로토콜에 대한 검사

다음 항목에서는 관리 애플리케이션 프로토콜에 대한 애플리케이션 검사에 대해 설명합니다. 특정 프로토콜에 대해 검사를 사용해야 하는 이유 및 검사 적용을 위한 전반적인 방법에 대해 자세히 알아보려면 7-1 페이지의 애플리케이션 계층 프로토콜 검사 시작을 참조하십시오.

기본적으로 ASA에서는 몇 가지 일반적인 검사 엔진이 사용되지만, 네트워크에 따라 다른 엔진을 사용해야 할 수도 있습니다.

DCERPC 검사

다음 섹션에서는 DCERPC 검사 엔진에 대해 설명합니다.

DCERPC 개요

DCERPC는 Microsoft에서 배포한 클라이언트 및 서버 애플리케이션에서 널리 사용되는 프로토콜로서, 소프트웨어 클라이언트가 서버의 프로그램을 원격으로 실행하도록 허용합니다.

일반적으로 이 과정에서 잘 알려진 포트 번호에서 필수 서비스에 대한 동적으로 할당되는 네트워크 정보를 수신 대기하는 엔드포인트 매퍼(Endpoint Mapper)라는 서버에 쿼리합니다. 그런 다음 클라이언트는 서비스를 제공하는 서버 인스턴스에 대해 보조 연결을 설정합니다. 보안 어플라이언스는 적절한 포트 번호와 네트워크 주소를 허용하며, 필요한 경우 보조 연결을 위해 NAT를 적용합니다.

DCERPC 검사 맵은 잘 알려진 TCP 포트 135에서 EPM과 클라이언트 간 기본 TCP 통신을 검사합니다. 클라이언트에 대해 EPM의 맵 및 조회 작업이 지원됩니다. 클라이언트와 서버는 보안 영역의 어디에든 배치할 수 있습니다. 해당 EPM 응답 메시지로부터 내장 서버 IP 주소 및 포트 번호가 수신됩니다. 클라이언트는 EPM에서 반환하는 서버 포트에 대해 연결을 여러 번 시도할 수 있으므로 핀홀의 다중 사용이 허용되며, 이 경우 시간 제한을 구성할 수 있습니다.

참고 DCERPC 검사는 ASA를 통해 핀홀을 열 수 있도록 EPM과 클라이언트 간 통신만을 지원합니다. EPM을 사용하지 않는 RPC 통신을 사용하는 클라이언트의 경우 DCERPC 검사가 지원되지 않습니다.

DCERPC 검사 구성

DCERPC 검사는 기본적으로 사용되지 않습니다. DCERPC 검사를 사용하려면 구성해야 합니다.

절차

1단계 11-2 페이지의 DCERPC 검사 정책 맵 구성

2단계 11-3 페이지의 DCERPC 검사 서비스 정책 구성

DCERPC 검사 정책 맵 구성

추가 DCERPC 검사 매개 변수를 지정하려면 DCERPC 검사 정책 맵을 만듭니다. 그러면 DCERPC 검사를 사용할 때 검사 정책 맵을 적용할 수 있습니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 DCERPC 검사 정책 맵을 만들고 다음 명령을 입력합니다.

```
hostname(config)# policy-map type inspect dcerpc policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

3단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **timeout pinhole** *hh:mm:ss* - DCERPC 핀홀의 시간 제한을 구성하여 2분의 글로벌 시스템 핀홀 시간 제한을 재정의합니다. 시간 제한의 범위는 00:00:01~119:00:00입니다.

- **endpoint-mapper** [**epm-service-only**] [**lookup-operation** [**timeout** *hh:mm:ss*]] - 엔드포인트 매퍼 트래픽에 대한 옵션을 구성합니다. **epm-service-only** 키워드는 서비스 트래픽만 처리되도록 바인딩 중에 엔드포인트 매퍼 서비스를 적용합니다. **lookup-operation** 키워드는 엔드포인트 매퍼 서비스의 조회 작업을 활성화합니다. 조사 작업에서 생성되는 핀홀의 시간 제한을 구성할 수 있습니다. 조회 작업에 대해 시간 제한을 구성하지 않으면 시간 제한 핀홀 명령 또는 기본값이 사용됩니다.

예

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

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

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

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

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

DCERPC 검사 서비스 정책 구성

DCERPC 검사는 기본 검색 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. DCERPC 검사를 추가하려면 기본 글로벌 검사 정책을 편집하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map dcerpc_class_map
hostname(config-cmap)# match access-list dcerpc
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 DCERPC 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 DCERPC 검사를 구성합니다.

inspect dcerpc [*dcerpc_policy_map*]

여기서 *dcerpc_policy_map*은 선택적인 DCERPC 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. 검사 정책 맵 생성에 대한 자세한 내용은 11-2 페이지의 DCERPC 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect dcerpc
hostname(config-class)# inspect dcerpc dcerpc-map
```

참고 다른 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect dcerpc** 명령을 사용해 DCERPC 검사를 제거한 다음 새 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

GTP 검사

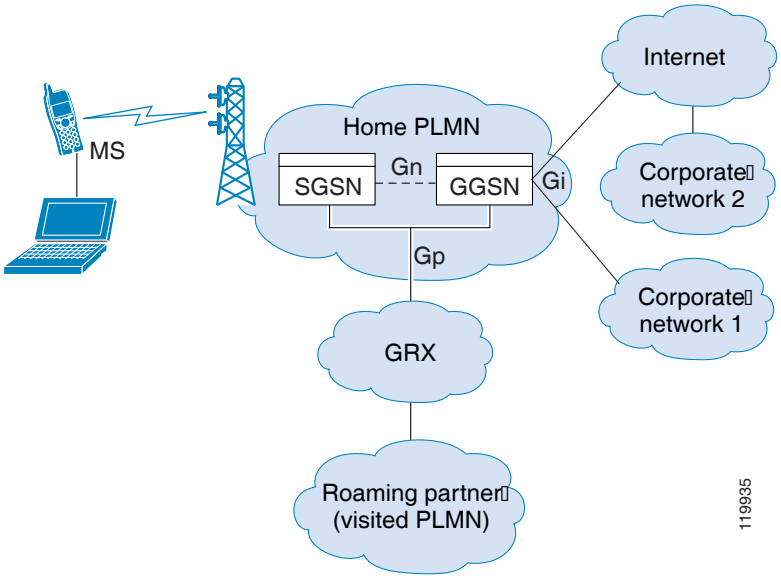
다음 섹션에서는 GTP 검사 엔진에 대해 설명합니다.

참고 GTP 검사에는 특별한 라이센스가 필요합니다.

GTP 검사 개요

GPRS는 모바일 가입자에게 GSM 네트워크와 회사 네트워크 또는 인터넷 간 무중단 연결을 제공합니다. GGSN은 GPRS 무선 데이터 네트워크 및 기타 네트워크 간의 인터페이스입니다. SGSN은 모빌리티, 데이터 세션 관리 및 데이터 압축을 수행합니다.

그림 11-1 GPRS 터널링 프로토콜



UMTS는 고정 라인 텔레포니, 모바일, 인터넷 및 컴퓨터 기술을 상업적으로 통합한 서비스입니다. UTRAN은 이 시스템의 무선 네트워크 구현에 사용되는 네트워킹 프로토콜입니다. GTP는 다중 프로토콜 패킷이 GGSN, SGSN 및 UTRAN 간 UMTS/GPRS 백본을 통해 터널링하도록 허용합니다.

GTP에는 내재적 보안 또는 사용자 데이터의 암호화가 포함되어 있지 않습니다. 그러나 ASA와 함께 GTP를 사용하면 네트워크를 위험으로부터 보호하는 데 도움이 됩니다.

SGSN은 GTP를 사용하여 GGSN에 논리적으로 연결됩니다. GTP는 다중 프로토콜 패킷이 GSN 간 GPRS 백본을 통해 터널링하도록 허용합니다. GTP는 SGSN에서 터널을 생성, 수정 및 삭제하여 이동 통신국용 GPRS 네트워크 액세스를 제공하도록 허용하는 터널 제어 및 관리 프로토콜을 제공합니다. GTP는 사용자 데이터 패킷 전송 서비스를 제공하기 위해 터널링 메커니즘을 사용합니다.

참고 장애 조치와 함께 GTP를 사용할 때 GTP 연결이 설정된 후 터널을 통해 데이터가 전송되기 전에 활성 유닛이 실패하면, GTP 데이터 연결("j" 플래그 세트)이 스탠바이 유닛에 복제되지 않습니다. 이는 활성 유닛이 미발달 연결을 대기 유닛으로 복제하지 않기 때문에 발생합니다.

GTP 검사를 위한 기본값

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

- 오류는 허용되지 않습니다.
- 최대 요청 수는 200입니다.

- 최대 터널 수는 500입니다.
- GSN 시간 제한은 30분입니다.
- PDP 컨텍스트 시간 제한은 30분입니다.
- 요청 시간 제한은 1분입니다.
- 신호 시간 제한은 30분입니다.
- 터널링 시간 제한은 1시간입니다.
- T3 응답 시간 제한은 20초입니다.
- 알 수 없는 메시지 ID가 삭제 및 기록됩니다.

GTP 검사 구성

GTP 검사는 기본적으로 사용되지 않습니다. GTP 검사를 사용하려면 구성해야 합니다.

절차

1단계 11-6 페이지의 GTP 검사 정책 맵 구성

2단계 11-9 페이지의 GTP 검사 서비스 정책 구성

3단계 (선택 사항) 과다 청구 공격을 방지하려면 RADIUS 어카운팅 검사를 구성합니다. 11-11 페이지의 RADIUS 어카운팅 검사 섹션을 참조하십시오.

GTP 검사 정책 맵 구성

GTP 트래픽에 추가 매개 변수를 적용하려고 하는데 기본 맵이 요구를 충족하지 않는 경우 GTP 맵을 만들고 구성합니다.

시작하기 전에

일부 트래픽 매칭 옵션에서는 매칭을 위해 정규식을 사용합니다. 이러한 방법 중 하나를 사용하려면 먼저 정규식 또는 정규식 클래스 맵을 만드십시오.

절차

1단계 GTP 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect gtp policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가하려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# description string
```

3단계 일치하는 트래픽에 작업을 적용하려면 다음 단계를 수행하십시오.

a. 다음의 **match** 명령 중 하나를 사용하여 작업을 수행할 트래픽을 지정합니다. **match not** 명령을 사용하는 경우 **match not** 명령의 기준과 일치하지 않는 트래픽에 작업이 적용됩니다.

- **match** [**not**] **apn regex** {*regex_name* | **class** *class_name*} - APN(Access Point Name)을 지정된 정규식 또는 정규식 클래스와 맞춰봅니다.
- **match** [**not**] **message id** {*message_id* | **range** *message_id_1 message_id_2*} - 1~255의 메시지 ID를 맞춰봅니다. 단일 ID 또는 ID의 범위를 지정할 수 있습니다.
- **match** [**not**] **message length min** *bytes* **max** *bytes* - UDP 페이로드의 길이(GTP 헤더 및 메시지의 나머지)가 최소값과 최대값(1~65536) 사이인 메시지를 맞춰봅니다.
- **match** [**not**] **version** {*version_id* | **range** *version_id_1 version_id_2*} - GTP 버전(0~255)을 맞춰봅니다. 단일 버전 또는 버전의 범위를 지정할 수 있습니다.

b. 다음 명령을 입력하여 일치하는 트래픽에 대해 수행할 작업을 지정합니다.

```
hostname(config-pmap-c)# {drop [log]| log | rate-limit message_rate}
```

각 **match** 명령에서 모든 옵션을 사용할 수 있는 것은 아닙니다.

- **drop** 키워드는 패킷을 삭제합니다.
- 단독으로 또는 **drop**과 함께 사용할 수 있는 **log** 키워드는 시스템 로그 메시지를 전송합니다.
- **rate-limit** *message_rate* 인수는 메시지의 속도를 제한합니다. 이 옵션은 **message id**에서만 사용할 수 있습니다.

정책 맵에서 여러 **match** 명령을 지정할 수 있습니다. **match** 명령의 순서에 대한 자세한 내용은 2-4 페이지의 검사 정책 맵에서 작업 정의를 참조하십시오.

4단계 검사 엔진에 영향을 미치는 매개 변수를 구성하려면 다음 단계를 수행하십시오.

a. 매개변수 컨피그레이션 모드로 들어가려면 다음 명령을 입력합니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **permit errors** - 유효하지 않은 GTP 패킷 또는 구문 분석에 실패하여 삭제될 수 있는 패킷을 허용합니다.
- **request-queue** *max_requests* - 응답을 대기하도록 큐에 추가할 최대 GTP 요청 수를 설정합니다. 기본값은 200입니다. 제한에 도달한 상태에서 새 요청이 도착하면 큐에 있는 가장 오래된 요청이 제거됩니다. Error Indication, Version Not Supported 및 SGSN Context Acknowledge 메시지는 요청으로 간주되지 않으며 응답 대기를 위해 요청 큐에 추가되지 않습니다.
- **tunnel-limit** *max_tunnels* - ASA에서 활성화할 수 있는 최대 GTP 터널 수를 설정합니다. 기본값은 500입니다. 이 명령으로 지정한 터널 수에 도달하면 새 요청은 삭제됩니다.
- **timeout** {**gsn** | **pdp-context** | **request** | **signaling** | **tunnel**} *time* - 지정한 서비스의 유휴 시간 제한을 설정합니다(hh:mm:ss 형식). 시간 제한을 없애려면 숫자에 0을 지정합니다. 각 시간 제한에 대해 명령을 별도로 입력합니다.

  gsn 키워드는 GSN이 제거되기까지의 비활성 상태 기간을 지정합니다.

  pdp-context 키워드는 PDP 컨텍스트 수신을 시작하기 전에 허용되는 최대 기간을 지정합니다.

  request 키워드는 GTP 메시지 수신을 시작하기 전에 허용되는 최대 기간을 지정합니다.

  signaling 키워드는 GTP 신호가 제거되기까지의 비활성 상태 기간을 지정합니다.

  tunnel 키워드는 GTP 터널이 해제되기까지의 비활성 상태 기간을 지정합니다.

5단계 아직 매개 변수 컨피그레이션 모드에 있을 때 원하는 경우 IMSI 접두사 필터링을 구성합니다.

```
hostname(config-pmap-p)# mcc country_code mnc network_code
```

기본적으로 보안 어플라이언스는 유효한 MCC(Mobile Country Code)/MNC(Mobile Network Code) 조합을 확인하지 않습니다. IMSI 접두사 필터링을 구성하면, 수신된 패킷의 IMSI에 있는 MCC 및 MNC가 구성된 MCC/MNC 조합과 비교된 후 일치하지 않을 경우 삭제됩니다.

MCC(Mobile Country Code)는 0이 아닌 3자리 값입니다. 1자리나 2자리 값에는 0을 접두사로 추가합니다. MNC(Mobile Network Code)는 2자리 또는 3자리 값입니다.

허가된 모든 MCC 및 MNC 조합을 추가합니다. 기본적으로 ASA에서는 MNC 및 MCC 조합의 유효성을 확인하지 않으므로, 구성된 조합의 유효성을 사용자가 직접 확인해야 합니다. MCC 및 MNC 코드에 대해 자세히 알아보려면 ITU E.212 권장 사항, *Identification Plan for Land Mobile Stations*를 참조하십시오.

6단계 아직 매개 변수 컨피그레이션 모드에 있을 때 원하는 경우 GSN 풀링을 구성합니다.

```
hostname(config-pmap-p)# permit response to-object-group SGSN_name
from-object-group GSN_pool
```

ASA에서 GTP 검사를 수행할 때, GTP 요청에 지정되지 않은 GSN에서 오는 GTP 응답은 기본적으로 ASA에 의해 삭제됩니다. 이러한 상황은 GPRS의 효율성과 확장성을 제공하기 위해 GSN 풀 간 부하 균형을 사용할 때 발생합니다.

GSN 풀링을 구성하고 부하 균형도 지원하려면 GSN을 지정하는 네트워크 객체 그룹을 만들고 이를 **from-object-group** 매개 변수에서 지정합니다. 마찬가지로 SGSN에 대한 네트워크 객체 그룹을 만들고 **to-object-group** 매개 변수로써 선택합니다. GSN 응답이 GTP 요청을 전송한 GSN과 동일한 객체 그룹에 속하는 경우, 그리고 응답하는 GSN이 GTP 응답을 보내도록 허용된 객체 그룹에 SGSN이 속하는 경우, ASA에서는 응답을 허용합니다.

네트워크 객체 그룹은 호스트 주소 또는 포함된 서브넷에 의해 GSN 또는 SGSN을 식별할 수 있습니다.

예

다음 예는 GSN 풀 및 SGSN에 대한 네트워크 객체를 정의하여 GSN 풀링을 지원하는 방법을 보여줍니다. 전체 Class C 네트워크는 GSN 풀로 정의되지만, 전체 네트워크를 지정하는 대신 **network-object** 명령으로 하나씩 여러 개의 개별 IP 주소를 지정할 수도 있습니다. 다음 예에서는 또한 GSN 풀에서 SGSN으로의 응답을 허용하도록 GTP 검사 맵을 수정합니다.

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config)# gtp-map gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit response to-object-group sgsn32
from-object-group gsnpool32
```

예

다음 예는 네트워크에서 터널 수를 제한하는 방법을 보여줍니다.

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

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

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

GTP 검사 서비스 정책 구성

GTP 검사는 기본 검색 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. GTP 검사를 추가하려면 기본 글로벌 검사 정책을 편집하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

class-map *name*
match *parameter*

예:

```
hostname(config)# class-map gtp_class_map
hostname(config-cmap)# match access-list gtp
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 GTP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

4단계 GTP 검사를 구성합니다.

inspect gtp [*gtp_policy_map*]

여기서 *gtp_policy_map*은 선택적인 GTP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다. 검사 정책 맵 생성에 대한 자세한 내용은 11-6 페이지의 GTP 검사 정책 맵 구성을 참조하십시오.

예:

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

참고 다른 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect gtp** 명령을 사용해 GTP 검사를 제거한 다음 새 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

GTP 검사 확인 및 모니터링

GTP 컨피그레이션을 표시하려면 권한이 있는 EXEC 모드에서 **show service-policy inspect gtp** 명령을 입력합니다.

GTP 검사의 통계를 표시하려면 **show service-policy inspect gtp statistics** 명령을 사용합니다. 다음은 **show service-policy inspect gtp statistics** 명령의 샘플 출력입니다.

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                   0     total_dropped             0
  signalling_msg_dropped            0     data_msg_dropped          0
  signalling_msg_forwarded          0     data_msg_forwarded        0
  total created_pdp                 0     total deleted_pdp         0
  total created_pdpmcb              0     total deleted_pdpmcb      0
  pdp_non_existent                  0
```

다음은 **show service-policy inspect gtp statistics gsn** 명령의 샘플 GSN 출력입니다.

```
hostname# show service-policy inspect gtp statistics gsn 10.9.9.9
1 in use, 1 most used, timeout 0:00:00

GTP GSN Statistics for 10.9.9.9, Idle 0:00:00, restart counter 0
    Tunnels Active 0Tunnels Created 0
    Tunnels Destroyed 0
    Total Messages Received 2
    Signaling Messages Data Messages
```

```
    total received 2 0
    dropped 0 0
    forwarded 2 0
```

PDP 컨텍스트 관련 정보를 표시하려면 **show service-policy inspect gtp pdp-context** 명령을 사용합니다. 예:

```
hostname# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used, timeout 0:00:00

Version TID                MS Addr         SGSN Addr     Idle      APN
v1      1234567890123425         10.0.1.1        10.0.0.2 0:00:13  gprs.cisco.com

    user_name (IMSI): 214365870921435    MS address:          1.1.1.1
    primary pdp: Y                       nsapi: 2
    sgsn_addr_signal:         10.0.0.2   sgsn_addr_data:           10.0.0.2
    ggsn_addr_signal:         10.1.1.1   ggsn_addr_data:           10.1.1.1
    sgsn control teid:     0x000001d1    sgsn data teid:         0x000001d3
    ggsn control teid:     0x6306ffa0    ggsn data teid:         0x6305f9fc
    seq_tpdu_up:                    0    seq_tpdu_down:                   0
    signal_sequence:                0
    upstream_signal_flow:           0    upstream_data_flow:              0
    downstream_signal_flow:         0    downstream_data_flow:            0
    RAupdate_flow:                  0
```

PDP 컨텍스트는 터널 ID로 식별되며, 이는 IMSI 및 NSAPI 값의 조합입니다. GTP 터널은 서로 다른 GSN 노드에 있는 두 개의 관련된 PDP 컨텍스트에 의해 정의되며 터널 ID로 식별됩니다. 외부 패킷 데이터 네트워크와 MS 사용자 간에 패킷을 전달하려면 GTP 터널이 필요합니다.

RADIUS 어카운팅 검사

다음 섹션에서는 RADIUS 어카운팅 검사 엔진에 대해 설명합니다.

- 11-11 페이지의 RADIUS 어카운팅 검사 개요
- 11-12 페이지의 RADIUS 어카운팅 검사 구성

RADIUS 어카운팅 검사 개요

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

GPRS 네트워크에서 과다 청구 공격이 발생하면 사용하지 않은 서비스가 소비자에게 청구됩니다. 이 경우 악의적인 공격자는 서버에 연결하고 SGSN에서 IP 주소를 가져옵니다. 공격자가 호출을 종료해도 악의적인 서버는 여전히 패킷을 보내며, GGSN에서 이를 삭제하지만 서버와의 연결은 계속 활성 상태로 유지됩니다. 악의적인 공격자에게 할당된 IP 주소는 해제된 후 합법적인 사용자에게 다시 할당됩니다. 그러면 공격자가 사용한 서비스가 해당 사용자에게 청구됩니다.

RADIUS 어카운팅 검사는 GGSN에 표시되는 트래픽이 합법적인지 확인하여 이러한 유형의 공격을 방지합니다. RADIUS 어카운팅 기능을 올바르게 구성하면 ASA에서는 Radius Accounting Request Start 메시지의 Framed IP 특성을 Radius Accounting Request Stop 메시지와 비교해보고 연결을 차단합니다. Framed IP 특성의 매칭 IP 주소에 Stop 메시지가 있으면 ASA에서는 IP 주소와 일치하는 소스와의 모든 연결을 살펴봅니다.

ASA에서 메시지의 유효성을 확인할 수 있도록 RADIUS 서버와 암호 사전 공유 키를 구성할 수 있습니다. 공유 암호가 구성되지 않으면 ASA에서는 소스 IP 주소가 RADIUS 메시지를 전송할 수 있도록 구성된 IP 주소인지만을 확인합니다.

참고 GPRS와 함께 RADIUS 어카운팅 검사를 사용하면 ASA에서는 Accounting Request STOP 메시지의 3GPP-Session-Stop-Indicator를 확인하여 보조 PDP 컨텍스트를 적절하게 처리합니다. 특히 ASA에서는 사용자 세션 및 모든 관련 연결을 종료하기 전에 Accounting Request STOP 메시지에 3GPP-SGSN-Address 특성이 포함되어 있는지 확인합니다. 일부 타사 GGSN에서는 기본적으로 이 특성을 전송할 수 없습니다.

RADIUS 어카운팅 검사 구성

RADIUS 어카운팅 검사는 기본적으로 사용되지 않습니다. RADIUS 어카운팅 검사를 사용하려면 구성해야 합니다.

절차

1단계 11-12 페이지의 RADIUS 어카운팅 검사 정책 맵 구성

2단계 11-13 페이지의 RADIUS 어카운팅 검사 서비스 정책 구성

RADIUS 어카운팅 검사 정책 맵 구성

검사에 필요한 특성을 구성하려면 RADIUS 어카운팅 검사 정책 맵을 만들어야 합니다.

절차

1단계 RADIUS 어카운팅 검사 정책 맵을 만듭니다.

```
hostname(config)# policy-map type inspect radius-accounting policy_map_name
hostname(config-pmap)#
```

여기에서 *policy_map_name*은 정책 맵의 이름입니다. CLI가 정책 맵 컨피그레이션 모드로 전환됩니다.

2단계 (선택 사항) 정책 맵에 설명을 추가합니다.

```
hostname(config-pmap)# description string
```

3단계 매개변수 컨피그레이션 모드로 들어갑니다.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

4단계 하나 이상의 매개변수를 설정합니다. 다음 옵션을 설정할 수 있으며, 옵션을 비활성화하려면 **no** 형식의 명령을 사용합니다.

- **send response** - 메시지 전송자에게 Accounting-Request Start 및 Stop 메시지를 전송하도록 ASA에 지시합니다(**host** 명령에서 식별됨).
- **enable gprs** - GPRS 과다 청구 방지를 구현합니다. ASA는 보조 PDP 컨텍스트를 적절히 처리하기 위해 Accounting-Request Stop 및 Disconnect 메시지에서 3GPP VSA 26-10415 특성을 확인합니다. 이 특성이 있으면 ASA는 구성된 인터페이스의 사용자 IP 주소와 일치하는 소스 IP가 있는 모든 연결을 해제합니다.

- **validate-attribute** *number* -Accounting-Request Start 메시지를 수신할 때 사용자 계정 테이블을 구축하는 데 사용할 추가 기준입니다. 이 특성은 ASA에서 연결 해제 여부를 결정하는 데 도움이 됩니다.

  검증할 추가 특성을 지정하지 않으면 Framed IP Address 특성의 IP 주소만을 기준으로 결정이 내려집니다. 추가 특성을 구성하면 ASA는 현재 추적 중인 주소가 포함된 시작 어카운팅 메시지를 수신합니다. 그러나 검증할 기타 특성이 서로 다르면, 새 사용자에게 IP 주소가 다시 할당된 것으로 가정하여 이전 특성을 사용하여 시작된 모든 연결이 해제됩니다.

  값의 범위는 1~191이며, 명령을 여러 번 입력할 수 있습니다. 특성 번호 목록 및 해당 설명을 보려면 http://www.iana.org/assignments/radius-types를 방문하십시오.

- **host** *ip_address* [**key** *secret*] - RADIUS 서버 또는 GGSN의 IP 주소입니다. ASA에서 메시지를 검증할 수 있도록 선택적으로 암호 키를 포함할 수 있습니다. 키가 없으면 IP 주소만 확인됩니다. 여러 RADIUS 및 GGSN 호스트를 식별하기 위해 이 명령을 반복할 수 있습니다. ASA는 이러한 호스트에서 RADIUS 어카운팅 메시지의 사본을 수신합니다.
- **timeout users** *time* - 사용자에 대한 유휴 시간을 설정합니다(hh:mm:ss 형식). 시간 제한을 없애려면 숫자에 00:00:00을 지정합니다. 기본값은 1시간입니다.

예

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

RADIUS 어카운팅 검사 서비스 정책 구성

RADIUS 어카운팅 검사는 기본 검색 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. RADIUS 어카운팅 검사는 ASA에 대한 트래픽을 대상으로 하므로 표준 규칙이 아니라 관리 검사 규칙으로서 구성해야 합니다.

절차

1단계 검사를 적용할 트래픽 및 일치하는 트래픽을 식별하기 위한 L3/L4 관리 클래스 맵을 만듭니다.

class-map type management *name*
match {port | access-list} *parameter*

예:

```
hostname(config)# class-map type management radius-class-map
hostname(config-cmap)# match port udp eq radius-acct
```

이 예제는 radius-acct UDP 포트(1646)의 일치에 대한 것입니다. 다른 포트, 포트의 범위(**match port udp range** *number1 number2*)를 지정할 수도 있고 **match access-list** *acl_name* 및 ACL을 사용할 수도 있습니다.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 RADIUS 어카운팅 검사에 대해 사용 중인 L3/L4 관리 클래스 맵을 식별합니다.

class *name*

예:

```
hostname(config-pmap)# class radius-class-map
```

4단계 RADIUS 어카운팅 검사를 구성합니다.

inspect radius-accounting *radius_accounting_policy_map*

여기서 *radius_accounting_policy_map*은 11-12 페이지의 RADIUS 어카운팅 검사 정책 맵 구성에서 만든 RADIUS 어카운팅 검사 정책 맵입니다.

예:

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

참고 다른 검사 정책 맵을 사용하기 위해 현재 사용 중인 정책을 편집하려면 **no inspect radius-accounting** 명령을 사용해 RADIUS 어카운팅 검사를 제거한 다음 새 검사 정책 맵 이름으로 다시 추가해야 합니다.

5단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

RSH 검사

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

RSH 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

SNMP 검사

SNMP 애플리케이션 검사를 사용하면 SNMP 트래픽을 SNMP의 특정 버전으로 제한할 수 있습니다. SNMP의 이전 버전은 덜 안전하므로, 보안 정책에서 특정 SNMP 버전을 거부하는 설정이 필요할 수 있습니다. ASA는 SNMP 버전 1, 2, 2c 또는 3을 거부할 수 있습니다. SNMP 맵을 만들어 허용되는 버전을 제어하십시오.

SNMP 검사는 기본 검색 정책에서 활성화되지 않으므로 이 검사가 필요한 경우 직접 활성화해야 합니다. SNMP 검사를 추가하려면 기본 글로벌 검사 정책을 편집하면 됩니다. 또는 새 서비스 정책을 원하는 대로 만들 수 있습니다(예: 인터페이스 전용 정책).

절차

1단계 SNMP 맵을 만듭니다.

snmp-map *map_name* 명령을 사용하여 맵을 만들고 SNMP 맵 컨피그레이션 모드로 들어간 다음, **deny version** *version* 명령을 사용하여 허용하지 않을 버전을 지정합니다. 해당 버전은 1, 2, 2c 또는 3일 수 있습니다.

예:

다음 예에서는 SNMP 버전 1 및 2를 거부합니다.

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

2단계 필요한 경우 검사를 적용할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map snmp_class_map
hostname(config-cmap)# match access-list snmp
```

기본 글로벌 정책에서 inspection_default 클래스 맵은 모든 검사 유형에 대한 기본 포트를 포함하는 특수한 클래스 맵입니다(**match default-inspection-traffic**). 기본 정책 또는 새로운 서비스 정책에 이 클래스 맵을 사용하는 경우 이 단계를 건너뛸 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

3단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

4단계 SNMP 검사에 대해 사용 중인 L3/L4 클래스 맵을 식별합니다.

```
class name
```

예:

```
hostname(config-pmap)# class inspection_default
```

기본 정책을 편집하거나 새 정책에서 특별한 inspection_default 클래스 맵을 사용하려면 *name*에 대해 **inspection_default**를 지정합니다. 그렇지 않으면 이 절차에 앞부분에서 작성한 클래스를 지정합니다.

5단계 SNMP 검사를 구성합니다.

```
inspect snmp [snmp_map]
```

여기서 *snmp_map*은 선택적인 SNMP 검사 정책 맵입니다. 기본 검사 이외의 프로세스를 원하는 경우에만 맵이 필요합니다.

예:

```
hostname(config-class)# no inspect snmp
hostname(config-class)# inspect snmp snmp-map
```

참고 다른 검사 정책 맵을 사용하기 위해 기본 글로벌 정책(또는 사용 중인 정책)을 편집하려면 **no inspect snmp** 명령을 사용해 SNMP 검사를 제거한 다음 새 검사 정책 맵 이름으로 다시 추가해야 합니다.

6단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

```
service-policy policymap_name {global | interface interface_name}
```

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

XDMCP 검사

XDMCP 검사는 기본적으로 사용됩니다. 그러나 XDMCP 검사 엔진을 사용하려면 **established** 명령을 적절히 구성해야 합니다.

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

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

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

```
setenv DISPLAY Xserver:n
```

여기서 *n*은 디스플레이 번호입니다.

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

XDMCP 검사 사용에 대한 자세한 내용은 7-9 페이지의 애플리케이션 계층 프로토콜 검사 구성을 참조하십시오.

파 트 **4**

연결 설정 및 **QoS(Quality of Service)**

12 장

연결 설정

이 장에서는 ASA를 통과하는 연결 또는 ASA로 이동하는 관리 연결을 위해 연결 설정을 구성하는 방법에 대해 설명합니다. 연결 설정에는 다음이 포함됩니다.

- 최대 연결(TCP 및 UDP 연결, 미발달 연결, 클라이언트당 연결)
- 연결 시간 제한
- 데드 연결 감지
- TCP 시퀀스 임의 지정
- TCP 정규화 사용자 지정
- TCP 상태 바이패스
- 전역 시간 제한
- 12-1 페이지의 연결 설정에 대한 정보
- 12-4 페이지의 연결 설정에 대한 라이센스 요구 사항
- 12-4 페이지의 지침 및 제한
- 12-5 페이지의 기본 설정
- 12-6 페이지의 연결 설정 구성
- 12-12 페이지의 연결 설정 모니터링
- 12-12 페이지의 연결 설정의 컨피그레이션 예
- 12-14 페이지의 연결 설정에 대한 기능 기록

연결 설정에 대한 정보

이 섹션에서는 연결 제한이 필요할 수 있는 이유에 대해 설명합니다.

- 12-2 페이지의 TCP 가로채기 및 미발달 연결 제한
- 12-2 페이지의 클라이언트리스 SSL 호환성을 위해 관리 패킷에 대한 TCP 가로채기 비활성화
- 12-2 페이지의 DCD(데드 연결 감지)
- 12-3 페이지의 TCP 시퀀스 임의 지정
- 12-3 페이지의 TCP 정규화
- 12-3 페이지의 TCP 상태 바이패스

TCP 가로채기 및 미발달 연결 제한

미발달 연결 수를 제한하면 DoS 공격으로부터 보호할 수 있습니다. ASA에서는 클라이언트당 제한 및 미발달 연결 제한을 사용하여 TCP 가로채기를 트리거하며, 이 방법을 통해 TCP SYN 패킷으로 인터페이스를 플러딩하여 발생하는 DoS 공격으로부터 내부 시스템을 보호합니다. 미발달 연결은 소스와 대상 간에 필요한 핸드셰이크를 완료하지 않은 연결 요청입니다. TCP 가로채기는 TCP SYN 플러딩 공격을 막기 위해 SYN 쿠키 알고리즘을 사용합니다. SYN 플러딩 공격은 대개 스푸핑된 IP 주소에서 시작되는 일련의 SYN 패킷으로 구성됩니다. SYN 패킷의 지속적인 플러드로 인해 서버 SYN 큐가 계속해서 꽉 차기 때문에 연결 요청을 처리하지 못하게 됩니다. 미발달 연결이 임계값에 도달하면 ASA는 서버용 프록시 역할을 하며 클라이언트 SYN 요청에 대해 SYN-ACK 응답을 생성합니다. ASA는 클라이언트에서 ACK를 다시 받으면 클라이언트를 인증하고 서버로의 연결을 허용할 수 있습니다.

참고 SYN 공격으로부터 서버를 보호하기 위해 TCP SYN 쿠키 보호를 사용할 경우에는 보호해야 할 서버의 TCP SYN 백로그 큐보다 미발달 연결 제한을 낮게 설정해야 합니다. 그렇지 않을 경우 SYN 공격이 이루어지는 동안 유효한 클라이언트가 서버에 더 이상 액세스할 수 없게 됩니다.

공격을 받는 상위 10개의 서버를 비롯한 TCP 가로채기 통계를 보려면 16 장, “위협 감지”를 참조하십시오.

클라이언트리스 SSL 호환성을 위해 관리 패킷에 대한 TCP 가로채기 비활성화

기본적으로 TCP 관리 연결에는 TCP 가로채기가 항상 사용됩니다. 그러면 TCP 가로채기는 3방향 TCP 연결 설정 핸드셰이크 패킷을 가로채고 ASA에서 클라이언트리스 SSL에 대해 패킷을 처리하지 못하게 합니다. 클라이언트리스 SSL 연결에 선택적인 ACK 및 기타 TCP 옵션을 제공하려면 클라이언트리스 SSL에 3방향 핸드셰이크 패킷을 처리하는 기능이 필요합니다. 관리 트래픽에 대해 TCP 가로채기를 비활성화하려면 미발달 연결 제한을 설정할 수 있습니다. 미발달 연결 제한에 도달한 이후에만 TCP 가로채기가 활성화됩니다.

DCD(데드 연결 감지)

DCD는 데드 연결을 감지한 후, 트래픽을 여전히 처리할 수 있는 연결을 만료하지 않은 채 데드 연결의 만료를 허용합니다. 유휴 상태를 원하지만 유효한 연결을 지속하려는 경우 DCD를 구성할 수 있습니다.

DCD를 활성화하면 유휴 시간 제한 동작이 변경됩니다. 연결의 유효성을 확인하기 위해 2개의 엔드 호스트 각각에 유휴 시간 제한과 함께 DCD 프로브가 전송됩니다. 구성된 시간 간격으로 프로브가 전송된 후 엔드 호스트가 응답하지 않으면 해당 연결은 해제되며 재설정 값(구성된 경우)이 엔드 호스트 각각에 전송됩니다. 두 엔드 호스트가 모두 응답하면 연결이 유효한 것이며, 활동 시간 제한이 현재 시간으로 업데이트되고 유휴 시간 제한이 그에 따라 재조정됩니다.

DCD를 활성화하면 TCP 노멀라이저에서 처리하는 유휴 시간 제한의 동작이 변경됩니다. DCD 프로브는 **show conn** 명령에서 표시되는 연결에 대한 유휴 시간 제한을 재설정합니다. timeout 명령으로 구성한 시간 제한 값을 초과했지만 DCD 프로브 때문에 유지되고 있는 연결을 확인할 수 있도록 **show service-policy** 명령에는 DCD에 따른 활동의 양을 표시하는 카운터가 포함되어 있습니다.

TCP 시퀀스 임의 지정

각 TCP 연결에는 각각 클라이언트와 서버에서 생성된 2개의 ISN(초기 시퀀스 번호)이 있습니다. ASA에서는 인바운드 및 아웃바운드 방향 모두를 통과하는 TCP SYN의 ISN을 임의로 지정합니다.

보호된 호스트의 ISN을 임의로 지정하면 공격자가 새로운 연결을 위한 다음 ISN을 미리 감지하여 새 세션을 가로채는 위험을 방지할 수 있습니다.

필요한 경우 TCP 초기 시퀀스 번호 임의 지정을 비활성화할 수 있습니다. 예:

- 또 다른 인라인 방화벽에서도 ISN을 임의로 지정하는 경우, 이 작업이 트래픽에 영향을 미치지는 않지만 두 개의 방화벽에서 모두 이 작업을 수행해야 할 필요는 없습니다.
- 사용자는 ASA를 통해 eBGP 멀티홉을 사용하고 eBGP 피어는 MD5를 사용하는 경우, 임의 지정을 사용하면 MD5 체크섬이 손상됩니다.
- ASA에서 연결의 시퀀스 번호를 임의로 지정해서는 안 되는 WAAS 디바이스를 사용하는 경우입니다.

TCP 정규화

TCP 정규화 기능은 ASA에서 감지 시 동작(예: ASA에서 패킷을 허용하기, 삭제하기 또는 지우기)을 취할 수 있는 비정상 패킷을 식별합니다. TCP 정규화는 공격으로부터 ASA를 보호합니다. TCP 정규화는 항상 사용되지만, 일부 기능의 작동 방식을 사용자 지정할 수 있습니다.

TCP 노멀라이저에는 구성 가능한 작업과 구성 불가능한 작업이 모두 포함됩니다. 일반적으로, 연결을 삭제하거나 지우는 구성 불가능한 작업은 항상 불량한 패킷에 적용됩니다. 구성 가능한 작업(12-6 페이지의 TCP 맵으로 TCP 노멀라이저 사용자 지정에서 자세히 설명)은 네트워크 요구에 따라 사용자 지정이 필요할 수 있습니다.

TCP 정규화에 대한 다음 지침을 참조하십시오.

- 노멀라이저에는 SYN 플러드를 차단하는 기능이 없습니다. ASA에는 다른 방식으로 SYN 플러드를 차단하는 기능이 포함되어 있습니다.
- 장애 조치 때문에 ASA가 느슨한 모드에 있지 않은 한 노멀라이저는 항상 SYN 패킷을 흐름에서 첫 번째 패킷으로 간주합니다.

TCP 상태 바이패스

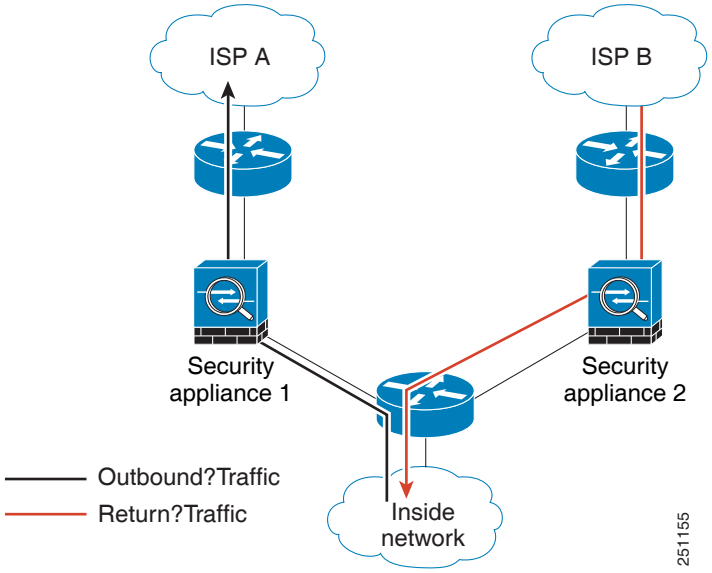
기본적으로 ASA로 들어가는 모든 트래픽은 Adaptive Security Algorithm을 사용하여 검사되며, 보안 정책에 따라 통과가 허용되거나 삭제됩니다. ASA에서는 각 패킷의 상태(새 연결 또는 기존 연결 여부)를 확인한 다음 세션 관리 경로(새 연결 SYN 패킷), 빠른 경로(기존 연결) 또는 제어 평면 경로(고급 검사) 중 하나에 할당하여 방화벽 성능을 극대화합니다. 스테이트풀 방화벽에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

빠른 경로에 있는 기존의 연결과 일치하는 TCP 패킷은 보안 정책의 모든 측면에 대한 재점검 없이도 ASA를 통과할 수 있습니다. 이 기능은 성능을 극대화합니다. 그러나 SYN 패킷을 사용하여 빠른 경로에서 세션을 설정하는 방법 및 빠른 경로에서 발생하는 점검(예: TCP 시퀀스 번호)은 비대칭 라우팅 솔루션의 대안이 될 수 있습니다. 연결의 아웃바운드 및 인바운드 흐름 모두 동일한 ASA를 통과해야 합니다.

예를 들어 새 연결은 ASA 1로 이동합니다. SYN 패킷은 세션 관리 경로로 들어가며, 연결에 대한 항목이 빠른 경로 테이블에 추가됩니다. 이 연결의 후속 패킷이 ASA 1로 들어가는 경우 빠른 경로에 있는 항목과 일치하므로 무사히 통과됩니다. 그러나 세션 관리 경로를 통과한 SYN 패킷이 없는

ASA 2로 후속 패킷이 이동하는 경우, 빠른 경로에 해당 연결에 대한 항목이 없으므로 패킷이 삭제됩니다. 그림 12-1에서는 아웃바운드 트래픽이 다른 ASA를 통과한 다음 인바운드 트래픽을 통과하는 비대칭 라우팅 예를 보여줍니다.

그림 12-1 비대칭 라우팅



업스트림 라우터에 비대칭 라우팅을 구성한 경우 트래픽이 두 개의 ASA를 통과하면, 특정 트래픽에 대해 TCP 상태 바이패스를 구성할 수 있습니다. TCP 상태 바이패스는 세션이 빠른 경로에 설정되는 방법을 변경하고 빠른 경로 점검을 비활성화합니다. 이 기능은 UDP 연결을 처리하듯 TCP 트래픽을 처리합니다. 지정된 네트워크와 일치하는 비 SYN 패킷이 ASA로 들어가고 빠른 경로 항목이 없으면, 빠른 경로에서 연결을 설정할 수 있도록 패킷이 세션 관리 경로로 들어가게 됩니다. 빠른 경로에 들어서면 트래픽은 빠른 경로 점검을 우회합니다.

연결 설정에 대한 라이센스 요구 사항

모델	라이센스 요구 사항
ASAv	표준 또는 프리미엄 라이센스
모든 다른 모델	기본 라이센스

지침 및 제한

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원됩니다.

방화벽 모드 지침

라우팅된 모드 및 투명 모드에서 지원됩니다.

장애 조치 지침

장애 조치가 지원됩니다.

TCP 상태 바이패스 지원되지 않는 기능

다음 기능은 TCP 상태 바이패스를 사용할 때 지원되지 않습니다.

- 애플리케이션 검사 - 애플리케이션 검사를 수행하려면 인바운드와 아웃바운드 트래픽이 모두 동일한 ASA를 통과해야 합니다. 따라서 TCP 상태 바이패스 시에는 애플리케이션 검사가 지원되지 않습니다.
- AAA 인증 세션 - 하나의 ASA로 사용자 인증이 이루어지는 경우, 다른 ASA를 통해 반환되는 트래픽은 거부됩니다. 사용자가 해당 ASA로 인증되지 않았기 때문입니다.
- TCP 가로채기, 최대 미발달 연결 제한, TCP 시퀀스 번호 임의 지정 - ASA에서는 연결 상태를 추적하지 않기 때문에 이러한 기능은 적용되지 않습니다.
- TCP 정규화 - TCP 노멀라이저는 사용되지 않습니다.
- SSM 및 SSC 기능 - TCP 상태 바이패스 및 SSM이나 SSC에서 실행되는 애플리케이션(예: IPS 또는 CSC)은 사용할 수 없습니다.

TCP 상태 바이패스 NAT 지침

변환 세션은 각 ASA에 대해 개별적으로 설정되기 때문에 TCP 상태 바이패스 트래픽을 위한 고정 NAT를 두 ASA에 모두 구성해야 합니다. 동적 NAT를 사용하는 경우 ASA 1의 세션에 대해 선택되는 주소와 ASA 2의 세션에 대해 선택되는 주소는 서로 다릅니다.

최대 동시 및 미발달 연결 지침

ASA 모델의 CPU 코어 수에 따라, 각 코어가 연결을 관리하는 방법 때문에 최대 동시 및 미발달 연결 수가 구성된 수를 초과할 수 있습니다. 최악의 시나리오에서는 ASA가 최대 *n*-1개의 별도 연결 및 미발달 연결을 허용할 수 있습니다. 여기서 *n*은 코어의 수입니다. 예를 들어 모델에 코어가 4개 있는데 6개의 동시 연결 및 4개의 미발달 연결을 구성하는 경우 각 유형에 대해 3개를 추가할 수 있습니다. 모델의 코어 수를 확인하려면 **show cpu core** 명령을 입력하십시오.

기본 설정

TCP 상태 바이패스

TCP 상태 바이패스는 기본적으로 사용되지 않습니다.

TCP 노멀라이저

기본 컨피그레이션에는 다음 설정이 포함됩니다.

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 255 clear
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
```

```
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

연결 설정 구성

연결 설정 구성을 위한 작업 흐름

1단계 TCP 정규화 사용자 지정을 위해 12-6 페이지의 TCP 맵으로 TCP 노멀라이저 사용자 지정에 따라 TCP 맵을 만듭니다.

2단계 한 모든 연결 설정에 대해 1 장, “Modular Policy Framework를 사용하는 서비스 정책”에 따라 서비스 정책을 구성합니다.

3단계 12-9 페이지의 연결 설정 구성에 따라 연결 설정을 구성합니다.

TCP 맵으로 TCP 노멀라이저 사용자 지정

TCP 노멀라이저를 사용자 지정하려면 먼저 TCP 맵을 사용하여 설정을 정의합니다.

자세한 단계

1단계 검색할 TCP 정규화 기준을 지정하려면 다음과 같은 명령을 입력하여 TCP 맵을 만듭니다.

```
hostname(config)# tcp-map tcp-map-name
```

각 TCP 맵에 대해 하나 이상의 설정을 사용자 지정할 수 있습니다.

2단계 (선택 사항) 다음과 같은 명령 중 하나 이상을 입력하여 TCP 맵 기준을 구성합니다(표 12-1 참조). 일부 설정을 사용자 지정하는 경우 입력하지 않는 명령에는 기본값이 사용됩니다.

표 12-1 tcp-map 명령

명령	참고
check-retransmission	일관성 없는 TCP 재전송을 방지합니다.
checksum-verification	체크섬을 확인합니다.
exceed-mss {allow | drop}	데이터 길이가 TCP 최대 세그먼트 크기를 초과하는 패킷에 대한 작업을 설정합니다. (기본값) **allow** 키워드는 데이터 길이가 TCP 최대 세그먼트 크기를 초과하는 패킷을 허용합니다. **drop** 키워드는 데이터 길이가 TCP 최대 세그먼트 크기를 초과하는 패킷을 삭제합니다.

표 12-1 tcp-map 명령 (계속)

명령	참고
invalid-ack {**allow** | **drop**}	유효하지 않은 ACK가 포함된 패킷에 대한 작업을 설정합니다. 유효하지 않은 ACK의 예는 다음과 같습니다. • TCP 연결 SYN-ACK-received 상태에서 수신된 TCP 패킷의 ACK 번호가 다음번 전송 TCP 패킷의 시퀀스 번호와 정확히 같지 않으면 유효하지 않은 ACK입니다. • 수신된 TCP 패킷의 ACK 번호가 다음번 전송 TCP 패킷의 시퀀스 번호보다 크면 유효하지 않은 ACK입니다. **allow** 키워드는 유효하지 않은 ACK가 포함된 패킷을 허용합니다. (기본값) **drop** 키워드는 유효하지 않은 ACK가 포함된 패킷을 삭제합니다. **참고** 유효하지 않은 ACK가 포함된 TCP 패킷은 WAAS 연결에서 자동으로 허용됩니다.
queue-limit *pkt_num* [**timeout** *seconds*]	버퍼링 가능하고 TCP 연결을 위해 순서를 지정할 수 있는 무순서 패킷의 최대 수(1~250)를 설정합니다. 기본값은 0입니다. 즉, 트래픽의 유형에 따라 이 설정이 비활성화되고 기본 시스템 큐 제한이 사용될 수 있음을 의미합니다. • 애플리케이션 검사(**inspect** 명령), IPS(**ips** 명령), TCP 확인 재전송(TCP map **check-retransmission** 명령)에 대한 연결에서는 큐 제한이 패킷 3개입니다. ASA에서 다른 윈도우 크기의 TCP 패킷을 수신하면 알려진 설정과 일치하도록 큐 제한이 동적으로 변경됩니다. • 다른 TCP 연결의 경우 무순서 패킷은 원래의 상태대로 전달됩니다. **queue-limit** 명령을 1 이상으로 설정한 경우, 모든 TCP 트래픽에 허용되는 무순서 패킷의 수는 이 설정과 일치합니다. 예를 들어 애플리케이션 검사, IPS 및 TCP 확인 재전송 트래픽의 경우 TCP 패킷의 알려진 설정은 **queue-limit** 설정으로 무시됩니다. 다른 TCP 트래픽의 경우 무순서 패킷은 이제 버퍼링되며, 원래대로 전달되는 대신 순서가 지정됩니다. **timeout** *seconds* 인수는 무순서 패킷이 버퍼에 머물 수 있는 최대 시간(1~20초)을 설정합니다. 시간 내에 순서가 정해져 전달되지 않으면 해당 패킷은 삭제됩니다. 기본값은 4초입니다. *pkt_num* 인수를 0으로 설정하면 트래픽의 시간 제한을 변경할 수 없습니다. **timeout** 키워드가 작동하도록 하려면 제한을 1 이상으로 설정해야 합니다.
reserved-bits {**allow** | **clear** | **drop**}	TCP 헤더에 있는 예약된 비트를 위한 작업을 설정합니다. (기본값) **allow** 키워드는 TCP 헤더에 예약된 비트가 포함된 패킷을 허용합니다. **clear** 키워드는 TCP 헤더에서 예약된 비트를 지우고 패킷을 허용합니다. **drop** 키워드는 TCP 헤더에 예약된 비트가 포함된 패킷을 삭제합니다.

표 12-1 tcp-map 명령 (계속)

명령	참고
seq-past-window {**allow** | **drop**}	past-window 시퀀스 번호가 있는 패킷에 대한 작업을 설정합니다. 즉, 수신된 TCP 패킷의 시퀀스 번호가 TCP 수신 윈도우의 오른쪽 가장자리보다 큽니다. **allow** 키워드는 past-window 시퀀스 번호가 있는 패킷을 허용합니다. 이 작업은 **queue-limit** 명령이 0(비활성)으로 설정된 경우에만 허용됩니다. (기본값) **drop** 키워드는 past-window 시퀀스 번호가 있는 패킷을 삭제합니다.
synack-data {**allow** | **drop**}	데이터가 포함된 TCP SYNACK 패킷에 대한 작업을 설정합니다. **allow** 키워드는 데이터가 포함된 TCP SYNACK 패킷을 허용합니다. (기본값) **drop** 키워드는 데이터가 포함된 TCP SYNACK 패킷을 삭제합니다.
syn-data {**allow** | **drop**}	데이터가 포함된 SYN 패킷에 대한 작업을 설정합니다. (기본값) **allow** 키워드는 데이터가 포함된 SYN 패킷을 허용합니다. **drop** 키워드는 데이터가 포함된 SYN 패킷을 삭제합니다.
tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**} 또는 **tcp-options range** *lower upper* {**allow** | **clear** | **drop**}	selective-ack, timestamp 또는 window-scale TCP 옵션 등의 TCP 옵션이 포함된 패킷에 대한 작업을 설정합니다. (기본값) **allow** 키워드는 지정된 옵션이 포함된 패킷을 허용합니다. (**range**의 기본값) **clear** 키워드는 옵션을 지우고 패킷을 허용합니다. **drop** 키워드는 지정된 옵션이 포함된 패킷을 삭제합니다. **selective-ack** 키워드는 SACK 옵션에 대한 작업을 설정합니다. **timestamp** 키워드는 타임스탬프 옵션에 대한 작업을 설정합니다. 타임스탬프 옵션을 지우면 PAWS 및 RTT가 비활성화됩니다. **widow-scale** 키워드는 윈도우 확장 메커니즘 옵션에 대한 작업을 설정합니다. **range** 키워드는 옵션의 범위를 지정합니다. *lower* 인수는 범위의 하단을 6, 7 또는 9~255로 설정합니다. *upper* 인수는 범위의 상단을 6, 7 또는 9~255로 설정합니다.
ttl-evasion-protection	TTL 회피 방지를 비활성화합니다. 보안 정책 회피를 시도하는 공격을 방지하려는 경우 이 명령을 입력하지 마십시오. 예를 들어, 공격자는 매우 짧은 TTL로 정책을 통과하는 패킷을 보낼 수 있습니다. TTL이 0이 되면 ASA와 엔드포인트 간 라우터가 패킷을 차단합니다. ASA에 재전송처럼 보여 통과되는 긴 TTL의 악의적인 패킷을 공격자가 전송할 수 있는 시점이 바로 지금입니다. 그러나 엔드포인트 호스트에서는 이것이 공격자가 수신한 첫 번째 패킷입니다. 이 경우 공격자는 해당 공격에 대한 보안 제지를 받지 않고 성공할 수 있습니다.

표 12-1 tcp-map 명령 (계속)

명령	참고
urgent-flag {**allow** | **clear**}	URG 플래그가 포함된 패킷에 대한 작업을 설정합니다. URG 플래그는 패킷이 스트림 내 다른 데이터보다 우선 순위가 높은 정보를 포함하고 있음을 나타내는 데 사용됩니다. TCP RFC는 URG 플래그의 올바른 해석에 대해서는 분명하지 않으므로 엔드 시스템에서 긴급 오프셋을 다른 방식으로 처리하는데, 이로 인해 엔드 시스템이 공격에 취약해질 수 있습니다. **allow** 키워드는 URG 플래그가 포함된 패킷을 허용합니다. (기본값) **clear** 키워드는 URG 플래그를 지우고 패킷을 허용합니다.
window-variation {**allow** | **drop**}	예기치 않게 윈도우 크기를 변경한 연결에 대한 작업을 설정합니다. 윈도우 크기 메커니즘에서는 TCP가 큰 윈도우를 알리고 그 이후 너무 많은 데이터를 수락하지 않고도 훨씬 작은 윈도우를 알리도록 허용합니다. TCP 사양에서 "윈도우의 축소"는 수행하지 않는 것이 좋습니다. 이러한 조건이 감지되면 연결을 삭제할 수 있습니다. (기본값) **allow** 키워드는 윈도우 변형이 포함된 연결을 허용합니다. **drop** 키워드는 윈도우 변형이 포함된 연결을 삭제합니다.

연결 설정 구성

연결 설정을 지정하려면 다음 단계를 수행하십시오.

자세한 단계

	명령	목적
1단계	**class-map** *name* 예: `hostname(config)# class-map bypass_traffic`	상태 기반 방화벽 검사를 비활성화할 트래픽을 식별하기 위한 클래스 맵을 만듭니다.
2단계	**match** *parameter* 예: `hostname(config-cmap)# match access-list bypass`	클래스 맵에서 트래픽을 지정합니다. 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵) 섹션을 참조하십시오.

	명령	목적
3단계	**policy-map** *name* 예: hostname(config)# policy-map tcp_bypass_policy	클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.
4단계	**class** *name* 예: hostname(config-pmap)# class bypass_traffic	1단계에서 생성한 클래스 맵을 식별합니다.
5단계	다음 중 하나 이상을 수행합니다.	
	set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]} 예: hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable	최대 연결 제한 또는 TCP 시퀀스 임의 지정의 사용 여부를 설정합니다. **conn-max** *n* 인수는 허용되는 동시 TCP 및/또는 UDP 연결의 최대 수(0~2000000)를 설정합니다. 기본값은 무제한 연결을 허용하는 0입니다. 서버 두 대가 동시 TCP 및/또는 UDP 연결을 허용하도록 구성된 경우 구성된 각 서버에 연결 제한이 별도로 적용됩니다. 클래스 아래에 구성된 경우 이 인수는 전체 클래스에 대해 허용되는 동시 연결의 최대 수를 제한합니다. 이 경우 공격 호스트 하나가 모든 연결을 사용하여, 나머지 호스트 중 해당 클래스 아래의 ACL에서 일치하는 호스트가 하나도 없을 수 있습니다. **embryonic-conn-max** *n* 인수는 허용되는 동시 미발달 연결의 최대 수(0~2000000)를 설정합니다. 기본값은 무제한 연결을 허용하는 0입니다. **per-client-embryonic-max** *n* 인수는 클라이언트당 허용되는 동시 미발달 연결의 최대 수(0~2000000)를 설정합니다. 기본값은 무제한 연결을 허용하는 0입니다. **per-client-max** *n* 인수는 클라이언트당 허용되는 동시 연결의 최대 수(0~2000000)를 설정합니다. 기본값은 무제한 연결을 허용하는 0입니다. 클래스 아래에 구성된 경우 이 인수는 해당 클래스 아래의 ACL을 통해 일치하는 각 호스트에 대해 허용되는 동시 연결의 최대 수를 제한합니다. **random-sequence-number** {**enable** | **disable**} 키워드는 TCP 시퀀스 번호 임의 지정을 활성화하거나 비활성화합니다. 자세한 내용은 12-3 페이지의 TCP 시퀀스 임의 지정 섹션을 참조하십시오. 이 명령을 임의의 순서로 한 줄에 입력할 수도 있고, 각 특성을 별도의 명령으로 입력할 수도 있습니다. ASA에서는 실행 중인 컨피그레이션에서 명령을 한 줄로 결합합니다. **참고** 관리 트래픽의 경우 **conn-max** 및 **embryonic-conn-max** 키워드만 설정할 수 있습니다.

명령	목적
set connection timeout {[**embryonic** *hh*:*mm*:*ss*] {**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [dcd *hh*:*mm*:*ss* [*max_retries*]]}	연결 시간 제한을 설정합니다. 전역 시간 제한의 경우 명령 참조의 **timeout** 명령을 참조하십시오. 아래에 설명된 기본값은 사용자가 이러한 동작의 전역 기본값을 변경하지 않은 것으로 가정합니다. 전역 기본값은 여기에서 설명한 값을 재지정합니다. **embryonic** *hh*:*mm*:*ss* 키워드는 TCP 미발달(절반이 열림) 연결이 닫힐 때까지의 시간 제한 기간(0:0:5~1193:00:00)을 설정합니다. 기본값은 0:0:30입니다. 연결 시간 제한이 발생하지 않음을 의미하는 0으로 이 값을 설정할 수도 있습니다. **idle** *hh*:*mm*:*ss* 키워드는 프로토콜의 기존 연결이 닫히기까지의 유휴 시간 제한 기간(0:0:1~1193:0:0)을 설정합니다. 기본값은 1:0:0입니다. 연결 시간 제한이 발생하지 않음을 의미하는 0으로 이 값을 설정할 수도 있습니다. TCP 트래픽의 경우 **reset** 키워드는 연결 시간 제한이 발생할 때 TCP 엔드포인트에 재설정을 전송합니다. **half-closed** *hh*:*mm*:*ss* 키워드는 절반이 닫힌 연결이 닫힐 때까지의 유휴 시간 제한을 설정합니다. 범위는 0:5:0(9.1(1) 이하의 경우) 또는 0:0:30(9.1(2) 이상의 경우)~1193:0:0입니다. 기본값은 0:10:0입니다. 절반이 닫힌 연결은 DCD의 영향을 받지 않습니다. 절반이 닫힌 연결을 닫을 때 ASA에서는 재설정을 보내지 않습니다. **dcd** 키워드는 DCD를 활성화합니다. DCD는 데드 연결을 감지한 후, 트래픽을 여전히 처리할 수 있는 연결을 만료하지 않은 채 데드 연결의 만료를 허용합니다. 유휴 상태를 원하지만 유효한 연결을 지속하려는 경우 DCD를 구성할 수 있습니다. 발신 TCP 연결 시간이 초과되면 ASA에서는 연결의 유효성을 확인하기 위해 엔드 호스트에 DCD 프로브를 보냅니다. 다시 시도의 최대 횟수가 소진된 후 엔드 호스트 중 하나에서 응답하지 않으면 ASA에서는 연결을 해제합니다. 두 엔드 호스트에서 모두 연결이 유효한 것으로 응답하면, ASA에서는 활동 시간 제한을 현재 시간으로 업데이트하고 유휴 시간 제한을 그에 따라 재조정합니다. *retry-interval*은 DCD 프로브에서 응답이 없을 때 또 다른 프로브를 보내기까지 대기하는 시간을 *hh*:*mm*:*ss* 형식으로 설정합니다(0:0:1~24:0:0). 기본값은 0:0:15입니다. *max-retries*는 연결이 데드 상태임을 선언하기 전 DCD에 대한 연속 실패 재시도 횟수를 설정합니다. 최소값은 1이고 최대값은 255입니다. 기본값은 5입니다. 기본 **udp** 유휴 시간 제한은 2분입니다. 기본 **icmp** 유휴 시간 제한은 2초입니다. 기본 **esp** 및 **ha** 유휴 시간 제한은 30초입니다. 다른 모든 프로토콜의 경우 기본 유휴 시간 제한은 2분입니다. 시간 제한이 없도록 설정하려면 0:0:0을 입력합니다. 이 명령을 임의의 순서로 한 줄에 입력할 수도 있고, 각 특성을 별도의 명령으로 입력할 수도 있습니다. 실행 중인 컨피그레이션에서는 명령이 한 줄로 결합됩니다. 관리 트래픽에는 이 명령을 사용할 수 없습니다.
예: `hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed 0:20:0 dcd`	

	명령	목적
	set connection advanced-options *tcp-map-name* **예:** hostname(config-pmap-c)# set connection advanced-options tcp_map1	TCP 노멀라이저를 사용자 지정합니다. TCP 맵 작성은 12-6 페이지의 TCP 맵으로 TCP 노멀라이저 사용자 지정을 참조하십시오.
	set connection advanced-options tcp-state-bypass **예:** hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass	TCP 상태 바이패스를 활성화합니다.
6단계	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **예:** hostname(config)# service-policy tcp_bypass_policy outside	하나 이상의 인터페이스에서 정책 맵을 활성화합니다. **global**은 모든 인터페이스에서 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

연결 설정 모니터링

TCP 상태 바이패스를 모니터링하려면 다음 작업 중 하나를 수행합니다.

명령	목적
show conn	**show conn** 명령을 사용하는 경우, TCP 상태 바이패스를 사용하는 연결에 대한 표시에 플래그 "b"가 포함됩니다.

연결 설정의 컨피그레이션 예

- 12-12 페이지의 연결 제한 및 시간 제한의 컨피그레이션 예
- 12-13 페이지의 TCP 상태 바이패스의 컨피그레이션 예
- 12-13 페이지의 TCP 정규화의 컨피그레이션 예

연결 제한 및 시간 제한의 컨피그레이션 예

다음 예에서는 모든 트래픽에 대해 연결 제한 및 시간 제한을 설정합니다.

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
```

```
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

여러 매개 변수와 함께 **set connection** 명령을 입력할 수도 있고, 각 매개 변수를 별도의 명령으로 입력할 수도 있습니다. ASA에서는 실행 중인 컨피그레이션에서 명령을 한 줄로 결합합니다. 예를 들어, 클래스 컨피그레이션 모드에서 다음의 두 명령을 입력한 경우:

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

show running-config policy-map 명령의 출력에는 두 명령이 결합된 단일 명령으로 표시될 수 있습니다.

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

TCP 상태 바이패스의 컨피그레이션 예

다음은 TCP 상태 바이패스의 샘플 컨피그레이션입니다.

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

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

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

hostname(config-pmap-c)# service-policy tcp_bypass_policy outside

hostname(config-pmap-c)# static (inside,outside) 209.165.200.224 10.1.1.0 netmask
255.255.255.224
```

TCP 정규화의 컨피그레이션 예

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

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

연결 설정에 대한 기능 기록

표 12-2에는 각 기능 변경 사항 및 그것이 구현된 플랫폼 릴리스가 나열되어 있습니다.

표 12-2 연결 설정에 대한 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
TCP 상태 바이패스	8.2(1)	이 기능이 추가되었습니다. 추가된 명령: **set connection advanced-options tcp-state-bypass**.
모든 프로토콜에 대한 연결 시간 제한	8.2(2)	TCP를 제외한 모든 프로토콜에 적용할 수 있도록 유휴 시간 제한이 변경되었습니다. 수정된 명령: **set connection timeout**
백업 고정 경로를 사용하는 연결에 대한 시간 제한	8.2(5)/8.4(2)	서로 다른 메트릭의 여러 고정 경로가 네트워크에 존재하는 경우 ASA에서는 연결 생성 시 최고의 메트릭이 포함된 경로를 사용합니다. 더 나은 경로가 사용 가능해지면, 이 시간 제한을 통해 더 나은 경로를 사용하여 연결을 다시 설정할 수 있습니다. 기본값은 0(연결 시간 제한 없음)입니다. 이 기능을 사용하려면 시간 제한을 새 값으로 변경합니다. 수정된 명령: **timeout floating-conn**.
PAT xlate에 대해 구성 가능한 시간 제한	8.4(3)	PAT xlate가 시간 초과되고(기본적으로 30초 후) ASA에서 새 변환에 포트를 다시 사용하면 일부 업스트림 라우터는 새 연결을 거부할 수 있는데, 그 이유는 업스트림 디바이스에서 이전 연결이 여전히 열려 있기 때문일 수 있습니다. PAT xlate 시간 제한을 이제 30초에서 5분 사이의 값으로 구성할 수 있습니다. 추가된 명령: **timeout pat-xlate**. *이 기능은 8.5(1) 또는 8.6(1)에서 사용할 수 없습니다.*
서비스 정책 규칙에 대한 최대 연결 제한 증가	9.0(1)	서비스 정책 규칙에 대해 최대 연결 수가 65535에서 2000000으로 증가했습니다. 수정된 명령: **set connection conn-max**, **set connection embryonic-conn-max**, **set connection per-client-embryonic-max**, **set connection per-client-max**.
절반이 닫힌 시간 제한 최소값이 30초로 감소	9.1(2)	DoS 공격을 더 잘 차단할 수 있도록 전역 시간 제한 및 연결 시간 제한 모두에 대해 절반이 닫힌 시간 제한 최소값이 5분에서 30초로 낮아졌습니다. 수정된 명령: **set connection timeout half-closed**, **timeout half-closed**.

13 장

Quality of Service

위성 연결 방식의 장거리 전화를 사용해본 적이 있으십니까? 일정하지 않은 간격으로 대화가 짧게 중단될 수는 있지만 알아들을 수 있는 수준입니다. 이러한 간격이 바로 네트워크를 통해 전송되는 패킷의 도착 사이에서 발생하는 레이턴시라는 시간입니다. 음성과 비디오 등 일부 네트워크 트래픽은 긴 레이턴시를 허용하지 않습니다. QoS(Quality of Service)는 중요한 트래픽에 우선 순위를 두고, 대역폭 과다 사용을 막고, 패킷 삭제를 방지하기 위해 네트워크 병목을 관리하는 기능입니다.

참고 ASASM의 경우 스위치에서 ASASM 대신 QoS를 수행하는 것이 좋습니다. 이 영역에서는 스위치의 기능이 더 풍부합니다. 일반적으로 QoS는 네트워크의 라우터와 스위치에서 가장 뛰어나며, ASA보다 기능이 훨씬 광범위한 경향이 있습니다.

이 장에서는 QoS 정책을 적용하는 방법에 대해 설명합니다.

QoS 소개

끊임없이 변화하는 네트워크 환경에서 QoS는 일회 배포로 끝나는 것이 아니라 네트워크 설계에서 지속적으로 이루어지는 필수적인 부분이라는 점을 고려해야 합니다.

이 섹션에서는 ASA에서 사용 가능한 QoS 기능에 대해 설명합니다.

지원되는 QoS 기능

ASA에서는 다음 QoS 기능을 지원합니다.

- 폴리싱 - 분류된 트래픽의 네트워크 대역폭 과다 사용을 막기 위해 클래스당 사용되는 최대 대역폭을 제한할 수 있습니다. 자세한 내용은 13-2 페이지의 폴리싱 섹션을 참조하십시오.
- 우선 순위 큐잉 - VoIP(Voice over IP)와 같이 레이턴시가 허용되지 않는 중요한 트래픽의 경우, 다른 트래픽보다 항상 먼저 전송되도록 LLQ(Low Latency Queuing)에 대한 트래픽을 식별할 수 있습니다. 13-3 페이지의 우선 순위 큐잉 섹션을 참조하십시오.

토큰 버킷이란?

토큰 버킷은 트래픽 폴리서와 같은 흐름에서 데이터를 규제하는 디바이스를 관리하는 데 사용됩니다. 토큰 버킷 자체에는 폐기 또는 우선 순위 정책이 없습니다. 대신 조절기에서 흐름이 과도하게 이루어지는 경우 토큰 버킷은 토큰을 폐기하고 전송 큐 관리의 문제를 흐름에 맡깁니다.

토큰 버킷은 전송 속도의 공식적인 정의로서 버스트 크기, 평균 속도 및 시간 간격의 세 가지 구성 요소로 이루어집니다. 평균 속도는 일반적으로 초당 비트 수로 표시되지만, 다음과 같은 관계에 의해 두 개의 값이 세 번째로부터 파생될 수 있습니다.

평균 크기 = 버스트 크기/시간 간격

일부 용어 정의는 다음과 같습니다.

- 평균 속도 - CIR(Committed Information Rate)이라고도 하며, 평균적으로 단위 시간당 전송 또는 전달 가능한 데이터의 양을 지정합니다.
- 버스트 크기 - Committed Burst라고도 하며, 일정 문제를 일으키지 않고 지정된 시간 단위 내에 전송할 수 있는 데이터의 양을 버스트당 바이트 단위로 지정합니다.
- 시간 간격 - 측정 간격이라고도 하며, 버스트당 초 단위로 시간의 양을 지정합니다.

토큰 버킷이라는 은유에서 알 수 있듯이 토큰이 일정한 속도로 버킷에 담깁니다. 버킷 자체에는 지정된 용량이 있습니다. 버킷의 용량이 차면 새로 도착하는 토큰은 폐기됩니다. 각 토큰은 소스에서 네트워크로 일정한 수의 비트를 전송하도록 허용하는 것입니다. 패킷 하나를 전송하려면 조절기는 해당 패킷 크기에 대해 표시된 것과 동등한 수의 토큰을 버킷에서 제거해야 합니다.

버킷에 패킷을 전송할 수 있을 만큼 충분한 토큰이 없으면 폐기 또는 하락할 때까지 패킷이 대기합니다. 버킷이 이미 토큰으로 가득 차 있으면 들어오는 토큰은 오버플로되어 향후 패킷에 사용할 수 없게 됩니다. 따라서 언제든지 소스가 네트워크로 전송할 수 있는 최대 버스트는 버킷의 크기와 거의 비례합니다.

폴리싱

폴리싱은 어떠한 트래픽도 사용자가 구성한 최대 속도(비트/초 단위)를 초과하지 못하게 함으로써 하나의 트래픽 클래스가 전체 리소스를 차지할 수 없도록 하는 방법입니다. 트래픽이 최대 속도를 초과하면 ASA에서 초과 트래픽을 취소합니다. 또한 폴리싱은 허용되는 최대 단일 트래픽 버스트를 설정합니다.

우선 순위 큐잉

LLQ 우선 순위 큐잉은 다른 트래픽에 앞서 특정 트래픽 흐름(예: 음성과 비디오 등 레이턴시에 민감한 트래픽)에 우선 순위를 지정하도록 허용합니다. 우선 순위 큐잉은 인터페이스에서 LLQ 우선 순위 큐를 사용하는 반면(13-6 페이지의 인터페이스에 대한 우선 순위 큐 구성 참조), 다른 모든 트래픽은 "BE(Best Effort)" 큐로 이동합니다. 큐의 크기는 무한하지 않으므로 가득 차서 오버플로될 수 있습니다. 큐가 가득 차면 해당 큐로 추가 패킷이 들어갈 수 없어 삭제됩니다. 이를 *tail drop*이라고 합니다. 큐가 가득 차는 것을 막으려면 큐 버퍼 크기를 늘릴 수 있습니다. 또한 전송 큐에 대해 허용되는 패킷의 최대 수를 조정할 수 있습니다. 이러한 옵션을 통해 우선 순위 큐잉의 레이턴시와 안정성을 제어할 수 있습니다. LLQ 큐에 있는 패킷은 항상 BE 큐에 있는 패킷보다 먼저 전송됩니다.

QoS 기능의 상호 작용 방식

ASA에서 필요한 경우 QoS의 각 기능을 따로 구성할 수 있습니다. 그러나 예를 들면 일부 트래픽의 우선 순위를 정하고 다른 트래픽이 대역폭 문제를 일으키지 못하도록 종종 ASA에서 여러 QoS 기능을 구성하기도 합니다. 다음을 구성할 수 있습니다.

우선 순위 큐잉(특정 트래픽용) + 폴리싱(나머지 트래픽용).

동일한 트래픽 집합에 대해서는 우선 순위 큐잉과 폴리싱을 구성할 수 없습니다.

DSCP(DiffServ) 보존

DSCP(DiffServ) 표시는 ASA를 통과하는 모든 트래픽에서 유지됩니다. ASA는 분류된 트래픽을 로컬로 표시하지 않습니다. 예를 들면, "우선 순위" 처리가 필요한지 확인하기 위해 각 패킷의 EF(Expedited Forwarding) DSCP 비트를 키오프(key off)하고 ASA에서 해당 패킷을 LLQ로 보내도록 지정할 수 있습니다.

QoS 지침

컨텍스트 모드 지침

단일 컨텍스트 모드에서만 지원됩니다. 다중 컨텍스트 모드는 지원되지 않습니다.

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

IPv6 지침

IPv6은 지원되지 않습니다.

모델 지침

- (ASA 5512-X~ASA 5555-X) 우선 순위 큐잉은 관리 0/0 인터페이스에서 지원되지 않습니다.
- (ASASM) 폴리싱만 지원됩니다.

추가 지침 및 제한

- QoS는 단방향으로 적용됩니다. 정책 맵을 적용하는 인터페이스로 들어가는 트래픽(또는 나가는 트래픽 - QoS 기능에 따라 다름)만 영향을 받습니다. 자세한 내용은 1-4 페이지의 기능 방향성 섹션을 참조하십시오.
- 우선 순위 트래픽에는 **class-default** 클래스 맵을 사용할 수 없습니다.
- 우선 순위 큐잉의 경우 물리적 인터페이스(또는 ASASM의 경우 VLAN)에 대해 우선 순위 큐를 구성해야 합니다.
- 폴리싱의 경우 to-the-box 트래픽은 지원되지 않습니다.
- 폴리싱의 경우 VPN 터널을 지나는 트래픽은 인터페이스 폴리싱을 우회합니다.
- 폴리싱의 경우 터널 그룹 클래스 맵을 일치시키면 아웃바운드 폴리싱만 지원됩니다.

QoS 구성

ASA에서 QoS를 구현하려면 다음 순서를 사용하십시오.

1단계 13-4 페이지의 우선 순위 큐에 대해 큐 및 TX 링 제한 결정

2단계 13-6 페이지의 인터페이스에 대한 우선 순위 큐 구성

3단계 13-7 페이지의 우선 순위 큐잉 및 폴리싱에 대한 서비스 규칙 구성

우선 순위 큐에 대해 큐 및 TX 링 제한 결정

우선 순위 큐 및 TX 링 제한을 결정하려면 다음 워크시트를 사용하십시오.

- 13-4 페이지의 큐 제한 워크시트
- 13-5 페이지의 TX 링 제한 워크시트

큐 제한 워크시트

다음 워크시트에서는 우선 순위 큐 크기를 계산하는 방법을 보여줍니다. 큐의 크기는 무한하지 않으므로 가득 차서 오버플로될 수 있습니다. 큐가 가득 차면 해당 큐로 추가 패킷이 들어갈 수 없어 삭제됩니다(*tail drop*이라고 함). 큐가 가득 차는 것을 막으려면 13-6 페이지의 인터페이스에 대한 우선 순위 큐 구성에 따라 버퍼 크기를 조정할 수 있습니다.

워크시트에 대한 팁:

- 아웃바운드 대역폭 - 예를 들어 DSL은 768Kbps의 업링크 속도를 사용할 수 있습니다. 공급업체에 문의하십시오.
- 평균 패킷 크기 - 코덱 또는 샘플링 크기에서 이 값을 결정합니다. 예를 들면 VoIP over VPN에 160바이트를 사용할 수 있습니다. 사용해야 할 크기를 잘 모르는 경우 256바이트를 권장합니다.
- 지연 - 지연은 애플리케이션에 따라 다릅니다. 예를 들어, VoIP의 최대 권장 지연은 200ms입니다. 사용해야 할 지연 값을 잘 모르는 경우 500ms를 권장합니다.

표 13-1 큐 제한 워크시트

1	_____ *아웃바운드 대역폭(Mbps 또는 Kbps)*	Mbps	x **125**	=	_____ *바이트/ms #*			
		Kbps	x **.125**	=	_____ *바이트/ms #*			
2	_____ *1 단계의 바이트/ms #*	÷	_____ *평균 패킷 크기(바이트)*	x	_____ *지연(ms)*	=	_____ *큐 제한(패킷의 #)*	

TX 링 제한 워크시트

다음 워크시트에서는 TX 링 제한을 계산하는 방법을 보여줍니다. 이러한 제한은 혼잡이 해소되기까지 패킷을 버퍼링할 수 있도록 드라이버가 인터페이스의 큐로 다시 보내기 전에 이더넷 전송 드라이버에 대해 허용되는 패킷의 최대 수를 결정합니다. 이 설정은 하드웨어 기반 전송 링이 우선 순위가 높은 패킷에 대해 추가 레이턴시를 제한된 양만큼만 부과하도록 보장합니다.

워크시트에 대한 팁:

- 아웃바운드 대역폭 - 예를 들어 DSL은 768Kbps의 업링크 속도를 사용할 수 있습니다. 공급업체에 문의하십시오.
- 최대 패킷 크기 - 일반적으로 태그가 지정된 이더넷에 대한 최대 크기는 1538바이트 또는 1542바이트입니다. 점보 프레임(플랫폼에서 지원되는 경우)을 허용하는 경우에는 패킷 크기가 더 클 수 있습니다.
- 지연 - 지연은 애플리케이션에 따라 다릅니다. 예를 들어, VoIP용 지터를 제어하려면 20ms를 사용해야 합니다.

표 13-2 TX 링 제한 워크시트

1	_____ *아웃바운드 대역폭(Mbps 또는 Kbps)*	Mbps	x **125**	=	_____ *바이트/ms #*			
		Kbps	x **0.125**	=	_____ *바이트/ms #*			
2	_____ *1 단계의 바이트/ms #*	÷	_____ *최대 패킷 크기(바이트)*	x	_____ *지연(ms)*	=	_____ *TX 링 제한(패킷의 #)*	

인터페이스에 대한 우선 순위 큐 구성

물리적 인터페이스에서 트래픽에 대해 우선 순위 큐를 활성화하는 경우 각 인터페이스에서 우선 순위 큐를 생성해야 합니다. 각 물리적 인터페이스는 2개의 큐, 즉 우선 순위 트래픽에 하나, 다른 모든 트래픽에 하나를 사용합니다. 다른 트래픽에 대해서는 폴리싱을 선택적으로 구성할 수 있습니다.

시작하기 전에

- (ASASM) ASASM은 우선 순위 큐잉을 지원하지 않습니다.
- (ASA 5512-X~ASA 5555-X) 우선 순위 큐잉은 관리 0/0 인터페이스에서 지원되지 않습니다.

절차

1단계 인터페이스에 대한 우선 순위 큐를 만듭니다.

priority-queue *interface_name*

예:

```
hostname(config)# priority-queue inside
```

interface_name 인수는 우선 순위 큐를 활성화할 물리적 인터페이스 이름(또는 ASASM의 경우 VLAN 인터페이스 이름)을 지정합니다.

2단계 우선 순위 큐의 크기를 변경합니다.

queue-limit *number_of_packets*

예:

```
hostname(config-priority-queue)# queue-limit 260
```

queue-limit 기본값은 1024패킷입니다. 큐의 크기는 무한하지 않으므로 가득 차서 오버플로될 수 있습니다. 큐가 가득 차면 해당 큐로 추가 패킷이 들어갈 수 없어 삭제됩니다(*tail drop*이라고 함). 큐가 가득 차는 것을 막으려면 **queue-limit** 명령을 사용하여 큐 버퍼 크기를 늘릴 수 있습니다.

queue-limit 명령에 대한 값 범위의 상한은 런타임에 동적으로 결정됩니다. 이 제한을 보려면 명령줄 **queue-limit ?** 명령을 입력합니다. 주요 결정 요인은 큐 지원에 필요한 메모리 및 디바이스에서 사용 가능한 메모리입니다.

지정하는 **queue-limit**은 우선 순위가 더 높은 LLQ(Low-Latency Queue) 및 BE(Best Effort) 큐 모두에 영향을 미칩니다.

3단계 우선 순위 큐의 깊이를 지정합니다.

tx-ring-limit *number_of_packets*

예:

```
hostname(config-priority-queue)# tx-ring-limit 3
```

tx-ring-limit 기본값은 128패킷입니다. 이 명령은 혼잡이 해소되기까지 패킷을 버퍼링할 수 있도록 드라이버가 인터페이스의 큐로 다시 보내기 전에 이더넷 전송 드라이버에 대해 허용되는 짧은 레이턴시 또는 일반 우선 순위 패킷의 최대 수를 설정합니다. 이 설정은 하드웨어 기반 전송 링이 우선 순위가 높은 패킷에 대해 추가 레이턴시를 제한된 양만큼만 부과하도록 보장합니다.

tx-ring-limit 명령에 대한 값 범위의 상한은 런타임에 동적으로 결정됩니다. 이 제한을 보려면 명령줄에 **tx-ring-limit ?** 명령을 입력합니다. 주요 결정 요인은 큐 지원에 필요한 메모리 및 디바이스에서 사용 가능한 메모리입니다.

지정하는 **tx-ring-limit**은 우선 순위가 더 높은 LLQ 및 BE 큐 모두에 영향을 미칩니다.

예

다음 예에서는 queue-limit 및 tx-ring-limit 기본값으로 인터페이스 "outside"(GigabitEthernet0/1 인터페이스)에 우선 순위 큐를 지정합니다.

```
hostname(config)# priority-queue outside
```

다음 예에서는 인터페이스 "outside"(GigabitEthernet0/1 인터페이스)에 우선 순위 큐를 지정하고, queue-limit을 260패킷으로, tx-ring-limit을 3으로 설정합니다.

```
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 260
hostname(config-priority-queue)# tx-ring-limit 3
```

우선 순위 큐잉 및 폴리싱에 대한 서비스 규칙 구성

동일한 정책 맵 내의 여러 클래스 맵에 대해 우선 순위 큐잉 및 폴리싱을 구성할 수 있습니다. 유효한 QoS 컨피그레이션에 대한 자세한 내용은 13-3 페이지의 QoS 기능의 상호 작용 방식을 참조하십시오.

시작하기 전에

- 우선 순위 트래픽에는 **class-default** 클래스 맵을 사용할 수 없습니다.
- (ASASM) ASASM은 폴리싱만 지원합니다.
- 폴리싱의 경우 to-the-box 트래픽은 지원되지 않습니다.
- 폴리싱의 경우 VPN 터널을 지나는 트래픽은 인터페이스 폴리싱을 우회합니다.
- 폴리싱의 경우 터널 그룹 클래스 맵을 일치시키면 아웃바운드 폴리싱만 지원됩니다.
- 우선 순위 트래픽의 경우 레이턴시 감지 트래픽만 식별합니다.
- 폴리싱 트래픽의 경우 다른 모든 트래픽을 폴리싱할 수도 있고, 트래픽을 특정 유형으로 제한할 수도 있습니다.

절차

1단계 우선 순위 큐잉을 수행할 트래픽을 식별하기 위한 클래스 맵을 만듭니다.

class-map *priority_map_name*

예:

```
hostname(config)# class-map priority_traffic
```

2단계 클래스 맵에서 트래픽을 지정합니다.

match *parameter*

예:

```
hostname(config-cmap)# match access-list priority
```

자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵) 섹션을 참조하십시오.

3단계 폴리싱을 수행할 트래픽을 식별하기 위한 클래스 맵을 만듭니다.

class-map *policing_map_name*

예:

```
hostname(config)# class-map policing_traffic
```

4단계 클래스 맵에서 트래픽을 지정합니다.

match *parameter*

예:

```
hostname(config-cmap)# match access-list policing
```

자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵) 섹션을 참조하십시오.

팁 트래픽 매칭을 위해 ACL을 사용하는 경우 ACL에 지정된 방향으로만 폴리싱이 적용됩니다. 즉, 소스에서 대상으로 가는 트래픽만 폴리싱되며, 그 역방향은 해당되지 않습니다.

5단계 정책 맵을 추가 또는 편집합니다.

policy-map *name*

예:

```
hostname(config)# policy-map QoS_policy
```

6단계 우선 순위가 지정된 트래픽에 대해 생성한 클래스 맵을 식별합니다.

class *priority_map_name*

예:

```
hostname(config-pmap)# class priority_class
```

7단계 클래스에 대한 우선 순위 큐잉을 구성합니다.

priority

예:

```
hostname(config-pmap-c)# priority
```

8단계 폴리싱된 트래픽에 대해 생성한 클래스 맵을 식별합니다.

class *policing_map_name*

예:

```
hostname(config-pmap)# class policing_class
```

9단계 클래스에 대한 폴리싱을 구성합니다.

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**]] [**exceed-action** [**drop** | **transmit**]]

예:

```
hostname(config-pmap-c)# police output 56000 10500
```

옵션은 다음과 같습니다.

- *conform-burst 인수* - 준수 속도 값으로 조정되기 전 지속적인 버스트에서 허용되는 순간 바이트의 최대 수를 지정합니다(1000~512000000바이트).
- **conform-action** - 속도가 *conform_burst* 값보다 낮을 때 수행할 작업을 설정합니다.
- *conform-rate* - 이 트래픽 클래스에 대한 속도 제한을 설정합니다(초당 8000~2000000000비트).
- **drop** - 패킷을 삭제합니다.

- **exceed-action** - 속도가 *conform-rate* 값과 *conform-burst* 값 사이인 경우 수행할 작업을 설정합니다.
- **input** - 입력 방향으로 흐르는 트래픽의 폴리싱을 활성화합니다.
- **output** - 출력 방향으로 흐르는 트래픽의 폴리싱을 활성화합니다.
- **transmit** - 패킷을 전송합니다.

10단계 하나 이상의 인터페이스에서 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

```
hostname(config)# service-policy QoS_policy interface inside
```

global 옵션은 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

QoS 모니터링

QoS 폴리스 통계

트래픽 폴리싱에 대한 QoS 통계를 보려면 **show service-policy police** 명령을 사용합니다.

```
hostname# show service-policy police

Global policy:
    Service-policy: global_fw_policy

Interface outside:
    Service-policy: qos
        Class-map: browse
            police Interface outside:
                cir 56000 bps, bc 10500 bytes
                conformed 10065 packets, 12621510 bytes; actions: transmit
                exceeded 499 packets, 625146 bytes; actions: drop
                conformed 5600 bps, exceed 5016 bps
        Class-map: cmap2
            police Interface outside:
                cir 200000 bps, bc 37500 bytes
                conformed 17179 packets, 20614800 bytes; actions: transmit
                exceeded 617 packets, 770718 bytes; actions: drop
                conformed 198785 bps, exceed 2303 bps
```

QoS 우선 순위 통계

priority 명령을 구현하는 서비스 정책의 통계를 보려면 **show service-policy priority** 명령을 사용합니다.

```
hostname# show service-policy priority
Global policy:
    Service-policy: global_fw_policy
Interface outside:
    Service-policy: qos
        Class-map: TG1-voice
            Priority:
                Interface outside: aggregate drop 0, aggregate transmit 9383
```

"Aggregate drop"은 이 인터페이스에서 집계된 삭제를 나타내고, "aggregate transmit"은 이 인터페이스에서 전송된 패킷의 집계된 수를 나타냅니다.

QoS 우선 순위 큐 통계

인터페이스에 대한 우선 순위 큐 통계를 표시하려면 **show priority-queue statistics** 명령을 사용합니다. BE(Best Effort) 큐 및 LLQ(Low Latency Queuing) 모두에 대한 통계가 결과로 표시됩니다. 다음 예는 인터페이스 명명 테스트를 위한 **show priority-queue statistics** 명령의 사용법을 보여줍니다.

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
hostname#
```

이 통계 보고서에서

- "Packets Dropped"는 이 큐에서 삭제된 패킷의 전체 수를 나타냅니다.
- "Packets Transmit"은 이 큐에서 전송된 패킷의 전체 수를 나타냅니다.
- "Packets Enqueued"는 이 큐에 추가된 패킷의 전체 수를 나타냅니다.
- "Current Q Length"는 이 큐의 현재 깊이를 나타냅니다.
- "Max Q Length"는 이 큐에서 발생한 최대 깊이를 나타냅니다.

우선 순위 큐잉 및 폴리싱의 컨피그레이션 예

다음 섹션에서는 우선 순위 큐잉 및 폴리싱을 구성하는 예를 제공합니다.

VPN 트래픽에 대한 클래스 맵 예

다음 예에서 **class-map** 명령은 tcp_traffic이라는 이름의 ACL을 사용하여 모든 비 터널링 TCP 트래픽을 분류합니다.

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

다음 예에서는 보안 관련 특정 터널 그룹에 대한 트래픽을 분류하기 위해 좀 더 구체적인 일치 기준이 사용됩니다. 이러한 구체적인 일치 기준은 특정 터널에 대한 트래픽을 분류하는 첫 번째 일치 특성으로서 터널 그룹(이 경우 전에 정의한 Tunnel-Group-1)에 대한 일치가 필요하다고 규정하며, 트래픽(IP 차등 서비스 코드 포인트, 빠른 전달) 분류를 위한 추가 일치 라인을 허용합니다.

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

다음 예에서 **class-map** 명령은 트래픽 유형에 따라 터널링 및 비 터널링 트래픽을 모두 분류합니다.

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

다음 예에서는, 분류된 트래픽이 터널로 지정되지 않았지만 터널을 *통과하는* 경우 터널 내에서 트래픽을 폴리싱하는 방법을 보여줍니다. 이 예에서 192.168.10.10은 원격 터널의 비공개 부분에 있는 호스트 시스템의 주소이며, ACL 이름은 "host-over-l2l"입니다. "host-specific"이라는 이름의 클래스 맵을 만든 후, LAN-to-LAN 연결이 터널을 폴리싱하기 전에 "host-specific" 클래스를 폴리싱할 수 있습니다. 이 예에서는 "host-specific" 트래픽의 속도가 터널보다 먼저 제한되고, 그런 다음 터널의 속도가 제한됩니다.

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

우선 순위 및 폴리싱의 예

다음 예는 이전 섹션에서 만든 컨피그레이션을 기반으로 합니다. 이전 예와 마찬가지로 두 개의 명명된 클래스 맵, 즉 tcp_traffic 및 TG1-voice가 있습니다.

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

세 번째 클래스 맵을 추가하면 다음과 같이 터널링 및 비 터널링 QoS 정책을 정의하기 위한 기반이 제공됩니다. 이를 통해 터널링 및 비 터널링 트래픽에 대한 간단한 QoS 정책이 생성되며, 클래스 TG1-voice의 패킷이 짧은 레이턴시 큐에 할당되고 tcp_traffic 및 TG1-best-effort 트래픽 흐름에 대한 속도 제한이 설정됩니다.

이 예제에서 tcp_traffic 클래스의 트래픽에 대한 최대 속도는 56,000비트/초이며 최대 버스트 크기는 10,500바이트/초입니다. TC1-BestEffort 클래스의 경우 최대 속도는 200,000비트/초이며 최대 버스트 크기는 37,500바이트/초입니다. TC1-voice 클래스는 우선 순위 클래스에 속하기 때문에 해당 트래픽에는 폴리싱된 최대 속도 또는 버스트 속도가 없습니다.

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

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

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos global
```

QoS의 기록

기능 이름	플랫폼 릴리스	설명
우선 순위 큐잉 및 폴리싱	7.0(1)	QoS 우선 순위 큐잉 및 폴리싱을 추가했습니다. 추가된 명령: **priority-queue**, **queue-limit**, **tx-ring-limit**, **priority, police, show priority-queue statistics, show service-policy police, show service-policy priority, show running-config priority-queue, clear configure priority-queue** .
셰이핑 및 계층적 우선 순위 큐잉	7.2(4)/8.0(4)	QoS 셰이핑 및 계층적 우선 순위 큐잉을 추가했습니다. 추가된 명령: **shape**, **show service-policy shape**.
ASA 5585-X에서 표준 우선 순위 큐를 위한 10기가비트 이더넷 지원	8.2(3)/8.4(1)	ASA 5585-X용 10기가비트 이더넷 인터페이스에서 표준 우선 순위 큐 지원을 추가했습니다.

14 장

연결 및 리소스 문제 해결

이 장에서는 ASA의 문제를 해결하는 방법에 대해 설명합니다.

컨피그레이션 테스트

이 섹션에서는 단일 모드 ASA 또는 각 보안 컨텍스트에 대한 연결을 테스트하는 방법, ASA 인터페이스를 ping하는 방법, 한 인터페이스의 호스트에서 다른 인터페이스의 호스트로 ping하도록 허용하는 방법에 대해 설명합니다.

문제 해결 중에는 ping 및 디버깅 메시지만 활성화하는 것이 좋습니다. ASA 테스트를 완료하면 14-5 페이지의 테스트 컨피그레이션 비활성화의 단계를 따르십시오.

ICMP 디버깅 메시지 및 Syslog 메시지 활성화

디버깅 메시지 및 syslog 메시지는 ping이 실패하는 이유를 파악하여 문제를 해결하는 데 도움이 됩니다. ASA는 ICMP 디버깅 메시지를 ASA 인터페이스 대상 ping에 대해서만 표시하고, ASA를 통한 다른 호스트 대상 ping에 대해서는 표시하지 않습니다.

디버깅 및 syslog 메시지를 활성화하려면 다음 단계를 수행하십시오.

	명령	목적

1단계	`debug icmp trace`
	
	예:
	`hostname(config)# debug icmp trace`
		ASA 인터페이스 대상 ping에 대한 ICMP 패킷 정보를 표시합니다.

2단계	**logging monitor debug** **예:** hostname(config)# logging monitor debug	텔넷 또는 SSH 세션에 보낼 syslog 메시지를 설정합니다. **참고** 또는 **logging buffer debug** 명령을 사용하여 로그 메시지를 버퍼로 보낸 다음 나중에 **show logging** 명령을 사용하여 볼 수도 있습니다.
3단계	**terminal monitor** **예:** hostname(config)# terminal monitor	텔넷 또는 SSH 세션으로 syslog 메시지를 보냅니다.
4단계	**logging on** **예:** hostname(config)# logging on	syslog 메시지 생성을 활성화합니다.

예

다음 예는 외부 호스트(209.165.201.2)에서 ASA 외부 인터페이스(209.165.201.1)에 대해 성공적으로 수행한 ping을 보여줍니다.

```
hostname(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

출력에는 ICMP 패킷 길이(32바이트), ICMP 패킷 식별자(1) 및 ICMP 시퀀스 번호가 표시됩니다. ICMP 시퀀스 번호는 0에서 시작하여 요청이 전송될 때마다 증가합니다.

ASA 인터페이스 ping하기

ASA 인터페이스가 운영 중인지, ASA 및 연결된 라우터가 올바르게 작동하는지 테스트하려면 ASA 인터페이스를 ping할 수 있습니다.

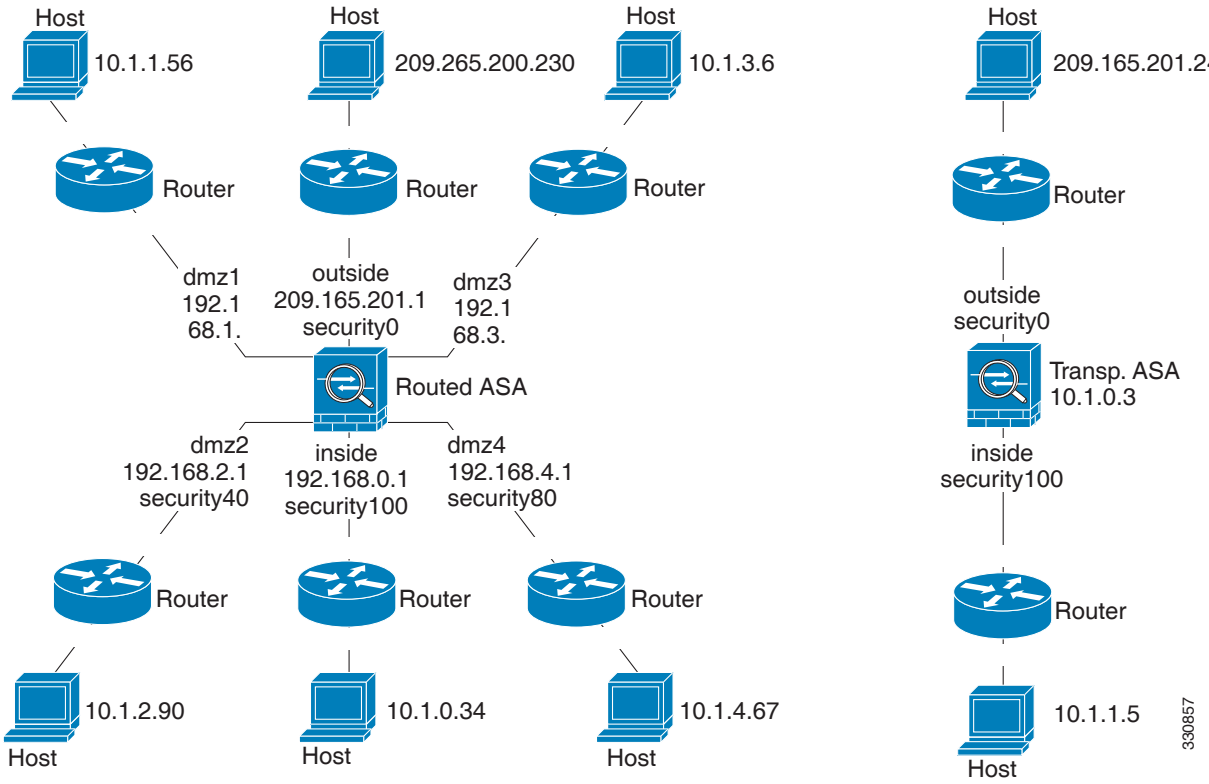
ASA 인터페이스를 ping하려면 다음 단계를 수행하십시오.

1단계 인터페이스 이름, 보안 수준 및 IP 주소를 보여주는 단일 모드 ASA 또는 보안 컨텍스트의 다이어그램을 그립니다.

참고 이 절차에서는 IP 주소를 사용하지만, **ping** 명령에서는 DNS 이름은 물론 **name** 명령으로 로컬 IP 주소에 할당한 이름도 지원됩니다.

다이어그램에는 직접 연결된 라우터 및 ASA를 ping할 라우터의 다른 쪽에 있는 호스트도 포함되어 있습니다. 이 절차 및 14-4 페이지의 ASA를 통해 트래픽 전달의 절차에서 이 정보를 사용합니다. (그림 14-1 참조.)

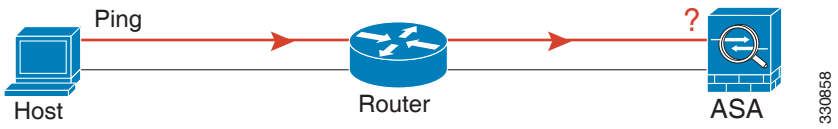
그림 14-1 인터페이스, 라우터 및 호스트가 포함된 네트워크 다이어그램



2단계 직접 연결된 라우터에서 각 ASA 인터페이스를 ping합니다. 투명 모드의 경우 관리 IP 주소를 ping합니다. 이 테스트에서는 ASA 인터페이스가 활성 상태인지, 인터페이스 컨피그레이션이 올바른지 확인합니다.

ASA 인터페이스가 활성 상태가 아니거나, 인터페이스 컨피그레이션이 올바르지 않거나, ASA와 라우터 간 스위치가 다운된 경우 ping이 실패할 수 있습니다(그림 14-2 참조). 이 경우 패킷이 ASA에 도달하지 않기 때문에 디버깅 메시지 또는 syslog 메시지가 표시되지 않습니다.

그림 14-2 ASA 인터페이스에서 Ping 실패

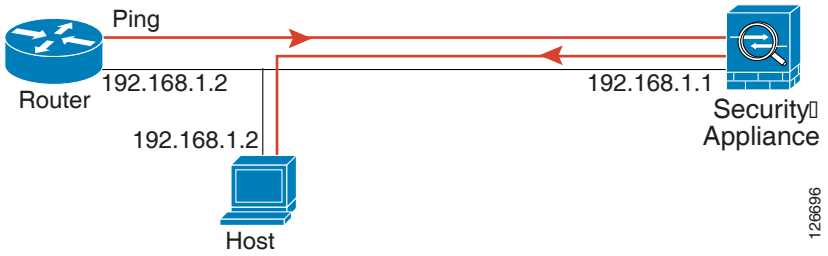


Ping이 ASA에 도달하고 응답이 수신되면 다음과 유사한 디버깅 메시지가 나타납니다.

```
ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
```

Ping 응답이 라우터로 반환되지 않으면 스위치 루프 또는 중복 IP 주소가 존재하는 것일 수 있습니다(그림 14-3 참조).

그림 14-3 IP 주소 지정 문제 때문에 Ping 실패



3단계 원격 호스트에서 각 ASA 인터페이스를 ping합니다. 투명 모드의 경우 관리 IP 주소를 ping합니다. 이 테스트에서는 직접 연결된 라우터가 호스트 및 ASA 간에 패킷을 라우팅할 수 있는지, ASA가 패킷을 정확하게 호스트로 다시 라우팅할 수 있는지 확인합니다.

ASA에 중간 라우터를 통해 호스트로 반환하는 경로가 없으면 ping이 실패할 수 있습니다(그림 14-4 참조). 이 경우 디버깅 메시지에는 ping이 성공한 것으로 표시되지만, 라우팅이 실패했음을 나타내는 syslog 메시지 110001이 표시됩니다.

그림 14-4 ASA에 반환 경로가 없기 때문에 Ping 실패

ASA를 통해 트래픽 전달

ASA 인터페이스를 성공적으로 ping한 후에는 트래픽이 ASA를 성공적으로 통과할 수 있는지 확인합니다. 기본적으로 높은 보안 인터페이스에서 낮은 보안 인터페이스로 ping할 수 있습니다. 반환 트래픽 통과를 허용하려면 ICMP 검사를 활성화해야 합니다. 높은 곳에서 낮은 곳으로 ping하려면 트래픽을 허용하는 ACL을 적용해야 합니다. NAT를 사용하는 경우 이 테스트에서는 NAT가 올바르게 작동하고 있음을 표시합니다.

호스트나 라우터에서 소스 인터페이스를 통해 다른 인터페이스의 다른 호스트나 라우터로 ping합니다. 확인하고 싶은 만큼의 인터페이스 쌍에 대해 이 단계를 반복합니다.

Ping이 성공할 경우, syslog 메시지가 나타나서 라우팅된 모드의 주소 변환을 확인하고(305009 또는 305011), ICMP 연결이 설정되었는지를 확인합니다(302020). 이 정보를 보려면 **show xlate** 또는 **show conns** 명령을 입력할 수도 있습니다.

NAT가 올바르게 구성되지 않으면 ping이 실패할 수 있습니다. 이 경우 NAT가 실패했음을 알리는 syslog 메시지가 표시됩니다(305005 또는 305006). 외부 호스트에서 내부 호스트로 ping하는 경우 고정 변환이 없으면 다음과 같은 syslog 메시지가 표시됩니다.

```
%ASA-3-106010: deny inbound icmp.
```

참고 ASA는 ICMP 디버깅 메시지를 ASA 인터페이스 대상 ping에 대해서만 표시하고, ASA를 통한 다른 호스트 대상 ping에 대해서는 표시하지 않습니다.

그림 14-5 ASA에서 주소를 변환하지 않기 때문에 Ping 실패

자세한 단계

	명령	목적
1단계	`policy-map global_policy`	기본 글로벌 정책을 편집하고 policy-map 컨피그레이션 모드로 들어갑니다.
2단계	`class inspection_default`	표준 프로토콜 및 포트에 대한 애플리케이션 트래픽과 일치하는 기본 클래스 맵을 편집합니다. ICMP의 경우 이 클래스는 모든 ICMP 트래픽과 일치합니다.
3단계	`inspect icmp`	ICMP 검사 엔진을 활성화하고 ICMP 응답이 소스 호스트로 반환되도록 합니다.
4단계	(보안이 낮은 인터페이스에 대해 선택적으로) `access-list ICMPACL extended permit icmp any any`	모든 소스 호스트의 ICMP 트래픽을 허용하기 위해 ACL을 추가합니다.
5단계	`access-group ICMPACL in interface outside`	외부 인터페이스에 ACL을 할당합니다. 이름이 다른 경우 "outside"를 해당 인터페이스 이름으로 바꾸십시오. 높은 곳에서 낮은 곳으로 ICMP 트래픽을 허용하려는 각 인터페이스에 대해 이 명령을 반복합니다. **참고** 가장 낮은 보안 인터페이스가 아닌 인터페이스에 이 ACL을 적용하면 ICMP 트래픽만 허용되고 높은 곳에서 낮은 곳으로의 암시적 허용이 제거됩니다. 예를 들어, DMZ 인터페이스(레벨 50)가 내부 인터페이스(레벨 100)를 ping하도록 허용하려면 이 ACL을 적용해야 합니다. 전에는 모든 트래픽이 암시적으로 허용되었지만 이제 DMZ에서 외부로의 트래픽(레벨 0)이 ICMP 트래픽으로만 제한됩니다. Ping 테스트가 완료되면 인터페이스, 특히 암시적 허용을 복원하려는 인터페이스에서 이 ACL을 제거해야 합니다(**no access-list ICMPACL**).

테스트 컨피그레이션 비활성화

테스트를 완료한 후에는 테스트 컨피그레이션을 비활성화하여, ICMP가 ASA를 통과하지 못하게 하고 디버깅 메시지가 인쇄되지 않도록 해야 합니다. 이 컨피그레이션을 그대로 두면 심각한 보안 위험이 발생할 수 있습니다. 또한 디버깅 메시지는 ASA의 성능을 저하시킵니다.

테스트 컨피그레이션을 비활성화하려면 다음 단계를 수행하십시오.

	명령	목적
1단계	`no debug icmp trace`	Disables ICMP debugging messages.
2단계	`no logging on`	Disables logging.
3단계	`no access-list ICMPACL`	ICMPACL ACL을 제거하고 관련 **access-group** 명령을 삭제합니다.

4단계	`policy-map global_policy`
	`  class inspection_default`
	`  no inspect icmp`
		(선택 사항) ICMP 검사 엔진을 비활성화합니다.

Traceroute로 패킷 라우팅 확인

Traceroute 기능을 사용하여 패킷의 경로를 추적할 수 있습니다(**traceroute** 명령으로 액세스). Traceroute는 잘못된 포트의 목적지로 UDP 패킷을 전송하는 방식으로 작동합니다. 포트가 유효하지 않기 때문에, 목적지로 가는 동안 라우터는 ICMP Time Exceeded Message로 응답하고 ASA에 오류를 보고합니다.

패킷 추적기를 이용해 패킷 추적

패킷 추적기 툴은 패킷 검사 및 네트워크 결함 분리를 위한 패킷 추적 기능은 물론, 패킷 및 ASA에서 패킷이 처리되는 방법에 대한 자세한 정보를 제공합니다. 컨피그레이션 명령으로 인해 패킷이 누락되지 않은 경우 패킷 추적기 툴은 원인에 대한 정보를 읽기 쉬운 형식으로 제공합니다.

패킷 추적기 툴을 사용하여 다음과 같은 작업을 수행할 수 있습니다.

- 패킷이 올바르게 작동하는지 확인하기 위해 ASA를 통해 패킷의 수명을 추적합니다.
- 프로덕션 네트워크의 모든 패킷 삭제를 디버깅합니다.
- 컨피그레이션이 예상대로 작동하는지 확인합니다.
- 규칙 추가를 일으킨 CLI 명령과 함께 패킷에 적용되는 모든 규칙을 표시합니다.
- 데이터 경로에 있는 패킷 변경의 타임라인을 표시합니다.
- 추적기 패킷을 데이터 경로에 삽입합니다.
- 사용자 ID 및 FQDN을 기반으로 IPv4 또는 IPv6 주소를 검색합니다.
- 특정 세션의 허용 또는 거부 이유를 디버깅합니다.
- 인터페이스에 구성된 **policy static sgt** 명령, 패킷의 SGT, IP-SGT Manager 등에서 사용되고 있는 SGT(Security Group Tag) 값을 확인합니다.
- 어떤 보안 그룹 기반 보안 정책이 적용되었는지 확인합니다.

패킷을 추적하려면 다음 명령을 입력합니다.

명령	목적
packet-tracer input [*ifc_name*] [**icmp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*]| **fqdn** *fqdn-string*] *type code ident* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*]] | [**tcp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *sport* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *dport*] | [**udp** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *sport* [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] *dport*] | [**rawip** [**inline-tag** *tag*] [*sip* | **user** *username* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] [*dip* | **security-group** [**name** *name* | **tag** *tag*] | **fqdn** *fqdn-string*] | **security-group** [**name** *name* | **tag** *tag*] [**detailed**] [**xml**] **예:** `hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed`	패킷 및 ASA에서 패킷이 처리되는 방식에 대한 자세한 정보를 제공합니다. 이 예에서는 내부 호스트 10.2.25.3에서 외부 호스트 209.165.202.158로 패킷 추적을 활성화하는 방법을 자세한 정보와 함께 보여줍니다.

Per-Process CPU Usage 모니터링

CPU에서 실행되는 프로세스를 모니터링할 수 있습니다. 특정 프로세스에서 사용하는 CPU 백분율에 대한 정보를 얻을 수 있습니다. CPU 사용량 통계는 내림차순으로 정렬됩니다(사용량이 가장 많은 프로세스가 맨 위에 표시됨). 또한 로그 시간 5초, 1분 및 5분 전의 프로세스당 CPU 부하에 대한 정보도 포함됩니다. 실시간 통계를 제공할 수 있도록 이 정보는 5초마다 자동으로 업데이트됩니다.

구성된 컨텍스트에 의해 사용된 프로세스 관련 load-to-CPU의 분석 결과를 찾아보려면 **show process cpu-usage sorted** 명령을 사용할 수 있습니다.

파 트 5

고급 네트워크 보호

15 장

ASA 및 Cisco Cloud Web Security

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

ASA에서 Cloud Web Security가 활성화되면 ASA는 선택한 HTTP 및 HTTPS 트래픽을 Cloud Web Security 프록시 서버로 투명하게 리디렉션합니다. 그러면 Cloud Web Security 프록시 서버는 내용을 스캔하고 Cisco ScanCenter에 구성된 정책을 기반으로 트래픽을 허용 또는 차단하거나 트래픽에 대한 경로를 전송하여, 허용 가능한 사용을 적용하고 사용자를 악성코드로부터 보호합니다.

ASA는 선택적으로 IDFW(Identity Firewall) 및 AAA 규칙을 사용해 사용자를 인증 및 식별할 수 있습니다. ASA는 사용자 자격 증명(사용자 이름 및/또는 사용자 그룹 포함)을 암호화하여 Cloud Web Security로 리디렉션하는 트래픽에 포함합니다. 그러면 Cloud Web Security 서비스는 사용자 자격 증명을 사용해 트래픽을 정책에 맞춰봅니다. 사용자 기반 보고에도 이러한 자격 증명을 사용합니다. Cloud Web Security 서비스에서 정책을 적용하는 데 사용자 이름과 그룹이 반드시 필요하지는 않지만, ASA는 사용자 인증 없이 선택적으로 기본 사용자 이름 및/또는 그룹을 제공할 수 있습니다.

서비스 정책 규칙을 만들 때 Cloud Web Security로 보낼 트래픽을 사용자 지정할 수 있습니다. 서비스 정책 규칙과 일치하는 웹 트래픽의 하위 집합을 대신 원래 요청한 웹 서버로 직접 보내고 Cloud Web Security에서 스캔하지 않도록 "화이트리스트"를 구성할 수도 있습니다.

기본 및 백업 Cloud Web Security 프록시 서버를 구성할 수 있습니다. ASA는 정기적으로 이들을 각각 폴링(polling)하여 가용성을 확인합니다.

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

Cisco Cloud Web Security에 대한 정보

웹 트래픽을 Cloud Web Security로 리디렉션

최종 사용자가 HTTP 또는 HTTPS 요청을 보내면 ASA에서 이를 수신하여 선택적으로 사용자 및/또는 그룹 정보를 검색합니다. 트래픽이 Cloud Web Security의 ASA 서비스 정책 규칙과 일치하면 ASA는 요청을 Cloud Web Security 프록시 서버로 리디렉션합니다. 연결을 프록시 서버로 리디렉션함으로써 ASA는 최종 사용자와 Cloud Web Security 프록시 서버 간의 중개 역할을 합니다. ASA는 클라이언트 요청의 수신 IP 주소 및 포트를 변경하고, Cloud Web Security 전용 HTTP 헤더를 추가한 다음, 수정된 요청을 Cloud Web Security 프록시 서버로 전송합니다. Cloud Web Security HTTP 헤더에는 사용자 이름 및 사용자 그룹(사용 가능한 경우)을 비롯한 각종 정보가 포함되어 있습니다.

사용자 인증 및 Cloud Web Security

Cloud Web Security에서 정책을 적용하는 데 사용자 ID를 사용할 수 있습니다. 사용자 ID는 Cloud Web Security 보고에도 유용할 수 있습니다. Cloud Web Security를 사용하는 데 사용자 ID가 반드시 필요한 것은 아닙니다. Cloud Web Security 정책에 대한 트래픽을 식별하기 위한 다른 방법이 있습니다.

ASA는 사용자의 ID를 확인하거나 기본 ID를 제공하는 다음과 같은 방법을 지원합니다.

- AAA 규칙 - ASA가 AAA 규칙을 사용하여 사용자 인증을 수행하면 AAA 서버 또는 로컬 데이터베이스에서 사용자 이름이 검색됩니다. AAA 규칙의 ID에는 그룹 정보가 포함되어 있지 않습니다. 구성할 경우 기본 그룹이 사용됩니다. AAA 규칙 구성에 대한 자세한 내용은 기존 기능 가이드를 참조하십시오.
- IDFW - ASA에서 AD(Active Directory)와 함께 IDFW를 사용하는 경우, 액세스 규칙 또는 서비스 정책과 같은 기능에서 ACL을 사용함으로써 또는 사용자 ID 정보를 직접 다운로드하도록 사용자 ID 모니터를 구성함으로써 사용자 및/또는 그룹을 활성화하면 AD 에이전트에서 사용자 이름 및 그룹이 검색됩니다.

  IDFW 구성에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.
- 기본 사용자 이름 및 그룹 - ASA에서는 사용자 인증 없이, Cloud Web Security의 서비스 정책 규칙과 일치하는 모든 사용자에 대해 선택적으로 기본 사용자 이름 및/또는 그룹을 사용합니다.

인증 키

각 ASA는 Cloud Web Security에서 가져온 인증 키를 사용해야 합니다. 인증 키를 통해 Cloud Web Security는 웹 요청과 연결된 회사를 식별할 수 있으며, 인증 키를 사용하면 ASA가 유효한 고객과 연결되었음을 확인할 수 있습니다.

ASA에 대해 다음의 두 가지 인증 키 유형(회사 키 및 그룹 키) 중 하나를 사용할 수 있습니다.

- 15-3 페이지의 회사 인증 키
- 15-3 페이지의 그룹 인증 키

회사 인증 키

회사 인증 키는 동일한 회사 내 여러 ASA에서 사용할 수 있습니다. 이 키는 단순히 ASA에 대한 Cloud Web Security 서비스를 활성화합니다. 관리자는 ScanCenter(https://scancenter.scansafe.com/portal/admin/login.jsp)에서 이 키를 생성하며, 나중에 사용하도록 이메일로 이 키를 보낼 수 있습니다. 나중에 ScanCenter에서 이 키를 찾을 수 없습니다. ScanCenter에서는 마지막 4자만 표시됩니다. 자세한 내용은 다음의 Cloud Web Security 설명서를 참조하십시오.
http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html.

그룹 인증 키

그룹 인증 키는 각 ASA에 대해 고유한 특수 키로서 두 가지 기능을 수행합니다.

- 하나의 ASA에 대해 Cloud Web Security 서비스를 활성화합니다.
- ASA에 대한 ScanCenter 정책을 만들 수 있도록 ASA에서 오는 모든 트래픽을 식별합니다.

그룹 인증 키 사용에 대한 자세한 내용은 15-3 페이지의 ScanCenter 정책을 참조하십시오.

관리자는 ScanCenter(https://scancenter.scansafe.com/portal/admin/login.jsp)에서 이 키를 생성하며, 나중에 사용하도록 이메일로 이 키를 보낼 수 있습니다. 나중에 ScanCenter에서 이 키를 찾을 수 없습니다. ScanCenter에서는 마지막 4자만 표시됩니다. 자세한 내용은 다음의 Cloud Web Security 설명서를 참조하십시오.
http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html.

ScanCenter 정책

ScanCenter에서는 일치하는 규칙이 발견될 때까지 트래픽을 정책 규칙과 맞춰봅니다. 그런 다음 Cloud Web Security는 해당 규칙에 대해 구성된 작업을 적용합니다. 그룹 연결(*디렉토리 그룹* 또는 *맞춤형 그룹*)을 기반으로 트래픽을 ScanCenter의 정책 규칙에 맞춰볼 수 있습니다.

- 15-4 페이지의 디렉토리 그룹
- 15-4 페이지의 맞춤형 그룹
- 15-5 페이지의 그룹과 인증 키의 상호 작용 방법

디렉토리 그룹

디렉토리 그룹은 트래픽이 속한 그룹을 정의합니다. 그룹은(있는 경우) 클라이언트 요청의 HTTP 헤더에 포함됩니다. 사용자가 IDFW를 구성하면 ASA에서는 HTTP 헤더에 그룹을 포함합니다. IDFW를 사용하지 않는 경우 Cloud Web Security 검사에서 트래픽을 ASA 규칙과 맞춰보기 위한 기본 그룹을 구성할 수 있습니다.

디렉토리 그룹을 구성할 때는 그룹 이름을 정확히 입력해야 합니다.

- IDFW 그룹 이름은 다음 형식으로 전송됩니다.

  domain-name\group-name

  ASA에서 IDFW 그룹 이름을 확인할 때 ASA에 나타나는 형식은 *domain-name\\group-name*입니다. 그러나 ASA는 일반 ScanCenter 표기법을 따르기 위해 이름을 수정하여 백슬래시를 하나만(\) 사용합니다.

- 기본 그룹 이름은 다음 형식으로 전송됩니다.

  [*domain*]*group-name*

  ASA에서는 백슬래시 2개(\\)가 오도록 선택적인 도메인 이름을 구성해야 합니다. 그러나 ASA는 일반 ScanCenter 표기법을 따르기 위해 이름을 수정하여 백슬래시를 하나만(\) 사용합니다. 예를 들어 사용자가 "Cisco\\Boulder1"을 지정하면 ASA는 그룹 이름을 Cloud Web Security로 전송할 때 백슬래시를 하나만(\) 사용하여 그룹 이름을 "Cisco\Boulder1"로 수정합니다.

맞춤형 그룹

맞춤형 그룹은 하나 이상의 다음 기준을 사용하여 정의합니다.

- ScanCenter Group 인증 키 - 맞춤형 그룹에 대한 Group 인증 키를 생성할 수 있습니다. 그러면 ASA를 구성할 때 이 그룹 키를 지정하는 경우 ASA에서 오는 모든 트래픽에 Group 키라는 태그가 붙습니다.
- 소스 IP 주소 - 맞춤형 그룹에서 소스 IP 주소를 지정할 수 있습니다. ASA 서비스 정책은 소스 IP 주소를 기반으로 하므로 ASA에서 임의의 IP 주소 기반 정책을 대신 구성할 수도 있습니다.
- 사용자 이름 - 맞춤형 그룹에서 사용자 이름을 지정할 수 있습니다.
  - IDFW 사용자 이름은 다음 형식으로 전송됩니다.

    domain-name\username

  - AAA 사용자 이름(RADIUS 또는 TACACS+를 사용하는 경우)은 다음 형식으로 전송됩니다.

    LOCAL*username*

  - AAA 사용자 이름(LDAP 사용 시)은 다음 형식으로 전송됩니다.

    domain-name\username

  - 기본 사용자 이름은 다음 형식으로 전송됩니다.

    [*domain-name*]*username*

    예를 들어 기본 사용자 이름을 "Guest"로 구성하면 ASA는 "Guest"를 전송합니다. 기본 사용자 이름을 "Cisco\Guest"로 구성하면 ASA는 "Cisco\Guest"를 전송합니다.

그룹과 인증 키의 상호 작용 방법

맞춤형 그룹+그룹 키가 제공하는 ASA 단위 정책이 필요하지 않은 경우에는 회사 키를 사용할 수 있습니다. 맞춤형 그룹이 모두 그룹 키와 연결되는 것은 아닙니다. 키가 지정되지 않은 맞춤형 그룹은 IP 주소 또는 사용자 이름을 식별하는 데 사용하거나, 디렉토리 그룹을 사용하는 규칙과 함께 정책에서 사용할 수 있습니다.

ASA 단위 정책이 필요하고 그룹 키를 사용 중인 경우에도 디렉토리 그룹 및 키가 지정되지 않은 맞춤형 그룹에서 제공하는 매칭 기능을 사용할 수 있습니다. 이 경우 그룹 멤버십, IP 주소 또는 사용자 이름 기반으로 일부를 제외하고 ASA 기반 정책을 사용할 수 있습니다. 예를 들면 모든 ASA에서 America\Management 그룹의 사용자를 제외할 수 있습니다.

1. America\Management에 대한 디렉토리 그룹을 추가합니다.
2. 이 그룹에 대한 제외 규칙을 추가합니다.
3. ASA 단위로 정책을 적용할 예외 규칙 뒤에 각 맞춤형 그룹+그룹 키에 대한 규칙을 추가합니다.
4. America\Management의 사용자로부터 오는 트래픽은 예외 규칙으로 확인하고, 다른 모든 트래픽은 ASA에 대한 규칙으로 확인하게 됩니다.

키, 그룹 및 정책 규칙을 다양하게 조합할 수 있습니다.

Cloud Web Security 작업

Cloud Web Security는 구성된 정책을 적용한 후 사용자 요청을 차단 또는 허용하거나 경고를 전송합니다.

- 허용 - Cloud Web Security는 클라이언트 요청을 허용하는 경우 원래 요청한 서버에 연결하여 데이터를 검색합니다. 서버 응답을 ASA로 전달한 후 사용자에게 전달합니다.
- 차단 - Cloud Web Security는 클라이언트 요청을 차단하는 경우 액세스가 차단되었음을 사용자에게 알리고 HTTP 302 "Moved Temporarily" 응답을 전송합니다. 그러면 클라이언트 애플리케이션은 Cloud Web Security 프록시 서버에서 호스팅하는 웹 페이지로 리디렉션되며, 차단을 알리는 오류 메시지가 표시됩니다. ASA는 클라이언트에 302 응답을 전달합니다.
- 경고 - 특정 사이트가 허용 가능한 사용 정책을 위반한 것으로 Cloud Web Security 프록시 서버에서 판단할 경우 해당 사이트에 대한 경고 페이지가 표시됩니다. 사용자는 경고에 따라 연결 요청을 삭제할 수도 있고, 경고를 클릭하여 요청 사이트로 계속 진행할 수도 있습니다.

또한 ASA에서 기본 또는 백업 Cloud Web Security 프록시 서버에 도달할 수 없을 경우 웹 트래픽을 처리하는 방법을 선택할 수도 있습니다. 모든 웹 트래픽을 차단하거나 허용할 수 있습니다. 기본적으로는 웹 트래픽을 차단합니다.

화이트리스트로 스캐닝 우회

AAA 규칙 또는 IDFW를 사용할 경우, 서비스 정책 규칙과 일치하는 특정 사용자 또는 그룹에서 오는 웹 트래픽이 스캐닝을 위해 Cloud Web Security 프록시 서버로 리디렉션되지 않도록 ASA를 구성할 수 있습니다. Cloud Web Security 스캐닝을 우회하는 경우, ASA에서는 프록시 서버에 연결하지 않은 채 원래 요청 웹 서버에서 직접 콘텐츠를 검색합니다. 웹 서버에서 응답을 수신하면 데이터를 클라이언트로 전송합니다. 이 과정을 트래픽의 "화이트리스팅"이라고 합니다.

Cloud Web Security로 전송하기 위해 ACL을 사용하여 트래픽의 클래스를 구성하는 경우 사용자 또는 그룹을 기반으로 트래픽을 제외하는 것과 동일한 결과를 얻을 수 있지만, 화이트리스트를 사용하는 방법이 좀 더 간단하다는 것을 알 수 있을 것입니다. 화이트리스트 기능은 IP 주소가 아니라 사용자 및 그룹만을 기반으로 합니다.

IPv4 및 IPv6 지원

Cloud Web Security에서는 현재 IPv4 주소만 지원합니다. 내부에서 IPv6을 사용하는 경우 Cloud Web Security로 전송해야 할 IPv6 흐름에 대해 NAT 64를 수행해야 합니다.

다음 표는 Cloud Web Security 리디렉션에서 지원되는 클래스 맵 트래픽을 보여줍니다.

클래스 맵 트래픽	Cloud Web Security 검사
IPv4에서 IPv4로	지원됨
IPv6에서 IPv4로(NAT64 사용)	지원됨
IPv6에서 IPv4로	지원되지 않음
IPv6에서 IPv6으로	지원되지 않음

기본 프록시 서버에서 백업 프록시 서버로 장애 조치

Cisco Cloud Web Security 서비스를 구독하는 사용자에게는 기본 Cloud Web Security 프록시 서버 및 백업 프록시 서버가 할당됩니다.

클라이언트가 기본 서버에 도달할 수 없는 경우 ASA에서는 가용성 확인을 위해 타워의 폴링을 시작합니다. 클라이언트 활동이 없으면 ASA는 15분마다 폴링합니다. 구성된 재시도 횟수(기본 5회이며 구성 가능) 이후에도 프록시 서버를 사용할 수 없는 경우, 해당 서버는 도달할 수 없는 상태로 선언되고 백업 프록시 서버가 활성화됩니다.

클라이언트 또는 ASA가 재시도 횟수에 도달하기 전 2회 이상 연속적으로 서버에 도달할 수 있으면 폴링이 멈추고 타워는 도달 가능한 것으로 확인됩니다.

백업 서버로의 장애 조치 이후에도 ASA는 계속해서 기본 서버를 폴링합니다. 기본 서버에 도달할 수 있게 되면 ASA는 다시 기본 서버를 사용합니다.

Cisco Cloud Web Security의 라이센싱 요구 사항

모델	라이센스 요구 사항
ASAv	표준 또는 프리미엄 라이센스
모든 다른 모델	보안 어플라이언스 및 Cloud Web Security 서버 간의 트래픽을 암호화하는 강력한 암호화(3DES/AES) 라이센스

Cloud Web Security 관점에서 사용자는 Cisco Cloud Web Security 라이센스를 구매하고 ASA에서 처리하는 사용자 수를 파악해야 합니다. 그런 다음 ScanCenter에 로그인하여 인증 키를 생성해야 합니다.

Cloud Web Security 전제 조건

(선택 사항) 사용자 인증 전제 조건

사용자 ID 정보를 Cloud Web Security로 전송하려면 ASA에서 다음 중 하나를 구성하십시오.

- AAA 규칙(사용자 이름 전용) - 기존 기능 가이드를 참조하십시오.
- IDFW(사용자 이름 및 그룹) - 일반 운영 컨피그레이션 가이드를 참조하십시오.

(선택 사항) 정규화된 도메인 이름 전제 조건

서비스 정책 규칙 또는 Cloud Web Security 서버에 대해 ACL에서 FQDN을 사용하는 경우 일반 운영 컨피그레이션 가이드에 따라 ASA용 DNS 서버를 구성해야 합니다.

지침 및 제한

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원됩니다.

다중 컨텍스트 모드에서는 시스템에서만 서버 컨피그레이션이 허용되며, 보안 컨텍스트에서만 서비스 정책 규칙 컨피그레이션이 허용됩니다.

필요한 경우 각 컨텍스트에 자체 인증 키를 둘 수 있습니다.

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

IPv6 지침

IPv6은 지원되지 않습니다. 15-6 페이지의 IPv4 및 IPv6 지원섹션을 참조하십시오.

추가 지침

- Cloud Web Security에서는 ASA 클러스터링이 지원되지 않습니다.
- Cloud Web Security에서는 클라이언트리스 SSL VPN이 지원되지 않습니다. Cloud Web Security용 ASA 서비스 정책에서 클라이언트리스 SSL VPN 트래픽을 제외하십시오.
- Cloud Web Security 프록시 서버에 대한 인터페이스가 중단되는 경우 **show scansafe server** 명령의 출력에서는 약 15~25분 동안 두 서버가 가동 상태인 것으로 표시됩니다. 폴링 메커니즘은 활성 연결을 기반으로 하기 때문에, 그리고 인터페이스가 중단되면 제로(0) 연결이 표시되고 폴링 접근 방식에 가장 긴 시간이 걸리므로 이러한 상황이 발생할 수 있습니다.
- Cloud Web Security는 ASA CX 모듈에서 지원되지 않습니다. 동일한 트래픽에 대해 ASA CX 작업과 Cloud Web Security 검사를 모두 구성하면 ASA에서는 ASA CX 작업만 수행합니다.
- Cloud Web Security 검사는 동일한 트래픽에 대해 HTTP 검사와 호환되지 않습니다. HTTP 검사는 기본 글로벌 정책의 일부로서 기본적으로 활성화됩니다.
- 별도의 연결에 대해 동일한 소스 포트와 IP 주소를 사용할 수 있는 애플리케이션 또는 확장 PAT에서는 Cloud Web Security가 지원되지 않습니다. 예를 들어 동일한 서버를 대상으로 하는 두 개의 서로 다른 연결에서 확장 PAT를 사용하는 경우, 목적지별로 두 연결이 구분되기 때문에 ASA는 두 연결 변환에 동일한 소스 IP 및 소스 포트를 재사용할 수 있습니다. ASA는 이러한 연결을 Cloud Web Security 서버로 리디렉션할 때 목적지를 Cloud Web Security 서버 IP 주소 및 포트(기본값 8080)로 교체합니다. 그 결과 두 연결이 이제 동일한 흐름(동일한 소스 IP/포트 및 목적지 IP/포트)에 속하는 것처럼 보이므로 반환 트래픽을 제대로 변환할 수 없습니다.
- **match** default-inspection-traffic 명령 Cloud Web Security 검사용 기본 포트(80 및 443)가 포함되지 않습니다.

기본 설정

기본적으로 Cisco Cloud Web Security는 활성화되지 않습니다.

Cisco Cloud Web Security 구성

Cloud Web Security 프록시 서버와의 통신 구성

지침

공개 키가 ASA 소프트웨어에 삽입되므로 구성할 필요가 없습니다.

자세한 단계

	명령	목적
1단계	**scansafe general-options** 예: hostname(config)# scansafe general-options	scansafe general-options 컨피그레이션 모드로 들어갑니다.
2단계	**server primary** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] 예: hostname(cfg-scansafe)# server primary ip 192.168.43.10	기본 Cloud Web Security 프록시 서버의 정규화된 도메인 이름 또는 IP 주소를 구성합니다. 기본적으로 Cloud Web Security 프록시 서버는 HTTP 및 HTTPS 트래픽에 대해 포트 8080을 사용합니다. 다른 설정을 원하는 경우가 아니라면 이 값을 변경하지 마십시오.
3단계	**server backup** {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*] 예: hostname(cfg-scansafe)# server backup fqdn server.example.com	(선택 사항) 백업 Cloud Web Security 프록시 서버의 정규화된 도메인 이름 또는 IP 주소를 구성합니다. 기본적으로 Cloud Web Security 프록시 서버는 HTTP 및 HTTPS 트래픽에 대해 포트 8080을 사용합니다. 다른 설정을 원하는 경우가 아니라면 이 값을 변경하지 마십시오.
4단계	**retry-count** *value* 예: hostname(cfg-scansafe)# retry-count 2	(선택 사항) 서버가 도달 불가능한 상태임을 확인할 때까지 Cloud Web Security 프록시 서버에 대한 연속 폴링 실패 횟수의 값을 입력합니다. 폴링은 30초마다 수행됩니다. 유효한 값은 2~100이고 기본값은 5입니다. 15-6 페이지의 기본 프록시 서버에서 백업 프록시 서버로 장애 조치 섹션을 참조하십시오.
5단계	**license** *hex_key* 예: hostname(cfg-scansafe)# license F12A588FE5A0A4AE86C10D222FC658F3	요청이 어느 조직에서 오는지를 나타내기 위해 ASA가 Cloud Web Security 프록시 서버에 전송하는 인증 키를 구성합니다. 인증 키는 16바이트 16진수입니다. 15-3 페이지의 인증 키 섹션을 참조하십시오.

예

다음 예는 기본 및 백업 서버를 구성합니다.

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

(다중 컨텍스트 모드) 보안 컨텍스트 단위로 Cloud Web Security 허용

다중 컨텍스트 모드에서는 컨텍스트 단위로 Cloud Web Security를 허용해야 합니다. 자세한 내용은 일반 운영 컨피그레이션 가이드 섹션을 참조하십시오.

참고 관리자 컨텍스트 및 특정 컨텍스트 모두에서 Scansafe 타워를 가리키는 경로를 구성해야 합니다. 이렇게 하면 Active/Active 장애 조치 시나리오에서 Scansafe 타워가 도달 불가능한 상태로 들어가는 것을 방지할 수 있습니다.

다음 샘플 컨피그레이션에서 context one에서는 기본 라이센스로, context two에서는 라이센스 키 재지정으로 Cloud Web Security를 활성화합니다.

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

Cloud Web Security로 트래픽을 전송하도록 서비스 정책 구성

서비스 정책 규칙에 대한 자세한 내용은 1 장, “Modular Policy Framework를 사용하는 서비스 정책”을 참조하십시오.

사전 요구 사항

(선택 사항) Cloud Web Security에 대한 전송에서 일부 트래픽을 제외하기 위해 화이트리스트를 사용해야 하는 경우, 서비스 정책 규칙에서 화이트리스트를 참조할 수 있도록 15-14 페이지의 (선택 사항) 화이트리스트에 있는 트래픽 구성에 따라 화이트리스트를 만드십시오.

자세한 단계

	명령	목적
1단계	**policy-map type inspect scansafe** *name1* 예: hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1	규칙에 대한 필수 매개변수를 구성하고 선택적으로 화이트리스트를 식별할 수 있도록 검사 정책 맵을 만듭니다. Cloud Web Security로 보내고자 하는 각 트래픽 클래스에 대해 검사 정책 맵이 필요합니다. *policy_map_name* 인수의 길이는 최대 40자입니다. policy-map 컨피그레이션 모드로 들어갑니다.
2단계	parameters 예: hostname(config-pmap)# parameters	매개변수를 사용하면 프로토콜 및 기본 사용자 또는 그룹을 구성할 수 있습니다. 매개변수 컨피그레이션 모드로 들어갑니다.
3단계	**{http | https}** 예: hostname(config-pmap-p)# http	이 검사 정책 맵에 대해 서비스 유형을 하나만(**http** 또는 **https**) 지정할 수 있습니다.
4단계	(선택 사항) **default** {**[user** *username*] [**group** *groupname*]} 예: hostname(config-pmap-p)# default group default_group	ASA가 ASA로 들어오는 사용자의 ID를 확인할 수 없는 경우 HTTP 헤더에 기본 사용자 및/또는 그룹이 포함되도록 지정합니다.
5단계	(선택 사항, 화이트리스트의 경우) **class** *whitelist_name* 예: hostname(config-pmap-p)# class whitelist1	15-14 페이지의 (선택 사항) 화이트리스트에 있는 트래픽 구성에서 만든 화이트리스트 클래스 맵 이름을 식별합니다.
6단계	whitelist 예: hostname(config-pmap-p)# class whitelist1 hostname(config-pmap-c)# whitelist	트래픽의 클래스에 대해 화이트리스트 작업을 수행합니다.

	명령	목적

7단계	**policy-map type inspect scansafe** *name2*
	  parameters
	  default {**[user** *user*] [**group** *group*]}
	  class *whitelist_name2*
	  whitelist
	
	예:
	hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
	hostname(config-pmap)# parameters
	hostname(config-pmap-p)# default group2 default_group2
	hostname(config-pmap-p)# class whitelist2
	hostname(config-pmap-c)# whitelist
		예를 들어, HTTPS 트래픽에 대해 별도의 클래스 맵을 만들려면 1단계~6단계를 반복하십시오. Cloud Web Security로 전송할 각 트래픽 클래스에 대해 검사 클래스 맵을 만들 수 있습니다. 원하는 경우 여러 트래픽 클래스에 대해 검사 클래스 맵을 재사용할 수 있습니다.

8단계	**access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **tcp** [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] 예: hostname(config)# object network cisco1 hostname(config-object-network)# fqdn www.cisco.com hostname(config)# object network cisco2 hostname(config-object-network)# fqdn tools.cisco.com hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80 hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80 hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80	Cloud Web Security로 전송할 트래픽의 클래스를 식별합니다. 하나 이상의 ACE(Access Control Entry)로 구성된 ACL을 만듭니다. ACL에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오. Cloud Web Security는 HTTP 및 HTTPS 트래픽에서만 작동합니다. 각 트래픽 유형은 ASA에서 별도로 취급됩니다. 따라서 HTTP 전용 ACL 및 HTTPS 전용 ACL을 만들어야 합니다. 정책에 대해 필요한 만큼 ACL을 만드십시오. **permit** ACE는 일치하는 트래픽을 Cloud Web Security로 전송합니다. **deny** ACE는 Cloud Web Security로 전송되지 않도록 서비스 정책 규칙에서 트래픽을 제외합니다. ACL을 만들 때에는 인터넷을 위한 적절한 트래픽을 확인하되 기타 내부 네트워크를 위한 트래픽은 확인하지 않는 방법을 고려해야 합니다. 예를 들어 목적지가 DMZ에 있는 내부 서버일 때 내부 트래픽이 Cloud Web Security로 전송되지 않도록 하려면, DMZ에 대한 트래픽을 제외하는 ACL에 deny ACE를 추가해야 합니다. 특정 서버에 대한 트래픽을 제외하는 데 FQDN 네트워크 객체가 유용할 수 있습니다. *user_argument*를 사용하면 인라인으로 또는 객체 그룹을 참조하여 IDFW 사용자 이름 또는 그룹을 지정할 수 있습니다. *security_group_argument*를 사용하면 인라인으로 또는 객체 그룹을 참조하여 TrustSec 보안 그룹을 지정할 수 있습니다. 보안 그룹에서 Cloud Web Security로 전송할 트래픽을 확인할 수는 있지만, ASA는 HTTP 헤더에서 보안 그룹 정보를 Cloud Web Security로 전송하지 않습니다. Cloud Web Security는 보안 그룹을 기반으로 정책을 만들 수 없습니다.
9단계	**class-map** *name1* 예: hostname(config)# class-map cws_class1	Cloud Web Security 필터링을 활성화할 트래픽을 식별하기 위한 클래스 맵을 만듭니다.

	명령	목적
10단계	**match access-list** *acl1* 예: hostname(config-cmap)# match access-list SCANSAFE_HTTP	8단계에서 만든 ACL을 지정합니다. 이 규칙에 대해 다른 match 문을 사용할 수도 있지만, 가장 다양하게 HTTP 또는 HTTPS 전용 트래픽을 식별할 수 있는 **match access-list** 명령을 사용할 것을 권장합니다. 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵) 섹션을 참조하십시오.
11단계	**class-map** *name2* **match access-list** *acl2* 예: hostname(config)# class-map cws_class2 hostname(config-cmap)# match access-list SCANSAFE_HTTPS	(선택 사항) 추가 클래스 맵(예: HTTPS 트래픽용)을 만듭니다. 이 서비스 정책 규칙에 필요한 만큼 클래스를 만들 수 있습니다.
12단계	**policy-map** *name* 예: hostname(config)# policy-map cws_policy	클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다. 기본 글로벌 정책의 정책 맵을 global_policy라고 합니다. 이 정책을 편집할 수도 있고 새로 만들 수도 있습니다. 각 인터페이스에 또는 전체적으로 정책을 하나만 적용할 수 있습니다.
13단계	**class** *name1* 예: hostname(config-pmap)# class cws_class1	9단계에서 생성한 클래스 맵을 식별합니다.
14단계	**inspect scansafe** *scansafe_policy_name1* [**fail-open** | **fail-close**] 예: hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open	이 클래스에서 트래픽에 대한 Cloud Web Security 검사를 활성화합니다. 1단계에서 만든 검사 클래스 맵 이름을 지정합니다. Cloud Web Security 서버를 사용할 수 없을 때 트래픽이 ASA를 통과하도록 허용하려면 **fail-open**을 지정합니다. Cloud Web Security 서버를 사용할 수 없을 때 모든 트래픽을 삭제하려면 **fail-close**를 지정합니다. **fail-close**가 기본값입니다.
15단계	**class** *name2* **inspect scansafe** *scansafe_policy_name2* [**fail-open** | **fail-close**] 예: hostname(config-pmap)# class cws_class2 hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open	(선택 사항) 11단계에서 만든 두 번째 클래스 맵을 식별하고, 이에 대한 Cloud Web Security 검사를 활성화합니다. 필요에 따라 여러 클래스 맵을 구성할 수 있습니다.
16단계	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} 예: hostname(config)# service-policy cws_policy inside	하나 이상의 인터페이스에서 정책 맵을 활성화합니다. **global**은 모든 인터페이스에서 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다. 자세한 내용은 1-17 페이지의 인터페이스에 작업 적용(서비스 정책) 섹션을 참조하십시오.

예

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

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

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

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

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

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

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

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

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

(선택 사항) 화이트리스트에 있는 트래픽 구성

사용자 인증을 사용하는 경우, 사용자 이름 및/또는 그룹 이름을 기반으로 Cloud Web Security에서 일부 트래픽이 필터링되는 것을 제외할 수 있습니다. Cloud Web Security 서비스 정책 규칙을 구성할 때 화이트리스팅 검사 클래스 맵을 참조할 수 있습니다. IDFW 및 AAA 사용자 자격 증명 모두 이 기능과 함께 사용할 수 있습니다.

서비스 정책 규칙을 구성하는 경우 사용자 또는 그룹을 기반으로 트래픽을 제외하는 것과 동일한 결과를 얻을 수 있지만, 화이트리스트를 사용하는 방법이 좀 더 간단하다는 것을 알 수 있을 것입니다. 화이트리스트 기능은 IP 주소가 아니라 사용자 및 그룹만을 기반으로 합니다.

자세한 단계

	명령	목적
1단계	**class-map type inspect scansafe** [**match-all** | **match-any**] *name* 예: hostname(config)# class-map type inspect scansafe match-any whitelist1	화이트리스트에 있는 사용자 및 그룹에 대한 검사 클래스 맵을 만듭니다. *class_map_name* 인수는 클래스 맵의 이름입니다(길이 최대 40자). **match-all** 키워드는 기본값이며, 트래픽이 모든 기준과 일치해야 클래스 맵과 일치하는 것임을 의미합니다. **match-any** 키워드는 트래픽이 하나 이상의 기준과 일치하는 경우 클래스 맵과 일치하는 것으로 지정합니다. CLI를 사용하면 하나 이상의 **match** 명령을 입력할 수 있는 클래스 맵 컨피그레이션 모드로 전환됩니다.
2단계	**match** [**not**] {[**user** *username*] [**group** *groupname*]} 예: hostname(config-cmap)# match	**match** 키워드 뒤에 특정 사용자 이름 또는 그룹 이름을 추가하면 화이트리스트에 추가할 사용자 또는 그룹을 지정할 수 있습니다. **match not** 키워드는 Web Cloud Security를 사용하여 사용자 및/또는 그룹을 필터링하도록 지정합니다. 예를 들어, 그룹 "cisco"를 화이트리스트에 추가하되 사용자 "johncrichton" 및 "aerynsun"의 트래픽을 스캔하려면 이 두 사용자에 대해 **match not**을 지정할 수 있습니다. 이 명령을 반복하여 사용자와 그룹을 필요한 만큼 추가합니다.

예

다음 예는 HTTP 및 HTTPS 검사 정책 맵에 대해 동일한 사용자 및 그룹을 화이트리스트에 추가합니다.

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

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

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

(선택 사항) 사용자 ID 모니터 구성

IDFW를 사용할 경우 ASA는 활성 ACL에 포함된 사용자 및 그룹에 대한 AD 서버에서 사용자 ID 정보만 다운로드합니다. ACL은 액세스 규칙, AAA 규칙, 서비스 정책 규칙 등의 기능 또는 활성 상태로 간주되는 기타 기능에 사용해야 합니다. Cloud Web Security는 정책의 기반을 사용자 ID에 두기 때문에, 모든 사용자에 대해 IDFW를 충분히 적용하려면 활성 ACL의 일부가 아닌 그룹을 다운로드해야 할 수 있습니다. 예를 들어 사용자 및 그룹에 ACL을 사용하여 관련 그룹을 활성화하도록 Cloud Web Security 서비스 정책 규칙을 구성할 수 있지만 반드시 그렇게 해야 하는 것은 아닙니다. IP 주소만을 기반으로 ACL을 사용할 수도 있습니다. 사용자 ID 모니터(user identity monitor) 기능을 사용하면 AD 에이전트에서 직접 그룹 정보를 다운로드할 수 있습니다.

제한

사용자 ID 모니터용으로 구성된 그룹 및 활성 ACL을 통해 모니터링하는 그룹을 포함하여 ASA는 최대 512개의 그룹만 모니터링할 수 있습니다.

자세한 단계

명령	목적
user-identity monitor {**user-group** [*domain-name*\\]*group-name* | **object-group-user** *object-group-name*} **예:** `hostname(config)# user-identity monitor user-group CISCO\\Engineering`	지정된 사용자 또는 그룹 정보를 AD 에이전트에서 다운로드합니다. • **user-group** - 그룹 이름을 인라인으로 지정합니다. 도메인과 그룹 사이에 백슬래시 2개(\\)를 지정해도, ASA에서는 Cloud Web Security로 전송할 때 Cloud Web Security 표기법을 따르기 위해 백슬래시를 하나만 포함하도록 이름을 수정합니다. • **object-group-user** - **object-group user** 이름을 지정합니다. 이 그룹에는 여러 그룹을 포함할 수 있습니다.

Cloud Web Security 정책 구성

ASA 서비스 정책 규칙을 구성한 다음 ScanCenter Portal을 실행하여 웹 콘텐츠 스캐닝, 필터링, 악성코드 방지 서비스 및 보고서를 구성하십시오.

자세한 단계

https://scancenter.scansafe.com/portal/admin/login.jsp로 이동하십시오.

자세한 내용은 Cisco ScanSafe Cloud Web Security Configuration Guides를 참조하십시오.

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

Cloud Web Security 모니터링

명령	목적
show scansafe server	서버의 상태, 즉 현재 활성 서버인지, 백업 서버인지 또는 도달할 수 없는 서버인지를 보여줍니다.
show scansafe statistics	전체 및 현재 HTTP(S) 연결을 보여줍니다.
show conn scansafe	모든 Cloud Web Security 연결을 보여줍니다(대문자 Z 플래그로 표시됨).
show service policy inspect scansafe	특별한 정책에 의해 리디렉션되거나 화이트리스트에 추가되는 연결의 수를 보여줍니다.
다음 URL을 참조하십시오. http://Whoami.scansafe.net	트래픽이 Cloud Web Security 서버로 이동하는지 확인하려면 클라이언트에서 이 웹사이트에 액세스하십시오.

show scansafe server 명령은 Cloud Web Security 프록시 서버에 도달할 수 있는지를 보여줍니다.

```
hostname# show scansafe server
hostname# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
hostname# Backup: proxy137.scansafe.net (80.254.152.99)
```

show scansafe statistics 명령은 프록시 서버로 리디렉션된 연결의 수, 리디렉션 중인 현재 연결의 수, 화이트리스트에 추가된 연결의 수 등 Cloud Web Security 활동에 대한 정보를 보여줍니다.

```
hostname# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

show service policy inspect scansafe 명령은 특별한 정책에 의해 리디렉션되거나 화이트리스트에 추가되는 연결의 수를 보여줍니다.

```
hostname(config)# show service-policy inspect scansafe
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
Interface inside:
  Service-policy: scansafe-pmap
    Class-map: scansafe-cmap
      Inspect: scansafe p-scansafe fail-open, packet 0, drop 0, reset-drop 0,
v6-fail-close 0
Number of whitelisted connections: 0
Number of connections allowed without scansafe inspection because of "fail-open" config: 0
Number of connections dropped because of "fail-close" config: 0
Number of HTTP connections inspected: 0
Number of HTTPS connections inspected: 0
Number of HTTP connections dropped because of errors: 0
Number of HTTPS connections dropped because of errors: 0
```

Cisco Cloud Web Security에 대한 컨피그레이션 예

단일 모드 예

다음 예는 Cisco Cloud Web Security의 완전한 컨피그레이션을 보여줍니다.

ACL 구성

별도의 HTTP 및 HTTPS 클래스 맵을 만들려면 통과한 HTTP 및 HTTPS 패킷의 수를 알 수 있도록 트래픽을 분할하는 것이 좋습니다.

그런 다음 문제 해결이 필요한 경우 디버그 명령을 실행하여, 각 클래스 맵을 통과한 패킷 수를 구분하고 HTTP 또는 HTTPS 트래픽이 더 많이 통과하도록 처리 중인지 알아낼 수 있습니다.

```
hostname(config)# access-list web extended permit tcp any any eq www
hostname(config)# access-list https extended permit tcp any any eq https
```

클래스 맵 구성

```
hostname(config)# class-map cmap-http
hostname(config-cmap)# match access-list web

hostname(config)# class-map cmap-https
hostname(config-cmap)# match access-list https
```

검사 정책 맵 구성

```
hostname(config)# policy-map type inspect scansafe http-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httptraffic
hostname(config-pmap-p)# http

hostname(config)# policy-map type inspect scansafe https-pmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# default group httpstraffic
hostname(config-pmap-p)# https
```

정책 맵 구성

```
hostname(config)# policy-map pmap-webtraffic
hostname(config-pmap)# class cmap-http
hostname(config-pmap-c)# inspect scansafe http-pmap fail-close

hostname(config-pmap)# class cmap-https
hostname(config-pmap-c)# inspect scansafe https-pmap fail-close
```

서비스 정책 구성

```
hostname(config)# service-policy pmap-webtraffic interface inside
```

ASA에서 Cloud Web Security 구성

```
hostname(config)# scansafe general-options
hostname(cfg-scansafe)# server primary ip 192.168.115.225 web 8080
hostname(cfg-scansafe)# retry-count 5
hostname(cfg-scansafe)# license 366C1D3F5CE67D33D3E9ACEC265261E5
```

다중 모드 예

다음 예는 context one에서는 기본 라이센스로, context two에서는 인증 키 재지정으로 Cloud Web Security를 활성화합니다.

```
! System Context
!
hostname(config)#scansafe general-options
hostname(cfg-scansafe)#server primary ip 180.24.0.62 port 8080
hostname(cfg-scansafe)#retry-count 5
hostname(cfg-scansafe)#license FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
hostname(cfg-scansafe)#publickey <path to public key>
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC265261E5
!
config-url disk0:/two_ctx.cfg
!
```

화이트리스트 예

어떤 access-list 트래픽을 Cloud Web Security로 전송해야 할지를 구성합니다.

```
access-list 101 extended permit tcp any4 any4 eq www
access-list 102 extended permit tcp any4 any4 eq https

class-map web
 match access-list 101
class-map https
 match access-list 102
```

user1이 Cloud Web Security를 우회하기 위한 이 access-list 범위에 있는지를 확인하기 위해 화이트리스트를 구성하려면:

```
class-map type inspect scansafe match-any whiteListCmap
 match user LOCAL\user1
```

Cloud Web Security Policy 맵에 class-map을 첨부하려면:

```
policy-map type inspect scansafe ss
 parameters
  default user user1 group group1
  HTTP
```

```
 class whiteListCmap
  whitelist

policy-map type inspect scansafe ss2
 parameters
  default user user1 group group1
  https
 class whiteListCmap
  whitelist
```

이 검사 정책을 만든 후, 서비스 그룹에 할당할 수 있도록 정책 맵에 첨부합니다.

```
policy-map pmap
 class web
  inspect scansafe ss fail-close
class https
  inspect scansafe ss2 fail-close
```

그런 다음 전체적으로 적용하거나 ASA 인터페이스에 적용할 수 있도록 정책 맵을 service-policy에 첨부합니다.

```
service-policy pmap interface inside
```

디렉토리 통합 예

이 섹션에는 디렉토리 통합을 위한 다양한 컨피그레이션 예가 포함되어 있습니다.

LDAP를 사용하여 Active Directory 서버 구성

다음 예는 ASA에서 LDAP를 사용하여 Active Directory 서버를 구성하는 방법을 보여줍니다.

```
hostname(config)# aaa-server AD protocol ldap
hostname(config-aaa-server-group)# aaa-server AD (inside) host 192.168.116.220
hostname(config-aaa-server-host)# ldap-base-dn DC=ASASCANLAB,DC=local
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# server-type microsoft
hostname(config-aaa-server-host)# server-port 389
hostname(config-aaa-server-host)# ldap-login-dn
cn=administrator,cn=Users,dc=asascanlab,dc=local
hostname(config-aaa-server-host)# ldap-login-password Password1
```

RADIUS를 사용하여 Active Directory 에이전트 구성

다음 예는 ASA에서 RADIUS를 사용하여 Active Directory 에이전트를 구성하는 방법을 보여줍니다.

```
hostname(config)# aaa-server adagent protocol radius
hostname(config-aaa-server-group)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.116.220
hostname(config-aaa-server-host)# key cisco123
hostname(config-aaa-server-host)# user-identity ad-agent aaa-server adagent
```

AD 에이전트 서버에서 클라이언트로서 ASA 생성

다음 예는 Active Directory 에이전트 서버에서 클라이언트로서 ASA를 생성하는 방법을 보여줍니다.

```
c:\IBF\CLI\adacfg client create -name ASA5520DEVICE -ip 192.168.116.90 -secret cisco123
```

AD 에이전트와 DC 간에 링크 생성

다음 예는 Active Directory 에이전트와 로그온/로그오프 이벤트를 모니터링할 모든 DC 간에 링크를 생성하는 방법을 보여줍니다.

```
c:\IBF\CLI\adacfg.exe dc create -name DCSERVER1 -host W2K3DC -domain
W2K3DC.asascanlab.local -user administrator -password Password1
c:\IBF\CLI\adacfg.exe dc list
```

마지막 명령을 실행하면 상태가 "UP"으로 표시됩니다.

AD_Agent에서 로그온/로그오프 이벤트를 모니터링하려면, 현재 활발하게 모니터링되고 있는 모든 DC에 에이전트가 로그온한 상태여야 합니다. 이를 위해 다음을 선택합니다.

Start > Administrative Tools > Domain Controller Security Policy

Local policies > Audit Policy > Audit account logon events (success and failure)

AD 에이전트 테스트

다음 예는 ASA와 통신할 수 있도록 테스트 Active Directory 에이전트를 구성하는 방법을 보여줍니다.

```
hostname# test aaa-server ad-agent adagent
Server IP Address or name: 192.168.116.220
INFO: Attempting Ad-agent test to IP address <192.168.116.220> (timeout: 12 seconds)
INFO: Ad-agent Successful
```

함께 참조할 명령: **show user-identity ad-agent**.

ASA에서 Identity 옵션 구성

다음 예는 ASA에서 identity 옵션을 구성하는 방법을 보여줍니다.

```
hostname(config)# user-identity domain ASASCANLAB aaa-server AD
hostname(config)# user-identity default-domain ASASCANLAB
```

User Identity 옵션 구성 및 세밀한 보고 활성화

다음 예는 ASA에 사용자 자격 증명을 전송하고 프록시 서버로부터 세밀한 사용자 보고를 활성화하는 User Identity 옵션을 구성하는 방법을 보여줍니다.

```
hostname(config)# user-identity inactive-user-timer minutes 60
hostname(config)# user-identity action netbios-response-fail remove-user-ip
hostname(config)# user-identity user-not-found enable
hostname(config)# user-identity action mac-address-mismatch remove-user-ip
hostname(config)# user-identity ad-agent active-user-database full-download
```

도메인을 두 개 이상 사용 중인 경우 다음 명령을 입력합니다.

```
hostname(config)# user-identity domain OTHERDOMAINNAME
```

Active Directory 그룹 모니터링

다음 예는 모니터링할 Active Directory 그룹의 구성 방법을 보여줍니다.

```
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME1
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME2
hostname(config)# user-identity monitor user-group ASASCANLAB\\GROUPNAME3
```

주의 위의 작업을 완료한 후 반드시 컨피그레이션을 저장하십시오.

Active Directory 서버에서 전체 Active-User 데이터베이스 다운로드

다음 명령은 poll-import-user-group-timer의 만료를 기다리지 않고 Active Directory 서버에 쿼리하여 지정된 가져오기 사용자 그룹 데이터베이스를 업데이트합니다.

```
hostname(config)# user-identity update import-user
```

AD 에이전트에서 데이터베이스 다운로드

다음 예는 사용자 데이터베이스가 Active Directory와 동기화되지 않았다고 생각하는 경우 Active Directory 에이전트에서 수동으로 데이터베이스 다운로드를 시작하는 방법을 보여줍니다.

```
hostname(config)# user-identity update active-user-database
```

활성 사용자의 리스트 표시

다음 예는 활성 사용자를 표시하는 방법을 보여줍니다.

```
hostname# show user-identity user active list detail
```

Identify Firewall에는 두 가지 다운로드 모드(Full 및 On-demand)가 있습니다.

- Full download - 사용자가 네트워크에 로그인하면 IDFW는 ASA에 사용자 ID를 즉시 알려줍니다(ASA 5512-X 이상에서 권장).
- On-demand - 사용자가 네트워크에 로그인하면 ASA는 AD(ADHOC)로부터 사용자 ID를 요청합니다.

Cloud Web Security 및 Identity Firewall의 예

다음 예는 ASA에서 Cloud Web Security를 Identity Firewall과 함께 구성하는 방법을 보여줍니다.

```
hostname# sh run
ASA Version 100.8(24)32
!
hostname QFW-201-QASS
domain-name uk.scansafe.net
enable password liqhNWIOSfzvir2g encrypted
passwd liqhNWIOSfzvir2g encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.116.90 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 192.168.114.90 255.255.254.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa100824-32-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name uk.scansafe.net
object network obj0192.168.116.x
 subnet 192.168.116.0 255.255.255.0
access-list 101 extended permit tcp any any eq www
access-list 101 extended permit tcp any any eq https
access-list web extended permit tcp any any eq www
access-list icmp extended permit icmp any any
access-list https extended permit tcp any any eq https
!
scansafe general-options
 server primary ip 192.168.115.225 web 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC26789534f
!
pager lines 24
logging buffered debugging
mtu inside 1500
mtu outside 1500
no failover
```

```
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
!
object network obj0192.168.116.x
 nat (inside,outside) dynamic interface
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.114.19 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AD protocol ldap
aaa-server AD (inside) host 192.168.116.220
 server-port 389
 ldap-base-dn DC=ASASCANLAB,DC=local
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn cn=administrator,cn=Users,dc=asascanlab,dc=local
 server-type microsoft
aaa-server adagent protocol radius
 ad-agent-mode
aaa-server adagent (inside) host 192.168.116.220
 key *****
user-identity domain ASASCANLAB aaa-server AD
user-identity default-domain ASASCANLAB
user-identity action netbios-response-fail remove-user-ip
user-identity poll-import-user-group-timer hours 1
user-identity ad-agent aaa-server adagent
user-identity user-not-found enable
user-identity monitor user-group ASASCANLAB\\GROUP1
user-identity monitor user-group ASASCANLAB\\GROUPNAME
no snmp-server location
no snmp-server contact
crypto ca trustpool policy
telnet timeout 5
ssh 192.168.0.0 255.255.255.0 inside
ssh 192.168.21.0 255.255.255.0 inside
ssh timeout 30
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map cmap-https
 match access-list https
class-map inspection_default
 match default-inspection-traffic
class-map cmap-http
 match access-list web
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map type inspect scansafe ss
 parameters
  default user john group qa
```

```
  HTTP
policy-map type inspect scansafe https-pmap
 parameters
  https
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
policy-map type inspect scansafe http-pmap
 parameters
  default group http-scansafe
  HTTP
policy-map pmap-http
 class cmap-http
  inspect scansafe http-pmap fail-open
 class cmap-https
  inspect scansafe https-pmap fail-open
!
service-policy pmap-http global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:667ba936945b370c394806a63548e7a0
: end
QFW-201-QASS#
```

관련 문서

관련 문서	URL
Cisco ScanSafe Cloud Web Security Configuration Guides	http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

Cisco Cloud Web Security의 기능 기록

표 15-1에는 각 기능 변경 사항 및 그것이 구현된 플랫폼 릴리스가 나열되어 있습니다.

표 15-1 Cloud Web Security 의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
Cloud Web Security	9.0(1)	이 기능이 추가되었습니다. Cisco Cloud Web Security는 웹 트래픽에 대한 콘텐츠 스캐닝 및 기타 악성코드 차단 서비스를 제공합니다. 또한 사용자 ID를 기반으로 웹 트래픽을 리디렉션하고 보고서를 생성할 수 있습니다. 추가 또는 수정된 명령: **class-map type inspect scansafe**, **default user group**, **http[s]** (parameters), **inspect scansafe**, **license**, **match user group**, **policy-map type inspect scansafe**, **retry-count**, **scansafe**, **scansafe general-options**, **server** {**primary** | **backup**}, **show conn scansafe**, **show scansafe server**, **show scansafe statistics**, **user-identity monitor**, **whitelist**.

16 장

위협 감지

이 장에서는 위협 감지 통계를 구성하는 방법 및 스캐닝 위협 감지에 대해 설명합니다.

위협 감지

ASA에서의 위협 감지는 공격에 대한 일선 방어를 제공합니다. 위협 감지는 디바이스의 트래픽에 대한 기준을 만들 수 있도록 레이어 3 및 4에서 작동하며, 트래픽 패턴을 기반으로 패킷 삭제 통계를 분석하고 "상위" 보고서를 축적합니다. 비교해보면, IPS 또는 Next Generation IPS 서비스를 제공하는 모듈은 ASA에서 허용한 트래픽에 대해 최대 레이어 7까지 공격 벡터를 식별 및 완화하며, ASA에 의해 이미 삭제된 트래픽은 볼 수 없습니다. 따라서 위협 감지와 IPS를 함께 사용할 경우 좀 더 포괄적인 위협 방어를 구현할 수 있습니다.

위협 감지는 다음 요소로 구성됩니다.

- 다양한 위협에 대해 수집되는 서로 다른 수준의 통계.

  위협 감지 통계를 사용하면 ASA에 대한 위협을 편리하게 관리할 수 있습니다. 예를 들어, 스캐닝 위협 감지를 활성화하면 통계를 보면서 위협을 분석할 수 있습니다. 두 가지 유형의 위협 감지 통계를 구성할 수 있습니다.

  - 기본 위협 감지 통계 - 시스템 공격 활동에 대한 정보를 전체적으로 포함합니다. 기본 위협 감지 통계는 기본적으로 사용되며 성능에 영향을 미치지 않습니다.
  - 고급 위협 감지 통계 - 객체 수준에서 활동을 추적하므로 ASA는 개별 호스트, 포트, 프로토콜 또는 ACL에 대한 활동을 보고할 수 있습니다. 고급 위협 감지 통계는 수집하는 통계에 따라 성능에 크게 영향을 미칠 수 있으므로, 기본적으로 ACL 통계만 사용됩니다.
- 호스트가 스캔을 수행할 시기를 결정하는 스캐닝 위협 감지. 스캐닝 위협이 될 수 있을 것 같은 호스트는 선택적으로 차단할 수 있습니다.

기본 위협 감지 통계

ASA는 기본 위협 감지 통계를 사용하여 다음과 같은 이유에 따른 보안 이벤트 및 삭제된 패킷의 속도를 모니터링합니다.

- ACL에 의한 거부.
- 불량 패킷 형식(예: invalid-ip-header 또는 invalid-tcp-hdr-length).
- 연결 제한 초과(시스템 전체의 리소스 제한 및 컨피그레이션에 설정된 제한 모두).
- DoS 공격 감지(예: 잘못된 SPI, Stateful Firewall 점검 실패).
- 기본 방화벽 점검 실패. 이 옵션은 리스트의 모든 방화벽 관련 패킷 삭제를 포함하는 결합된 속도입니다. 인터페이스 오버로드, 애플리케이션 검사에서 실패한 패킷, 스캐닝 공격 감지 등 방화벽과 관련되지 않은 삭제는 포함되지 않습니다.
- 의심스러운 ICMP 패킷 감지.
- 애플리케이션 검사 실패 패킷.
- 인터페이스 오버로드.
- 스캐닝 공격 감지. 이 옵션은 스캐닝 공격을 모니터링합니다(예: 첫 번째 TCP 패킷이 SYN 패킷이 아니거나 TCP 연결이 3방향 핸드셰이크에서 실패함). 완전한 스캐닝 위협 감지에서는 이 스캐닝 공격 속도 정보를 사용하여, 예를 들면 호스트를 공격자로 분류하고 자동으로 차단하는 조치를 취합니다.
- 불완전한 세션 감지(예; TCP SYN 공격 감지됨 또는 데이터 UDP 세션 공격이 감지되지 않음)

ASA는 위협을 감지하는 즉시 시스템 로그 메시지(733100)를 전송합니다. ASA는 간격 중의 평균 이벤트 속도와 좀 더 짧은 버스트 간격 중의 버스트 이벤트 속도, 이 두 유형의 속도를 추적합니다. 버스트 속도 간격은 평균 속도 간격의 1/30과 10초 중 더 높은 값입니다. 각 수신 이벤트에 대해 ASA는 평균 및 버스트 속도 제한을 점검합니다. 두 속도 모두 제한을 초과하면 ASA는 버스트 기간당 각 속도 유형에 대해 최대 메시지 하나씩 모두 두 개의 시스템 메시지를 전송합니다.

기본 위협 감지는 삭제 또는 잠재적 위협이 있는 경우에만 성능에 영향을 미칩니다. 이 시나리오에서도 성능 영향력은 크지 않습니다.

고급 위협 감지 통계

고급 위협 감지 통계는 호스트, 포트, 프로토콜, ACL 등 개별 객체에 대한 허용 트래픽 속도 및 삭제 트래픽 속도를 보여줍니다.

주의 고급 통계를 활성화할 경우 통계 유형에 따라 ASA 성능에 영향이 미칠 수 있습니다. 호스트 통계를 활성화하는 **threat-detection statistics host** 명령은 심각한 영향을 미칩니다. 트래픽 로드가 큰 경우에는 이 유형의 통계를 일시적으로만 활성화하는 것이 좋습니다. 그러나 포트 통계를 활성화하는 **threat-detection statistics port** 명령은중간 정도의 영향을 미칩니다.

스캐닝 위협 감지

일반적인 스캐닝 공격은 서브넷의 모든 IP 주소에 대한 액세스 가능성을 테스트하는 호스트로 구성됩니다(서브넷의 많은 호스트를 스캐닝하거나 호스트 또는 서브넷의 많은 포트를 스위핑하여). 스캐닝 위협 감지 기능은 호스트가 스캔을 수행할 시기를 결정합니다. 트래픽 시그니처를 기반으로 하는 IPS 스캔 감지와는 달리 ASA 스캐닝 위협 감지는 스캐닝 활동을 분석할 수 있는 호스트 통계가 포함된 폭넓은 데이터베이스를 유지 관리합니다.

호스트 데이터베이스는 반환 활동이 없는 연결, 닫힌 서비스 포트에 액세스, 비 임의 IPID 등의 취약한 TCP 동작, 기타 많은 동작 등 의심스러운 활동을 추적합니다.

스캐닝 위협 속도가 제한을 초과하면 ASA는 syslog 메시지(733101)를 전송하고, 선택적으로 공격자를 차단합니다. ASA는 간격 중의 평균 이벤트 속도와 좀 더 짧은 버스트 간격 중의 버스트 이벤트 속도, 이 두 유형의 속도를 추적합니다. 버스트 이벤트 속도는 평균 속도 간격의 1/30과 10초 중 더 높은 값입니다. 감지된 이벤트 중 스캐닝 공격의 일부라고 간주되는 각 이벤트에 대해 ASA는 평균 및 버스트 속도 제한을 점검합니다. 호스트에서 전송된 트래픽에 대해 두 속도 중 하나가 제한을 초과하면 해당 호스트는 공격자로 간주됩니다. 호스트에서 수신된 트래픽에 대해 두 속도 중 하나가 제한을 초과하면 해당 호스트는 공격 대상으로 간주됩니다.

다음 표에는 스캐닝 위협 감지의 기본 속도 제한이 나열되어 있습니다.

표 16-1 스캐닝 위협 감지의 기본 속도 제한

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

주의 스캐닝 위협 감지 기능은 호스트 및 서브넷 기반 데이터 구조와 정보를 만들고 수집하는 동안 ASA의 성능 및 메모리에 크게 영향을 미칠 수 있습니다.

위협 감지 지침

보안 컨텍스트 지침

고급 위협 통계를 제외하고 위협 감지는 단일 모드에서만 지원됩니다. 다중 모드에서는 TCP 가로채기 통계만 지원됩니다.

방화벽 모드 지침

투명 및 라우팅된 방화벽 모드에서 지원됩니다.

모니터링하는 트래픽 유형

- Through-the-box 트래픽만 모니터링되고 to-the-box 트래픽은 위협 감지에 포함되지 않습니다.
- ACL에 의해 거부되는 트래픽은 스캐닝 위협 감지를 트리거하지 않습니다. ASA의 통과가 허용되고 흐름을 만드는 트래픽만이 스캐닝 위협 감지의 영향을 받습니다.

위협 감지 기본값

기본 위협 감지 통계는 기본적으로 사용됩니다.

다음 표에는 기본 설정이 나열되어 있습니다. **show running-config all threat-detection** 명령을 사용하거나를 사용하여 이러한 기본 설정을 볼 수 있습니다.

고급 통계의 경우에는 기본적으로 ACL에 대한 통계가 사용됩니다.

표 16-2 기본 위협 감지 기본 설정

패킷 삭제 이유	트리거 설정	
	평균 속도	버스트 속도
• DoS 공격 감지 • 불량 패킷 형식 • 연결 제한 초과 • 의심스러운 ICMP 패킷 감지	지난 600초 동안 초당 100개 삭제	지난 20초 동안 초당 400개 삭제
	지난 3600초 동안 초당 80개 삭제	지난 120초 동안 초당 320개 삭제
스캐닝 공격 감지	지난 600초 동안 초당 5개 삭제	지난 20초 동안 초당 10개 삭제
	지난 3600초 동안 초당 4개 삭제	지난 120초 동안 초당 8개 삭제
불완전한 세션 감지(예: TCP SYN 공격 감지됨 또는 데이터 UDP 세션 공격이 감지되지 않음)(결합됨)	지난 600초 동안 초당 100개 삭제	지난 20초 동안 초당 200개 삭제
	지난 3600초 동안 초당 80개 삭제	지난 120초 동안 초당 160개 삭제
ACL에 의한 거부	지난 600초 동안 초당 400개 삭제	지난 20초 동안 초당 800개 삭제
	지난 3600초 동안 초당 320개 삭제	지난 120초 동안 초당 640개 삭제
• 기본 방화벽 점검 실패 • 애플리케이션 검사 실패 패킷	지난 600초 동안 초당 400개 삭제	지난 20초 동안 초당 1600개 삭제
	지난 3600초 동안 초당 320개 삭제	지난 120초 동안 초당 1280개 삭제
인터페이스 오버로드	지난 600초 동안 초당 2000개 삭제	지난 20초 동안 초당 8000개 삭제
	지난 3600초 동안 초당 1600개 삭제	지난 120초 동안 초당 6400개 삭제

위협 감지 구성

기본 위협 감지 통계는 기본적으로 사용되며, 사용자에게 필요한 유일한 위협 감지 서비스일 수 있습니다. 추가 위협 감지 서비스를 구현하려면 다음 절차를 사용하십시오.

절차

1단계 16-5 페이지의 기본 위협 감지 통계 구성.

기본 위협 감지 통계에는 공격(예: DoS 공격)과 관련될 수 있는 활동이 포함됩니다.

2단계 16-5 페이지의 고급 위협 감지 통계 구성.

3단계 16-7 페이지의 스캐닝 위협 감지 구성.

기본 위협 감지 통계 구성

기본 위협 감지 통계는 기본적으로 사용됩니다. 이 통계를 비활성화할 수도 있고, 비활성화된 경우 다시 활성화할 수도 있습니다.

절차

1단계 기본 위협 감지 통계를 활성화합니다(전에 비활성화한 경우).

```
threat-detection basic-threat
```

예:

```
hostname(config)# threat-detection basic-threat
```

기본 위협 감지는 기본적으로 사용됩니다. 비활성화하려면 **no threat-detection basic-threat**를 사용하십시오.

2단계 (선택 사항) 하나 이상의 이벤트 유형에 대한 기본 설정을 변경합니다.

```
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
```

예:

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

각 이벤트 유형에 대한 자세한 설명은 16-2 페이지의 기본 위협 감지 통계를 참조하십시오.

이 명령과 **scanning-threat** 키워드를 함께 사용할 경우 스캐닝 위협 감지에서도 이 명령이 사용됩니다. 기본 위협 감지를 구성하지 않아도 여전히 이 명령과 **scanning-threat** 키워드를 사용하여 스캐닝 위협 감지에 대한 속도 제한을 구성할 수 있습니다.

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

고급 위협 감지 통계 구성

폭넓은 통계를 수집하려면 ASA를 구성할 수 있습니다. 기본적으로 ACL에 대한 통계는 사용됩니다. 다른 통계를 활성화하려면 다음 단계를 수행하십시오.

절차

1단계 (선택 사항) *모든* 통계를 활성화합니다.

```
threat-detection statistics
```

예:

```
hostname(config)# threat-detection statistics
```

특정 통계만 활성화하려면 각 통계 유형에 대해 이 명령을 입력하고(표 참조), 옵션 없이는 이 명령을 사용하지 마십시오. **threat-detection statistics**(옵션 없이)를 입력한 다음 statistics-specific 옵션과 함께 명령을 입력하여 특정 통계를 사용자 지정할 수 있습니다(예: **threat-detection statistics host number-of-rate 2**). **threat-detection statistics**(옵션 없이)를 입력한 다음 특정 통계에 대한 명령을 입력하면(statistic-specific 옵션 없이), 명령이 이미 활성화되었기 때문에 아무런 효과도 없습니다.

이 명령의 **no** 형식을 입력하면 이미 기본적으로 활성화된 **threat-detection statistics access-list** 명령을 포함하여 모든 **threat-detection statistics** 명령이 제거됩니다.

2단계 (선택 사항) ACL에 대한 통계를 활성화합니다(전에 비활성화한 경우).

```
threat-detection statistics access-list
```

예:

```
hostname(config)# threat-detection statistics access-list
```

ACL에 대한 통계는 기본적으로 사용됩니다. **show threat-detection top access-list** 명령을 사용하면 ACL 통계만 표시됩니다. 이 명령은 기본적으로 사용됩니다.

3단계 (선택 사항) 호스트(**host** 키워드), TCP 및 UDP 포트(**port** 키워드) 또는 비 TCP/UDP IP 프로토콜(**protocol** 키워드)에 대한 통계를 구성합니다.

```
threat-detection statistics {host | port | protocol} [number-of-rate {1 | 2 | 3}]
```

예:

```
hostname(config)# threat-detection statistics host number-of-rate 2

hostname(config)# threat-detection statistics port number-of-rate 2

hostname(config)# threat-detection statistics protocol number-of-rate 3
```

number-of-rate 키워드는 통계용으로 유지되는 속도 간격의 수를 설정합니다. 속도 간격의 기본값은 메모리 사용량 수준이 낮은 **1**입니다. 속도 간격의 수를 늘리려면 값을 **2** 또는 **3**으로 설정하십시오. 예를 들어 값을 **3**으로 설정하면 마지막 1시간, 8시간 및 24시간 동안의 데이터를 볼 수 있습니다. 이 키워드를 **1**(기본값)로 설정하면 가장 짧은 속도 간격 통계만 유지됩니다. 값을 **2**로 설정하면 가장 짧은 간격 두 개가 유지됩니다.

호스트가 활성 상태이고 스캐닝 위협 호스트 데이터베이스에 있는 한 호스트 통계가 누적됩니다. 비활성 상태로 10분이 지나면 호스트는 데이터베이스에서 삭제되고 통계도 지워집니다.

4단계 (선택 사항) TCP 가로채기에서 가로채는 공격에 대한 통계를 구성합니다(TCP 가로채기 활성화 방법은 12 장, “연결 설정”, 참조).

```
threat-detection statistics tcp-intercept [rate-interval minutes]
[burst-rate attacks_per_sec] [average-rate attacks_per_sec]
```

예:

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60 burst-rate
800 average-rate 600
```

rate-interval 키워드는 기록 모니터링 윈도우의 크기를 설정합니다(1~1440분). 기본값은 30분입니다. 이 간격 중에 ASA는 공격 횟수를 30회로 샘플링합니다.

burst-rate 키워드는 syslog 메시지 생성의 임계값을 설정합니다(25~2147483647). 기본값은 초당 400입니다. 버스트 속도가 제한을 초과하면 syslog 메시지 733104가 생성됩니다.

average-rate 키워드는 syslog 메시지 생성의 평균 속도 임계값을 설정합니다(25~2147483647). 기본값은 초당 200입니다. 평균 속도가 제한을 초과하면 syslog 메시지 733105가 생성됩니다.

참고 다른 위협 감지 명령과는 달리 이 명령은 여러 컨텍스트 모드에서 사용 가능합니다.

스캐닝 위협 감지 구성

공격자를 식별하여 선택적으로 차단하도록 스캐닝 위협 감지를 구성할 수 있습니다.

절차

1단계 스캐닝 위협 감지를 활성화합니다.

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

예:

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
```

기본적으로, 호스트가 공격자로 식별되면 시스템 로그 메시지 733101이 생성됩니다. 차단에서 제외할 여러 IP 주소 또는 네트워크 객체 그룹을 지정하려면 이 명령을 여러 번 입력합니다.

2단계 (선택 사항) 공격 호스트의 차단 기간을 설정합니다.

threat-detection scanning-threat shun duration *seconds*

예:

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

3단계 (선택 사항) ASA가 호스트를 공격자 또는 대상으로 식별할 경우 기본 이벤트 제한을 변경합니다.

threat-detection rate scanning-threat rate-interval *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

예:

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

기본 위협 감지 컨피그레이션에서 이 명령을 이미 구성한 경우 스캐닝 위협 감지 기능에서도 해당 설정이 공유됩니다. 기본 위협 감지와 스캐닝 위협 감지에 대해 속도를 별도로 구성할 수 없습니다. 이 명령을 사용해 속도를 설정하지 않으면 기본 위협 감지 기능과 스캐닝 위협 감지 기능에 대해 모두 기본값이 사용됩니다. 별도의 명령을 입력하여 최대 3개의 서로 다른 속도 간격을 구성할 수 있습니다.

위협 감지 모니터링

다음 항목에서는 위협 감지를 모니터링하고 트래픽 통계를 보는 방법에 대해 설명합니다.

기본 위협 감지 통계 모니터링

기본 위협 감지 통계를 표시하려면 다음 명령을 사용합니다.

```
show threat-detection rate [min-display-rate min_display_rate]
[acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop |
icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack]
```

min-display-rate *min_display_rate* 인수는 최소 표시 속도를 초과하는 통계의 디스플레이를 제한합니다(초당 이벤트 수 단위). *min_display_rate*는 0~2147483647 범위에서 설정할 수 있습니다.

나머지 인수들로는 특정 범주에 대한 디스플레이를 제한할 수 있습니다. 각 이벤트 유형에 대한 자세한 설명은 16-2 페이지의 기본 위협 감지 통계를 참조하십시오.

아래의 출력은 두 개의 고정된 기간(마지막 10분 및 마지막 1시간) 동안 초당 이벤트 수 단위로 평균 속도를 보여줍니다. 그 밖에 마지막 완료된 버스트 간격 동안의 현재 버스트 속도로 평균 속도 간격의 1/30 또는 10초 중 더 큰 것(초당 이벤트 수 단위), 속도가 초과된(트리거된) 횟수, 기간 동안의 총 이벤트 수도 보여줍니다.

ASA는 총 30개의 완료된 버스트 간격에 대해 각 버스트 기간의 끝에 개수를 저장합니다. 현재 진행 중인 완료되지 않은 버스트 간격은 평균 속도에 포함되지 않습니다. 예를 들어, 평균 속도 간격이 20분이면 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20이었고 3:00:25에 **show** 명령을 사용하면 마지막 5초는 출력에 포함되지 않습니다.

이 규칙의 유일한 예외는, 총 이벤트 수를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(30개 중 1번)의 이벤트 수를 이미 초과하는 경우입니다. 이 경우 ASA는 총 이벤트 수를 마지막 29개의 완료된 간격으로 계산하고 여기에 완료되지 않은 버스트 간격에서 지금까지의 이벤트 수를 더합니다. 이 예외 덕분에 실시간 이벤트가 크게 증가하는 상황을 모니터링할 수 있습니다.

clear threat-detection rate 명령을 사용하여 통계를 지울 수 있습니다.

다음은 **show threat-detection rate** 명령의 샘플 출력입니다.

```
hostname# show threat-detection rate

                        Average(eps)     Current(eps) Trigger         Total events
  10-min ACL  drop:                0                0       0                   16
  1-hour ACL  drop:                0                0       0                  112
  1-hour SYN attck:                5                0       2                21438
  10-min  Scanning:                0                0      29                  193
  1-hour  Scanning:              106                0      10               384776
  1-hour Bad  pkts:               76                0       2               274690
  10-min  Firewall:                0                0       3                   22
  1-hour  Firewall:               76                0       2               274844
  10-min DoS attck:                0                0       0                    6
  1-hour DoS attck:                0                0       0                   42
  10-min Interface:                0                0       0                  204
  1-hour Interface:               88                0       0               318225
```

고급 위협 감지 통계 모니터링

고급 위협 감지 통계를 모니터링하려면 다음 표에 있는 명령을 사용하십시오. 화면 출력에는 다음이 표시됩니다.

- 고정된 기간 동안의 평균 속도(초당 이벤트 수 단위).
- 마지막 완료된 버스트 간격 동안의 현재 버스트 속도로 평균 속도 간격의 1/30 또는 10초 중 더 큰 것(초당 이벤트 수 단위)

- 속도가 초과된 횟수(삭제된 트래픽 통계 전용)
- 고정된 기간 동안의 총 이벤트 수

ASA는 총 30개의 완료된 버스트 간격에 대해 각 버스트 기간의 끝에 개수를 저장합니다. 현재 진행 중인 완료되지 않은 버스트 간격은 평균 속도에 포함되지 않습니다. 예를 들어, 평균 속도 간격이 20분이면 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20이었고 3:00:25에 **show** 명령을 사용하면 마지막 5초는 출력에 포함되지 않습니다.

이 규칙의 유일한 예외는, 총 이벤트 수를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(30개 중 1번)의 이벤트 수를 이미 초과하는 경우입니다. 이 경우 ASA는 총 이벤트 수를 마지막 29개의 완료된 간격으로 계산하고 여기에 완료되지 않은 버스트 간격에서 지금까지의 이벤트 수를 더합니다. 이 예외 덕분에 실시간 이벤트가 크게 증가하는 상황을 모니터링할 수 있습니다.

명령	목적
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] **detail**]]	상위 10개 통계를 표시합니다. 옵션을 입력하지 않으면 모든 범주의 상위 10개 통계가 표시됩니다. **min-display-rate** *min_display_rate* 인수는 최소 표시 속도를 초과하는 통계의 디스플레이를 제한합니다(초당 이벤트 수 단위). *min_display_rate*는 0~2147483647 범위에서 설정할 수 있습니다. 아래의 행에서는 선택적인 키워드에 대해 설명합니다.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top access-list** [**rate-1** | **rate-2** | **rate-3**]	패킷과 일치하는 상위 10개 ACE(허용 및 거부 ACE 모두 포함)를 보려면 **access-list** 키워드를 사용하십시오. 이 디스플레이에서는 허용된 트래픽과 거부된 트래픽이 구분되지 않습니다. **threat-detection basic-threat** 명령을 사용하여 기본 위협 감지를 활성화한 경우 **show threat-detection rate acl-drop** 명령을 사용하여 ACL 거부를 추적할 수 있습니다. **rate-1** 키워드는 디스플레이에서 이용할 수 있는 가장 작은 고정 속도 간격에 대한 통계를 보여줍니다. **rate-2**는 두 번째로 가장 큰 속도 간격을 보여주고, **rate-3**은 가장 큰 속도 간격을 보여줍니다(3개 간격을 정의한 경우). 예를 들면 디스플레이에 마지막 1시간, 8시간 및 24시간에 대한 통계가 표시됩니다. **rate-1** 키워드를 설정하면 ASA는 1시간 간격만 표시합니다.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top host** [**rate-1** | **rate-2** | **rate-3**]	호스트 통계만 보려면 **host** 키워드를 사용하십시오. **참고:** 위협 감지 알고리즘 때문에, 장애 조치 및 상태 링크로 사용된 인터페이스가 상위 10개 호스트에 나타날 수 있습니다. 이는 예상되는 동작이므로 디스플레이의 IP 주소를 무시할 수 있습니다.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top port-protocol** [**rate-1** | **rate-2** | **rate-3**]	포트 및 프로토콜에 대한 통계를 보려면 **port-protocol** 키워드를 사용하십시오. **port-protocol** 키워드는 포트 및 프로토콜에 대한 통계를 보여주며(둘 다 표시하도록 활성화해야 함), TCP/UDP 포트 및 IP 프로토콜 유형이 결합된 통계도 보여줍니다. TCP(프로토콜 6) 및 UDP(프로토콜 17)는 IP 프로토콜에 대한 디스플레이에 포함되지 않습니다. 그러나 TCP 및 UDP 포트는 포트의 디스플레이에 포함됩니다. 이러한 유형, 포트 또는 프로토콜 중 하나에 대한 통계만 활성화하는 경우 활성화된 통계만 볼 수 있습니다.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **top tcp-intercept** [**all**] **detail**]]	TCP 가로채기 통계를 보려면 **tcp-intercept** 키워드를 사용하십시오. 공격을 받은 상위 10개의 보호된 서버가 표시됩니다. **all** 키워드는 추적된 모든 서버의 기록 데이터를 보여줍니다. **detail** 키워드는 기록 샘플링 데이터를 보여줍니다. 이 속도 간격 중에 ASA는 공격 횟수를 30회로 샘플링하므로, 기본값인 30분 동안 60초마다 통계가 수집됩니다.

명령	목적
show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]	모든 호스트 또는 특정 호스트나 서브넷에 대한 통계를 표시합니다.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[**-***end_port*]]	모든 포트 또는 특정 포트나 포트 범위에 대한 통계를 표시합니다.
show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | **ah** | **eigrp** | **esp** | **gre** | **icmp** | **icmp6** | **igmp** | **igrp** | **ip** | **ipinip** | **ipsec** | **nos** | **ospf** | **pcp** | **pim** | **pptp** | **snp** | **tcp** | **udp**]	모든 IP 프로토콜 또는 특정 프로토콜에 대한 통계를 표시합니다. *protocol_number* 인수는 0~255 사이의 인수입니다.

호스트 위협 감지 통계 평가

다음은 **show threat-detection statistics host** 명령의 샘플 출력입니다.

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:              2938              0       0             10580308
  8-hour Sent byte:               367              0       0             10580308
 24-hour Sent byte:               122              0       0             10580308
  1-hour Sent pkts:                28              0       0               104043
  8-hour Sent pkts:                 3              0       0               104043
 24-hour Sent pkts:                 1              0       0               104043
  20-min Sent drop:                 9              0       1                10851
  1-hour Sent drop:                 3              0       1                10851
  1-hour Recv byte:              2697              0       0              9712670
  8-hour Recv byte:               337              0       0              9712670
 24-hour Recv byte:               112              0       0              9712670
  1-hour Recv pkts:                29              0       0               104846
  8-hour Recv pkts:                 3              0       0               104846
 24-hour Recv pkts:                 1              0       0               104846
  20-min Recv drop:                42              0       3                50567
  1-hour Recv drop:                14              0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                 0              0       0                  614
  8-hour Sent byte:                 0              0       0                  614
 24-hour Sent byte:                 0              0       0                  614
  1-hour Sent pkts:                 0              0       0                    6
  8-hour Sent pkts:                 0              0       0                    6
 24-hour Sent pkts:                 0              0       0                    6
  20-min Sent drop:                 0              0       0                    4
  1-hour Sent drop:                 0              0       0                    4
  1-hour Recv byte:                 0              0       0                  706
  8-hour Recv byte:                 0              0       0                  706
 24-hour Recv byte:                 0              0       0                  706
  1-hour Recv pkts:                 0              0       0                    7
```

다음 표는 출력에 대해 설명합니다.

표 16-3 위협 감지 통계 호스트 표시

필드	설명
호스트	호스트 IP 주소입니다.
tot-ses	데이터베이스에 추가된 이후 이 호스트에 대한 총 세션의 수입니다.
act-ses	호스트가 현재 관련되어 있는 총 활성 세션의 수입니다.
fw-drop	방화벽 삭제의 수입니다. 방화벽 삭제는 기본 위협 감지에서 추적된 모든 방화벽 관련 패킷 삭제를 포함하는 결합된 속도입니다. 여기에는 ACL 거부, 불량 패킷, 연결 제한 초과, DoS 공격 패킷, 의심스러운 ICMP 패킷, TCP SYN 공격 패킷, 데이터 없는 UDP 공격 패킷이 포함됩니다. 인터페이스 오버로드, 애플리케이션 검사에서 실패한 패킷, 스캐닝 공격 감지 등 방화벽과 관련되지 않은 삭제는 포함되지 않습니다.
insp-drop	애플리케이션 검사에 실패하여 삭제된 패킷의 수입니다.
null-ses	Null 세션의 수입니다. 3초 시간 제한 내에 완료되지 않은 TCP SYN 세션 및 세션이 시작된 이후 3초 동안 서버에서 전송한 데이터가 없는 UDP 세션이 포함됩니다.
bad-acc	닫힌 상태의 호스트 포트에 대한 불량 액세스 시도 횟수입니다. 포트가 null 세션인 것으로 확인되면(null-ses 필드 설명 참조) 호스트의 포트 상태가 HOST_PORT_CLOSE로 설정됩니다. 호스트의 포트에 액세스하는 모든 클라이언트는 시간 제한 동안 기다릴 필요도 없이 즉시 불량 액세스로 분류됩니다.
Average(eps)	각 기간 동안의 평균 속도입니다(초당 이벤트 수 단위). ASA는 총 30개의 완료된 버스트 간격에 대해 각 버스트 기간의 끝에 개수를 저장합니다. 현재 진행 중인 완료되지 않은 버스트 간격은 평균 속도에 포함되지 않습니다. 예를 들어, 평균 속도 간격이 20분이면 버스트 간격은 20초입니다. 마지막 버스트 간격이 3:00:00~3:00:20이었고 3:00:25에 **show** 명령을 사용하면 마지막 5초는 출력에 포함되지 않습니다. 이 규칙의 유일한 예외는, 총 이벤트 수를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(30개 중 1번)의 이벤트 수를 이미 초과하는 경우입니다. 이 경우 ASA는 총 이벤트 수를 마지막 29개의 완료된 간격으로 계산하고 여기에 완료되지 않은 버스트 간격에서 지금까지의 이벤트 수를 더합니다. 이 예외 덕분에 실시간 이벤트가 크게 증가하는 상황을 모니터링할 수 있습니다.
Current(eps)	마지막 완료된 버스트 간격 동안의 현재 버스트 속도로 평균 속도 간격의 1/30 또는 10초 중 더 큰 것입니다(초당 이벤트 수 단위). Average(eps) 설명에 나와 있는 예에서 현재 속도는 3:19:30~3:20:00의 속도입니다.
Trigger	삭제된 패킷 속도 제한이 초과된 횟수입니다. 전송/수신 바이트와 패킷 행에서 식별된 유효한 트래픽의 경우에는 이 값이 항상 0입니다. 유효한 트래픽에 대한 트리거에는 속도 제한이 없기 때문입니다.

표 16-3 위협 감지 통계 호스트 표시 (계속)

필드	설명
Total events	각 속도 간격 동안의 총 이벤트 수입니다. 현재 진행 중인 완료되지 않은 버스트 간격은 총 이벤트 수에 포함되지 않습니다. 이 규칙의 유일한 예외는, 총 이벤트 수를 계산할 때 완료되지 않은 버스트 간격의 이벤트 수가 가장 오래된 버스트 간격(30개 중 1번)의 이벤트 수를 이미 초과하는 경우입니다. 이 경우 ASA는 총 이벤트 수를 마지막 29개의 완료된 간격으로 계산하고 여기에 완료되지 않은 버스트 간격에서 지금까지의 이벤트 수를 더합니다. 이 예외 덕분에 실시간 이벤트가 크게 증가하는 상황을 모니터링할 수 있습니다.
20-min, 1-hour, 8-hour, and 24-hour	고정된 속도 간격에 대한 통계입니다. 각 간격에서: • Sent byte - 호스트에서 성공적으로 전송한 바이트의 수입니다. • Sent pkts - 호스트에서 성공적으로 전송한 패킷의 수입니다. • Sent drop - 호스트에서 전송한 패킷 중 스캐닝 공격의 일부이기 때문에 삭제된 패킷의 수입니다. • Recv byte - 호스트에서 성공적으로 수신한 바이트의 수입니다. • Recv pkts - 호스트에서 성공적으로 수신한 패킷의 수입니다. • Recv drop - 호스트에서 수신한 패킷 중 스캐닝 공격의 일부이기 때문에 삭제된 패킷의 수입니다.

차단된 호스트, 공격자 및 대상 모니터링

차단된 호스트, 공격자 및 대상을 모니터링하려면 다음 명령을 사용하십시오.

- **show threat-detection shun**

  현재 차단된 호스트가 표시됩니다. 예:

  ```
  hostname# show threat-detection shun
  Shunned Host List:
  10.1.1.6
  192.168.6.7
  ```

- **clear threat-detection shun** [*ip_address* [*mask*]]

  호스트의 차단 상태를 해제합니다. IP 주소를 지정하지 않으면 차단 리스트에서 모든 호스트가 지워집니다.

  예를 들어 10.1.1.6의 호스트를 해제하려면 다음 명령을 입력합니다.

  ```
  hostname# clear threat-detection shun 10.1.1.6
  ```

- **show threat-detection scanning-threat** [**attacker** | **target**]

  ASA에서 공격자로 지정한 호스트(차단 리스트에 있는 호스트 포함) 및 공격 대상인 호스트를 표시합니다. 옵션을 입력하지 않으면 공격자 및 대상 호스트가 모두 표시됩니다. 예:

  ```
  hostname# show threat-detection scanning-threat attacker
  10.1.2.3
  10.8.3.6
  209.165.200.225
  ```

위협 감지의 예

다음 예는 기본 위협 감지 통계를 구성하며, DoS 공격 속도 설정을 변경합니다. 모든 고급 위협 감지 통계가 활성화되며, 속도 간격의 호스트 통계 숫자가 2로 줄어듭니다. TCP 가로채기 속도 간격도 사용자 지정됩니다. 10.1.1.0/24를 제외한 모든 주소가 자동으로 차단되면서 스캐닝 위협 감지가 활성화됩니다. 스캐닝 위협 속도 간격이 사용자 지정됩니다.

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

위협 감지의 기록

기능 이름	플랫폼 릴리스	설명
기본 및 고급 위협 감지 통계, 스캐닝 위협 감지	8.0(2)	기본 및 고급 위협 감지 통계, 스캐닝 위협 감지가 추가됨. 추가된 명령: **threat-detection basic-threat**, **threat-detection rate**, **show threat-detection rate**, **clear threat-detection rate, threat-detection statistics**, **show threat-detection statistics**, **threat-detection scanning-threat**, **threat-detection rate scanning-threat**, **show threat-detection scanning-threat**, **show threat-detection shun**, **clear threat-detection shun**.
차단 기간	8.0(4)/8.1(2)	이제 차단 기간을 설정할 수 있습니다. 추가된 명령: **threat-detection scanning-threat shun duration**.
TCP 가로채기 통계	8.0(4)/8.1(2)	TCP 가로채기 통계가 추가되었습니다. 수정 또는 추가된 명령: **threat-detection statistics tcp-intercept**, **show threat-detection statistics top tcp-intercept**, **clear threat-detection statistics**.
호스트 통계 속도 간격 사용자 지정	8.1(2)	이제 통계를 수집할 속도 간격의 수를 사용자 지정할 수 있습니다. 속도의 기본값이 3에서 1로 변경되었습니다. 수정된 명령: **threat-detection statistics host number-of-rates**.
버스트 속도 간격이 평균 속도의 1/30로 변경됨	8.2(1)	이전 릴리스에서는 버스트 속도 간격이 평균 속도의 1/60이었습니다. 메모리 사용을 최대화하기 위해 평균 속도 중에 샘플링 간격이 30회로 줄었습니다.

기능 이름	플랫폼 릴리스	설명
포트 및 프로토콜 통계 속도 간격 사용자 지정	8.3(1)	이제 통계를 수집할 속도 간격의 수를 사용자 지정할 수 있습니다. 속도의 기본값이 3에서 1로 변경되었습니다. 수정된 명령: **threat-detection statistics port number-of-rates**, **threat-detection statistics protocol number-of-rates**.
메모리 사용 개선	8.3(1)	위협 감지의 메모리 사용이 개선되었습니다. 추가된 명령: **show threat-detection memory**.

파 트 6

ASA 모듈

ASA FirePOWER(SFR) 모듈

이 장에서는 ASA에서 실행되는 ASA FirePOWER 모듈을 구성하는 방법에 대해 설명합니다.

ASA FirePOWER 모듈

ASA FirePOWER 모듈은 NGIPS(Next-Generation IPS), AVC(Application Visibility and Control), URL 필터링, AMP(Advanced Malware Protection)를 비롯한 차세대 방화벽 서비스를 제공합니다. 단일/다중 컨텍스트 모드 및 라우팅된/투명 모드에서 이 모듈을 사용할 수 있습니다.

이 모듈을 ASA SFR이라고도 합니다.

모듈에 초기 컨피그레이션과 문제 해결을 위한 기본적인 CLI(명령줄 인터페이스)가 있지만 별도의 애플리케이션인 FireSIGHT Management Center를 사용하여 디바이스에서 보안 정책을 구성할 수 있습니다. 이 애플리케이션은 별도의 FireSIGHT Management Center 어플라이언스에서 또는 VMware 서버에서 실행되는 가상 어플라이언스로서 호스팅할 수 있습니다. (FireSIGHT Management Center를 Defense Center라고도 합니다.)

모듈이 ASA에서 ASA FirePOWER작동하는 방식

ASA FirePOWER 모듈은 ASA에서 별도의 애플리케이션을 실행합니다. 모듈은 하드웨어 모듈(ASA 5585-X) 또는 소프트웨어 모듈(5512-X~5555-X)일 수 있습니다. 하드웨어 모듈인 경우 디바이스에는 별도의 관리 및 콘솔 포트, 그리고 ASA에서는 직접 사용하지만 모듈 자체에서는 사용하지 않는 추가 데이터 인터페이스가 포함됩니다.

패시브("모니터 전용") 또는 인라인 배포에서 디바이스를 구성할 수 있습니다.

- 패시브 배포에서는 트래픽의 복사본이 디바이스로 전송되지만 ASA로 반환되지는 않습니다. 패시브 모드에서는 네트워크에 영향을 미치지 않은 채, 디바이스가 트래픽에 대해 무엇을 수행했는지를 알 수 있으며, 트래픽의 내용을 평가할 수 있습니다.
- 인라인 배포 시에는 실제 트래픽이 디바이스로 전송되며, 디바이스의 정책이 트래픽에 영향을 미칩니다. 원하지 않는 트래픽을 취소하고 정책에 의해 적용되는 다른 작업을 수행한 후 추가 처리 및 최종 전송을 위해 트래픽을 ASA로 반환합니다.

다음 섹션에서는 이러한 모드에 대해 좀 더 자세히 설명합니다.

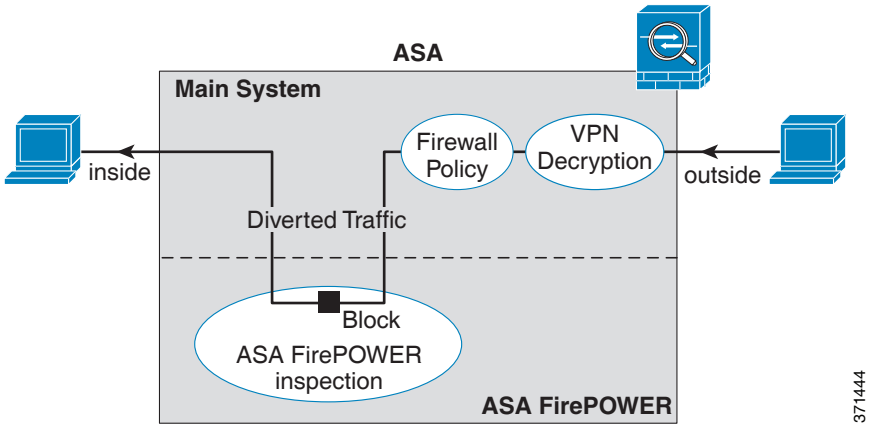
ASA FirePOWER 인라인 모드

인라인 모드에서는 트래픽이 방화벽 점검을 통과한 후 ASA FirePOWER 모듈로 전달됩니다. ASA에서 ASA FirePOWER 검사를 통해 트래픽을 식별할 경우, ASA 및 모듈에서 트래픽이 다음과 같이 흐릅니다.

1. 트래픽이 ASA로 들어갑니다.
2. 들어오는 VPN 트래픽이 암호 해독됩니다.
3. 방화벽 정책이 적용됩니다.
4. 트래픽이 ASA FirePOWER 모듈로 전송됩니다.
5. ASA FirePOWER 모듈이 보안 정책을 트래픽에 적용하고 적절한 작업을 수행합니다.
6. 유효한 트래픽은 ASA로 다시 전송됩니다. ASA FirePOWER 모듈은 자체 보안 정책에 따라 일부 트래픽을 차단할 수 있으며, 그러한 트래픽은 전달되지 않습니다.
7. 나가는 VPN 트래픽이 암호화됩니다.
8. 트래픽이 ASA를 빠져나갑니다.

다음 그림은 인라인 모드에서 ASA FirePOWER 모듈 사용 시 트래픽 흐름을 보여줍니다. 이 예에서 모듈은 특정 애플리케이션에 대해 허용되지 않는 트래픽을 차단합니다. 다른 모든 트래픽은 ASA를 통해 전달됩니다.

그림 17-1 ASA에서 ASA FirePOWER 모듈 트래픽 흐름



참고 두 개의 ASA 인터페이스에 있는 호스트가 연결되어 있는데 ASA FirePOWER 서비스 정책이 그중 하나에 대해서만 구성되어 있으면 비 ASA FirePOWER 인터페이스에서 시작된 트래픽을 포함하여 두 호스트 간 모든 트래픽이 ASA FirePOWER 모듈로 전송됩니다(이 기능은 양방향이기 때문).

ASA FirePOWER 패시브(모니터 전용) 모드

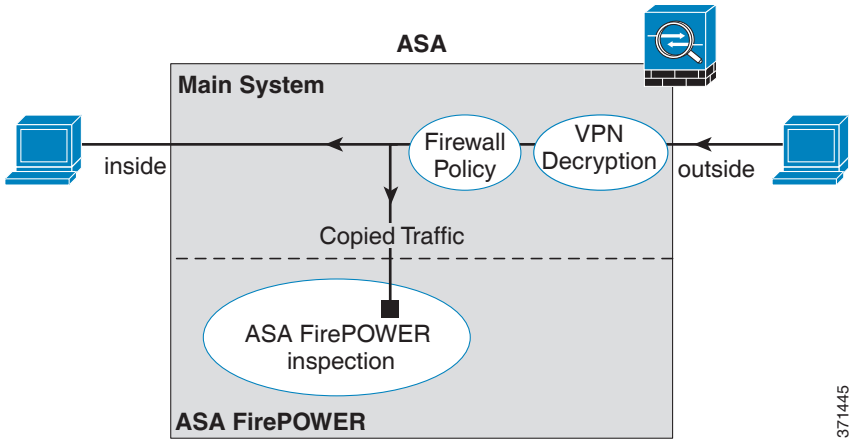
모니터 전용 모드의 트래픽 흐름은 인라인 모드의 경우와 같습니다. 유일한 차이점은 ASA FirePOWER 모듈이 트래픽을 ASA로 다시 전달하지 않는다는 것입니다. 대신 모듈은 보안 정책을 트래픽에 적용하고, 인라인 모드였다면 어떤 일이 발생했을 것인지(예: 트래픽이 "삭제되었을 것"이라고 표시)를 사용자에게 알려줍니다. 이 정보를 사용하여 트래픽을 분석하고 인라인 모드가 바람직한지를 판단할 수 있습니다.

패시브 모드를 구성하려면, 트래픽을 모듈로 리디렉션하는 서비스 정책에 모니터 전용 표시를 포함해야 합니다.

참고 ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수 없습니다. 보안 정책 유형은 하나만 허용됩니다. 다중 컨텍스트 모드에서는 일부 컨텍스트에 대해 모니터 전용 모드를 구성할 수 없고, 다른 컨텍스트에 대해 일반 인라인 모드를 구성할 수 없습니다.

다음 그림은 패시브 모드에서 운영되는 트래픽 흐름을 보여줍니다.

그림 17-2 ASA FirePOWER 패시브, 모니터 전용 모드



ASA FirePOWER 관리 액세스

ASA FirePOWER 모듈을 관리하기 위한 두 개의 액세스 레이어, 즉 초기 컨피그레이션(및 후속 문제 해결) 레이어와 정책 관리 레이어가 있습니다.

- 17-4 페이지의 초기 컨피그레이션
- 17-5 페이지의 정책 컨피그레이션 및 관리

초기 컨피그레이션

초기 컨피그레이션의 경우 ASA FirePOWER 모듈에서 CLI를 사용해야 합니다. 기본 관리 주소에 대한 자세한 내용은 17-7 페이지의 ASA FirePOWER의 기본값을 참조하십시오.

CLI에 액세스하려면 다음 방법을 사용할 수 있습니다.

- ASA 5585-X:
  - ASA FirePOWER 콘솔 포트 - 모듈의 콘솔 포트는 별도의 외부 콘솔 포트입니다.
  - SSH를 사용하는 ASA FirePOWER Management 1/0 인터페이스 - 기본 IP 주소에 연결하거나, ASDM을 사용하여 관리 IP 주소를 변경한 다음 SSH를 사용하여 연결할 수 있습니다. 모듈의 관리 인터페이스는 별도의 외부 기가비트 이더넷 인터페이스입니다.

  참고 **session** 명령을 사용하여 ASA 백플레인을 통해 ASA FirePOWER 하드웨어 모듈 CLI에 액세스할 수 없습니다.

- ASA 5512-X~ASA 5555-X:
  - 백플레인을 통한 ASA 세션 - ASA에 CLI 액세스가 가능한 경우 모듈에 대한 세션을 시작하고 모듈 CLI에 액세스할 수 있습니다.

– SSH를 사용하는 ASA FirePOWER Management 0/0 인터페이스 - 기본 IP 주소에 연결하거나, ASDM을 사용하여 관리 IP 주소를 변경한 다음 SSH를 사용하여 연결할 수 있습니다. 이러한 모델은 ASA FirePOWER 모듈을 소프트웨어 모듈로서 실행합니다. ASA FirePOWER 관리 인터페이스는 Management 0/0 인터페이스를 ASA와 공유합니다. ASA 및 ASA FirePOWER 모듈에 대해 별도의 MAC 주소와 IP 주소가 지원됩니다. ASA FirePOWER 운영 체제 내에서 ASA FirePOWER IP 주소를 구성해야 합니다(CLI 또는 ASDM 사용). 그러나 물리적 특성(예: 인터페이스 활성화)은 ASA에서 구성됩니다. 이 인터페이스를 ASA FirePOWER 전용 인터페이스로 지정하려면 ASA 인터페이스 컨피그레이션(특히 인터페이스 이름)을 제거할 수 있습니다. 이 인터페이스는 관리 전용입니다.

정책 컨피그레이션 및 관리

초기 컨피그레이션을 수행한 후 FireSIGHT Management Center를 사용하여 ASA FirePOWER를 구성합니다. 그런 다음 ASDM 또는 Cisco Security Manager를 사용하여 ASA FirePOWER 모듈로 트래픽을 전송하기 위한 ASA 정책을 구성합니다.

ASA 기능과의 호환성

ASA에는 HTTP 검사를 비롯한 많은 고급 애플리케이션 검사 기능이 포함되어 있습니다. 그러나 ASA FirePOWER 모듈은 ASA에서 제공하는 것보다 더 향상된 HTTP 검사 기능은 물론, 애플리케이션 사용량 모니터링과 제어 등 애플리케이션에 대한 추가 기능도 제공합니다.

ASA FirePOWER 모듈 기능을 충분히 활용하려면 ASA FirePOWER 모듈로 전송하는 트래픽에 대한 다음 지침을 참조하십시오.

- HTTP 트래픽에 대해 ASA 검사를 구성하지 마십시오.
- Cloud Web Security(ScanSafe) 검사를 구성하지 마십시오. 동일한 트래픽에 대해 ASA FirePOWER 검사와 Cloud Web Security 검사를 모두 구성하면 ASA에서는 ASA FirePOWER 검사만 수행합니다.
- 기본 검사를 비롯하여 ASA에서 수행하는 기타 애플리케이션 검사는 ASA FirePOWER 모듈과 호환됩니다.
- MUS(Mobile User Security) 서버를 활성화하지 마십시오. ASA FirePOWER 모듈과 호환되지 않습니다.
- 장애 조치를 활성화한 경우 ASA가 장애 조치되면 기존 ASA FirePOWER 흐름이 새로운 ASA로 전송됩니다. 새로운 ASA의 ASA FirePOWER 모듈은 해당 시점부터 트래픽 검사를 시작하며 이전 검사 상태는 전송되지 않습니다.

ASA FirePOWER 모듈의 라이센싱 요구 사항

ASA FirePOWER 모듈과 FireSIGHT Management Center에는 추가 라이센스가 필요합니다. 이러한 라이센스는 ASA의 컨텍스트보다는 모듈 자체에 설치해야 합니다. ASA 자체에는 추가 라이센스가 필요하지 않습니다.

자세한 내용은 *FireSIGHT System User Guide*의 Licensing 장 또는 FireSIGHT Management Center의 온라인 도움말을 참조하십시오.

ASA FirePOWER 지침

장애 조치 지침

장애 조치를 직접 지원하지 않습니다. ASA가 장애 조치되면 기존 ASA FirePOWER 흐름이 새로운 ASA로 전송됩니다. 새로운 ASA의 ASA FirePOWER 모듈은 해당 시점부터 트래픽 검사를 시작하며 이전 검사 상태는 전송되지 않습니다.

일관된 장애 조치 동작을 보장하려면 고가용성 ASA 쌍의 ASA FirePOWER 모듈에 대해 일관된 정책을 유지 관리해야 합니다(FireSIGHT Management Center 사용).

ASA 클러스터링 지침

클러스터링을 직접 지원하지 않지만 클러스터에서 이러한 모듈을 사용할 수 있습니다. FireSIGHT Management Center를 사용하여 클러스터의 ASA FirePOWER 모듈에 대해 일관된 정책을 유지 관리해야 합니다. 클러스터의 디바이스에 대해 서로 다른 ASA 인터페이스 기반 영역 정의를 사용하지 마십시오.

모델 지침

- ASA 5585-X(하드웨어 모듈) 및 5512-X~ASA 5555-X(소프트웨어 모듈)에서 지원됩니다. 자세한 내용은 *Cisco ASA Compatibility Matrix*를 참조하십시오.

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X~ASA 5555-X의 경우 Cisco SSD(Solid State Drive)를 설치해야 합니다. 자세한 내용은 ASA 5500-X 하드웨어 지침을 참조하십시오.

추가 지침 및 제한

- 17-5 페이지의 ASA 기능과의 호환성섹션을 참조하십시오.
- 하드웨어 모듈에 설치된 소프트웨어 유형을 변경할 수 없습니다. ASA FirePOWER 모듈을 구매하면 나중에 여기에 다른 소프트웨어를 설치할 수 없습니다.
- ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수 없습니다. 보안 정책 유형은 하나만 허용됩니다. 다중 컨텍스트 모드에서는 일부 컨텍스트에 대해 모니터 전용 모드를 구성할 수 없고, 다른 컨텍스트에 대해 일반 인라인 모드를 구성할 수 없습니다.

ASA FirePOWER의 기본값

다음 표에는 ASA FirePOWER 모듈의 기본 설정이 나열되어 있습니다.

표 17-1 ASA FirePOWER 기본 네트워크 매개변수

매개변수	기본값
관리 IP 주소	• 시스템 소프트웨어 이미지: 192.168.45.45/24 • 부트 이미지: – ASA 5585-X: Management 1/0 192.168.8.8/24 – ASA 5512-X~ASA 5555-X: Management 0/0 192.168.1.2/24
게이트웨이	• 시스템 소프트웨어 이미지: 없음 • 부트 이미지: – ASA 5585-X: 192.168.8.1/24 – ASA 5512-X~ASA 5555-X: 192.168.1.1/24
SSH 또는 세션 사용자 이름	admin
비밀번호	• 시스템 소프트웨어 이미지: **Sourcefire** • 부트 이미지: **Admin123**

ASA FirePOWER 모듈 구성

ASA FirePOWER 모듈 컨피그레이션은 ASA FirePOWER 모듈에서 ASA FirePOWER 보안 정책을 구성하고 ASA FirePOWER 모듈에 트래픽을 전송하도록 ASA를 구성하는 프로세스입니다. ASA FirePOWER 모듈을 구성하려면 다음 단계를 수행하십시오.

1단계 17-8 페이지의 ASA FirePOWER 관리 인터페이스 연결. ASA FirePOWER 관리 인터페이스 및 선택적으로 콘솔 인터페이스를 연결합니다.

2단계 17-10 페이지의 (ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 설치 또는 재이미지화.

3단계 필요한 경우 17-14 페이지의 ASA FirePOWER 관리 IP 주소 변경.초기 SSH 액세스에 필요할 수 있습니다.

4단계 17-15 페이지의 ASA FirePOWER CLI에서 기본 ASA FirePOWER 설정 구성. ASA FirePOWER 모듈에서 수행합니다.

5단계 17-16 페이지의 FireSIGHT Management Center에 ASA FirePOWER 추가.이를 통해 디바이스를 관리할 FireSIGHT Management Center를 식별합니다.

6단계 17-17 페이지의 ASA FirePOWER 모듈에서 보안 정책 구성.

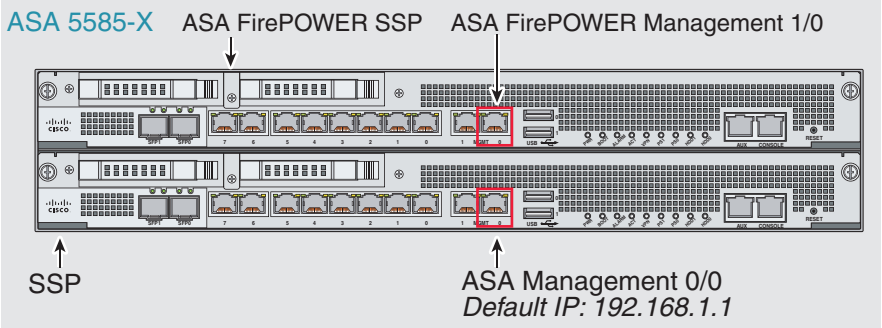
7단계 17-18 페이지의 ASA FirePOWER 모듈로 트래픽 리디렉션.

ASA FirePOWER 관리 인터페이스 연결

ASA FirePOWER 관리 인터페이스는 ASA FirePOWER 모듈에 대한 관리 액세스를 제공하는 것 외에도 시그니처 업데이트 등을 위해 HTTP 프록시 서버 또는 DNS 서버와 인터넷에 액세스해야 합니다. 이 섹션에서는 권장 네트워크 컨피그레이션에 대해 설명합니다. 네트워크는 환경에 따라 다를 수 있습니다.

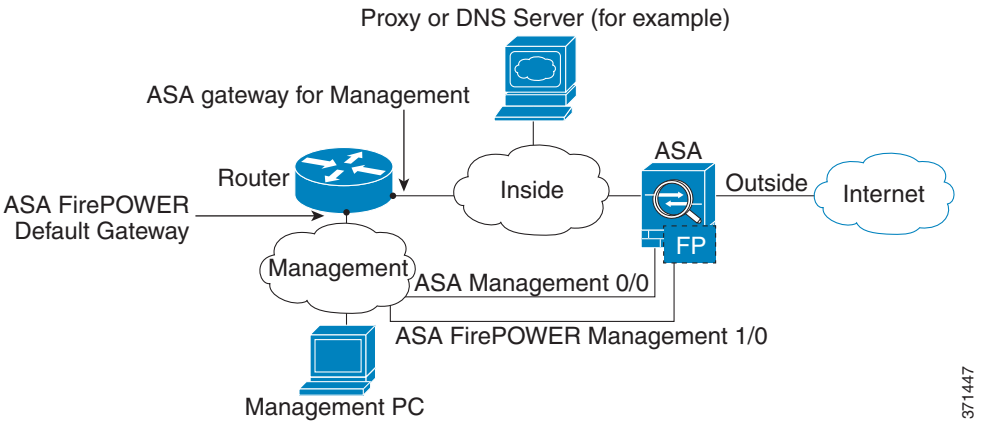
ASA 5585-X(하드웨어 모듈)

ASA FirePOWER 모듈에는 ASA에서 오는 별도의 관리 및 콘솔 인터페이스가 포함되어 있습니다. 초기 설정 시 기본 IP 주소를 사용하여 SSH로 ASA FirePOWER Management 1/0 인터페이스에 연결할 수 있습니다. 기본 IP 주소를 사용할 수 없는 경우, SSH를 사용하기 위해 콘솔 포트 또는 ASDM을 사용하여 관리 IP 주소를 변경할 수 있습니다. (17-14 페이지의 ASA FirePOWER 관리 IP 주소 변경 참조.)



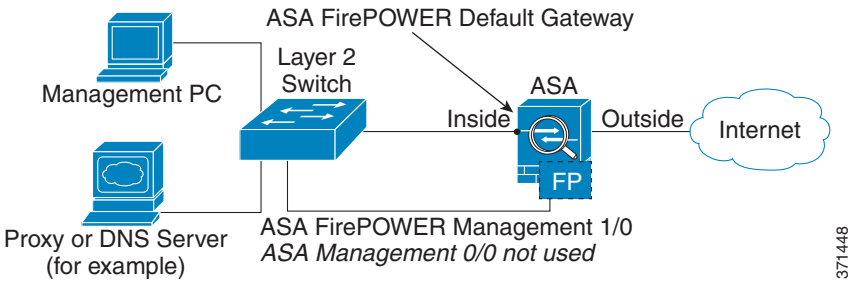
내부 라우터가 있는 경우

내부 라우터가 있으면 관리 네트워크(ASA Management 0/0 및 ASA FirePOWER Management 1/0 인터페이스를 모두 포함할 수 있음)와 인터넷 액세스용 ASA 내부 네트워크 간에 라우팅할 수 있습니다. 또한 내부 라우터를 통해 관리 네트워크에 도달하려면 ASA에서 경로를 추가해야 합니다.



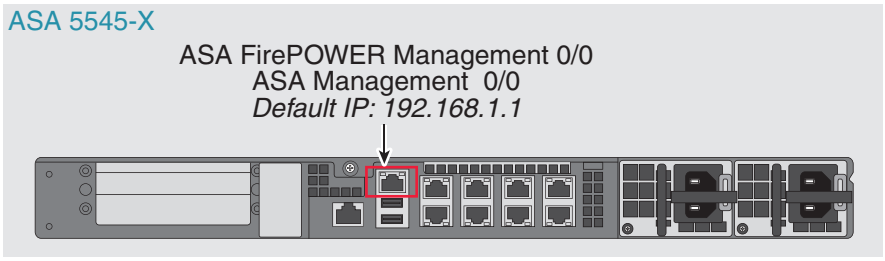
내부 라우터가 없는 경우

하나의 내부 네트워크만 있는 경우 별도의 관리 네트워크를 둘 수 없습니다. 네트워크 간 라우팅을 위해 내부 라우터가 필요하기 때문입니다.이 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. ASA FirePOWER 모듈은 ASA와 분리된 디바이스이므로 내부 인터페이스와 동일한 네트워크에 오도록 ASA FirePOWER Management 1/0 주소를 구성할 수 있습니다.



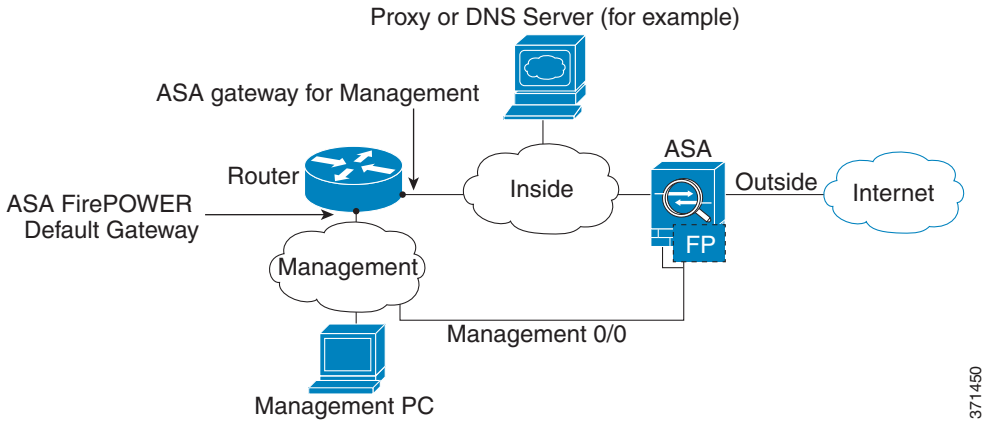
ASA 5512-X~ASA 5555-X(소프트웨어 모듈)

이러한 모듈은 ASA FirePOWER 모듈을 소프트웨어 모듈로서 실행하며, ASA FirePOWER 관리 인터페이스는 Management 0/0 인터페이스를 ASA와 공유합니다.초기 설정 시 SSH로 ASA FirePOWER 기본 IP 주소에 연결할 수 있습니다. 기본 IP 주소를 사용할 수 없는 경우, SSH를 사용할 수 있도록 ASDM을 사용하여 관리 IP 주소를 변경하거나 백플레인을 통해 ASA FirePOWER에 대한 세션을 시작할 수 있습니다.



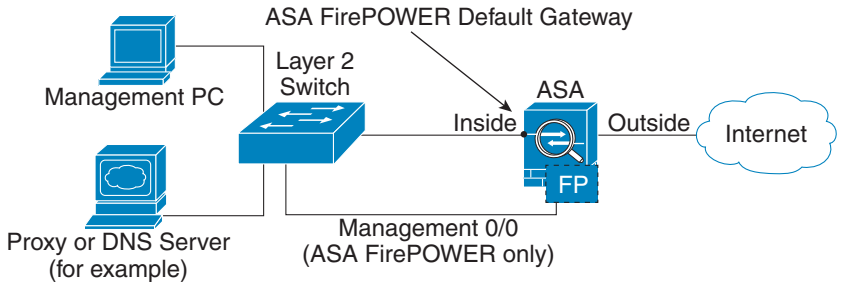
내부 라우터가 있는 경우

내부 라우터가 있으면 Management 0/0 네트워크(ASA 및 ASA FirePOWER 관리 IP 주소를 모두 포함)와 인터넷 액세스용 내부 네트워크 간에 라우팅할 수 있습니다.또한 내부 라우터를 통해 관리 네트워크에 도달하려면 ASA에서 경로를 추가해야 합니다.



내부 라우터가 없는 경우

하나의 내부 네트워크만 있는 경우 별도의 관리 네트워크를 둘 수 없습니다. 이 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. ASA에서 구성한 이름을 Management 0/0 인터페이스에서 제거하더라도 해당 인터페이스에 대해 ASA FirePOWER IP 주소를 구성할 수 있습니다. ASA FirePOWER 모듈은 기본적으로 ASA와 분리된 디바이스이므로 내부 인터페이스와 동일한 네트워크에 오도록 ASA FirePOWER 관리 주소를 구성할 수 *있습니다.*



참고 ASA에서 구성한 이름을 Management 0/0에서 제거해야 합니다. ASA에서 구성한 경우 ASA FirePOWER 주소는 ASA와 동일한 네트워크에 있어야 합니다. 그러면 기타 ASA 인터페이스에서 이미 구성된 모든 네트워크가 제외됩니다. 이름이 구성되지 않은 경우 ASA FirePOWER 주소는 어떤 네트워크에든 둘 수 있습니다(예: ASA 내부 네트워크).

(ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 설치 또는 재이미지화

ASA FirePOWER 모듈과 함께 ASA를 구매하면 모듈 소프트웨어 및 필수 SSD(Solid State Drive)가 사전 설치되어 바로 구성할 수 있는 상태가 됩니다. ASA FirePOWER 소프트웨어 모듈을 기존 ASA에 추가하거나 SSD를 교체해야 할 경우 ASA FirePOWER 부트 소프트웨어를 설치하고 다음 절차에 따라 SSD의 파티션을 만들어야 합니다.

모듈 재이미지화 절차도 동일합니다. 단, ASA FirePOWER 모듈을 먼저 제거해야 합니다. SSD를 교체하는 경우 시스템을 재이미지화하게 됩니다.

SSD를 물리적으로 설치하려는 방법은 ASA 하드웨어 가이드를 참조하십시오.

시작하기 전에

- 플래시의 빈 공간(disk0)은 최소 3GB + 부트 소프트웨어 크기가 되어야 합니다.
- 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.
- 실행 중인 다른 소프트웨어 모듈은 종료해야 합니다. 디바이스는 한 번에 하나의 소프트웨어 모듈을 실행할 수 있습니다. ASA CLI에서 수행해야 합니다. 예를 들어, 다음 명령은 IPS 소프트웨어 모듈을 종료 및 제거한 후 ASA를 다시 로드합니다. **ips** 대신 **cxsc** 키워드를 사용하는 것을 제외하면 CX 모듈을 제거하기 위한 명령도 동일합니다.

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

참고 트래픽을 IPS 또는 CX 모듈로 리디렉션하는 활성 서비스 정책이 있는 경우 해당 정책을 제거해야 합니다. 글로벌 정책이면 **no service-policy** *ips_policy* **global**을 사용하면 됩니다. CLI 또는 ASDM을 사용하여 정책을 제거할 수 있습니다.

- 모듈을 재이미지화할 때 동일한 종료 및 제거 명령을 사용하여 이전 이미지를 제거합니다. 예: **sw-module module sfr uninstall**.
- Cisco.com에서 ASA FirePOWER 부트 이미지 및 시스템 소프트웨어 패키지를 다운로드합니다.

절차

1단계 부트 이미지를 디바이스로 다운로드합니다. 시스템 소프트웨어를 전송하지 마십시오. 나중에 SSD로 다운로드됩니다. 다음 옵션을 이용할 수 있습니다.

- ASDM - 먼저 부트 이미지를 워크스테이션으로 다운로드하거나 FTP, TFTP, HTTP, HTTPS, SMB 또는 SCP 서버에 둡니다. ASDM에서 **Tools > File Management**를 선택한 다음 적절한 **File Transfer** 명령, **Between Local PC and Flash** 또는 **Between Remote Server and Flash**를 선택합니다. 부트 소프트웨어를 ASA의 disk0으로 전송합니다.
- ASA CLI - 먼저 부트 이미지를 TFTP, FTP, HTTP 또는 HTTPS 서버에 둔 다음 **copy** 명령을 사용하여 플래시로 다운로드합니다. 다음 예에서는 TFTP를 사용합니다. <TFTP Server>를 각자의 서버 IP 주소 또는 호스트 이름으로 교체하십시오.

```
ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
disk0:/asasfr-5500x-boot-5.3.1-58.img
```

2단계 Cisco.com의 ASA FirePOWER 시스템 소프트웨어를 ASA FirePOWER 관리 인터페이스에서 액세스할 수 있는 HTTP, HTTPS 또는 FTP 서버로 다운로드합니다.

3단계 다음 명령을 입력하여 ASA FirePOWER 모듈 부트 이미지 위치를 ASA disk0으로 설정합니다.

```
hostname# sw-module module sfr recover configure image disk0:file_path
```

참고 "ERROR: Another service (cxsc) is running, only one service is allowed to run at any time"과 같은 메시지가 표시되면 이미 다른 소프트웨어 모듈이 구성되어 있다는 의미입니다. 위의 전제 조건 섹션에서 설명한 대로 새 모듈을 설치하려면 기존 모듈을 종료하고 제거해야 합니다.

예:

```
hostname# sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

4단계 다음 명령을 입력하여 ASA FirePOWER 부트 이미지를 로드합니다.

```
hostname# sw-module module sfr recover boot
```

5단계 ASA FirePOWER 모듈이 부팅할 때까지 약 5분에서 15분 정도 기다린 후 현재 실행 중인 ASA FirePOWER 부트 이미지에 대한 콘솔 세션을 시작합니다. 로그인 프롬프트로 이동하려면 세션을 연 후 Enter 키를 눌러야 할 수 있습니다. 기본 사용자 이름은 **admin**이고 기본 비밀번호는 **Admin123**입니다.

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

팁 모듈 부팅이 완료되면, ttyS1을 통해 연결할 수 없다는 메시지와 함께 **session** 명령이 실패합니다. 기다렸다가 다시 시도하십시오.

6단계 시스템 소프트웨어 패키지를 설치할 수 있도록 시스템을 구성하려면 **setup** 명령을 사용합니다.

```
asasfr-boot> setup

               Welcome to SFR Setup
                [hit Ctrl-C to abort]
            Default values are inside []
```

다음에 대한 프롬프트가 표시됩니다. 관리 주소, 게이트웨이 및 DNS 정보는 구성을 위한 핵심 설정입니다.

- 호스트 이름 - 공백 없이 영숫자 최대 65자를 사용합니다. 하이픈은 허용됩니다.
- 네트워크 주소 - 고정 IPv4 또는 IPv6 주소를 사용하거나, DHCP(IPv4용) 또는 IPv6 무상태(stateless) 자동 컨피그레이션을 설정할 수 있습니다.
- DNS 정보 - 하나 이상의 DNS 서버를 지정해야 합니다. 도메인 이름 및 검색 도메인도 설정할 수 있습니다.
- NTP 정보 - NTP를 활성화하고, 시스템 시간 설정을 위해 NTP 서버를 구성할 수 있습니다.

7단계 **system install** 명령을 사용하여 시스템 소프트웨어 이미지를 설치합니다.

system install [**noconfirm**] *url*

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다. HTTP, HTTPS 또는 FTP URL을 사용합니다. 사용자 이름과 비밀번호가 필요한 경우 입력하라는 메시지가 표시됩니다.

설치가 완료되면 시스템이 다시 부팅됩니다. 애플리케이션 구성 요소가 설치되고 ASA FirePOWER 서비스가 시작될 때까지 10분 이상 기다립니다. (**show module sfr**이 출력되면 모든 프로세스가 완료된 것입니다.)

예:

```
asasfr-boot> system install http://asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.3.1-44 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

8단계 ASA FirePOWER 모듈에 대한 세션을 엽니다. 완전한 기능을 하는 모듈에 로그인하기 때문에 다른 로그인 프롬프트가 표시될 것입니다.

```
asa3# session sfr
Opening command session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:
```

9단계 사용자 이름 **admin** 및 비밀번호 **Sourcefire**로 로그인합니다.

10단계 표시되는 화면 컨피그레이션을 완료합니다.

먼저 EULA(최종 사용자 라이센스 계약)를 읽고 내용에 동의해야 합니다. 그런 다음 표시되는 프롬프트에 따라 admin 비밀번호를 변경하고, 관리 주소 및 DNS 설정을 변경합니다. IPv4 및 IPv6 관리 주소를 모두 구성할 수 있습니다. 예:

```
System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)
```

```
This sensor must be managed by a Defense Center.  A unique alphanumeric
registration key is always required.  In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

11단계 **configure manager add** 명령을 사용하여, 이 디바이스를 관리할 FireSIGHT Management Center 어플라이언스를 지정합니다.

등록 키(registration key)를 제공해야 하는데, 이 키는 디바이스를 인벤토리에 추가할 때 FireSIGHT Management Center에서 사용하게 됩니다. 다음 예는 간단한 사례를 보여줍니다. NAT 경계가 있으면 명령이 달라집니다. 17-16 페이지의 FireSIGHT Management Center에 ASA FirePOWER 추가를 참조하십시오.

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

12단계 브라우저에서 HTTPS를 사용하고, 위에서 입력한 호스트 이름 또는 주소를 사용하여 FireSIGHT Management Center에 로그인합니다. 예: https://DC.example.com.

디바이스를 추가하려면 Device Management(**Devices > Device Management**) 페이지를 사용합니다. 자세한 내용은 온라인 도움말 또는 *FireSIGHT System User Guide*의 Managing Devices 장을 참조하십시오.

팁 또한 FireSIGHT Management Center를 통해 NTP 및 시간 설정을 구성할 수 있습니다. 로컬 정책을 편집할 경우 **System > Local > System Policy** 페이지에서 Time Synchronization 설정을 사용하십시오.

ASA FirePOWER 관리 IP 주소 변경

기본 관리 IP 주소를 사용할 수 없는 경우 ASA에서 관리 IP 주소를 설정할 수 있습니다. 관리 IP 주소를 설정하면 SSH를 사용하여 ASA FirePOWER 모듈에 액세스하고 추가 설정을 수행할 수 있습니다.

초시 시스템 설정 중에 17-15 페이지의 ASA FirePOWER CLI에서 기본 ASA FirePOWER 설정 구성에서 설명한 대로 ASA FirePOWER CLI를 사용하여 관리 주소를 이미 구성한 경우 ASA CLI 또는 ASDM을 통해 구성할 필요가 없습니다.

참고 소프트웨어 모듈의 경우 ASA FirePOWER CLI에서 세션을 시작하고 ASA CLI에 액세스하여 설정을 수행할 수 있습니다. 그런 다음 설정 과정에서 ASA FirePOWER 관리 IP 주소를 설정할 수 있습니다. 하드웨어 모듈의 경우 콘솔 포트를 통해 초기 설정을 완료할 수 있습니다.

ASA를 통해 관리 IP 주소를 변경하려면 다음 중 하나를 수행하십시오. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

- CLI에서 다음 명령을 사용하여 ASA FirePOWER 관리 IP 주소, 마스크 및 게이트웨이를 설정합니다. 하드웨어 모듈에는 **1**, 소프트웨어 모듈에는 **sfr**을 지정합니다.

  session {1 | sfr} do setup host ip *ip_address*/*mask*,*gateway_ip*

  예: **session 1 do setup host ip 10.1.1.2/24,10.1.1.1**.

- ASDM에서 **Wizards > Startup Wizard**를 선택하고 마법사의 과정에 따라 ASA FirePOWER Basic Configuration으로 이동합니다. 여기서 IP 주소, 마스크 및 기본 게이트웨이를 설정할 수 있습니다.

ASA FirePOWER CLI에서 기본 ASA FirePOWER 설정 구성

보안 정책을 구성하려면 우선 ASA FirePOWER 모듈에서 기본 네트워크 설정 및 기타 매개변수를 구성해야 합니다. 이 절차에서는 완전한 시스템 소프트웨어(부트 이미지만이 아니라)를 설치했다고 가정합니다(직접 설치했거나 하드웨어 모듈에 이미 설치된 것으로 가정).

팁 또한 사용자가 초기 컨피그레이션을 수행하는 것으로 가정합니다. 초기 컨피그레이션 중에 이러한 설정에 대한 프롬프트가 표시됩니다. 나중에 이러한 설정을 변경하려면 **configure network** 명령을 사용하여 개별 설정을 변경할 수 있습니다. **configure network** 명령에 대해 자세히 알아보려면 **?** 명령을 입력하여 도움말을 보거나, *FireSIGHT System User Guide* 또는 FireSIGHT Management Center의 온라인 도움말을 참조하십시오.

절차

1단계 다음 중 하나를 수행합니다.

- (모든 모델) SSH를 사용하여 ASA FirePOWER 관리 IP 주소에 연결합니다.
- (ASA 5512-X~ASA 5555-X) ASA CLI에서 모듈에 대한 세션을 엽니다(ASA CLI에 액세스하는 방법은 일반 운영 컨피그레이션 가이드의 "Getting Started" 장 참조). 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 세션을 시작합니다.

  ```
  hostname# session sfr
  ```

2단계 사용자 이름 **admin** 및 비밀번호 **Sourcefire**로 로그인합니다.

3단계 표시되는 화면 컨피그레이션을 완료합니다.

먼저 EULA(최종 사용자 라이센스 계약)를 읽고 내용에 동의해야 합니다. 그런 다음 표시되는 프롬프트에 따라 admin 비밀번호를 변경하고, 관리 주소 및 DNS 설정을 변경합니다. IPv4 및 IPv6 관리 주소를 모두 구성할 수 있습니다. 센서를 FireSIGHT Management Center에서 관리해야 한다는 내용의 메시지가 표시되면 컨피그레이션이 완료된 것입니다.

예:

```
System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
```

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center.  A unique alphanumeric
registration key is always required.  In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

4단계 이제 17-16 페이지의 FireSIGHT Management Center에 ASA FirePOWER 추가에서 설명한 대로 이 디바이스를 관리할 FireSIGHT Management Center를 지정해야 합니다.

FireSIGHT Management Center에 ASA FirePOWER 추가

모듈에서 정책을 구성하기 위해 사용할 애플리케이션인 FireSIGHT Management Center에 ASA FirePOWER 모듈을 등록해야 합니다. FireSIGHT Management Center를 Defense Center라고도 합니다.

디바이스를 등록하려면 **configure manager add** 명령을 사용합니다. 디바이스를 FireSIGHT Management Center에 등록하려면 고유한 영숫자 등록 키가 항상 필요합니다. 등록 키는 사용자가 지정할 수 있는 간단한 키이며, 라이센스 키와는 다릅니다.

대부분의 경우 등록 키와 함께 FireSIGHT Management Center의 호스트 이름 또는 IP 주소를 제공해야 합니다. 예를 들면 다음과 같습니다.

```
configure manager add DC.example.com my_reg_key
```

그러나 디바이스와 FireSIGHT Management Center가 NAT 디바이스에 의해 분리된 경우, 등록 키와 함께 고유한 NAT ID를 입력하고 호스트 이름 대신 DONTRESOLVE를 지정합니다. 예를 들면 다음과 같습니다.

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

절차

1단계 다음 중 하나를 수행합니다.

- (모든 모델) SSH를 사용하여 ASA FirePOWER 관리 IP 주소에 연결합니다.
- (ASA 5512-X~ASA 5555-X) ASA CLI에서 모듈에 대한 세션을 엽니다(ASA CLI에 액세스하는 방법은 일반 운영 컨피그레이션 가이드의 "Getting Started" 장 참조). 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 세션을 시작합니다.

```
hostname# session sfr
```

2단계 사용자 이름 **admin** 또는 CLI 컨피그레이션(Administrator) 액세스 레벨이 있는 다른 사용자 이름으로 로그인합니다.

3단계 프롬프트에서 **configure manager add** 명령을 사용하여(다음 구문 참조) 디바이스를 FireSIGHT Management Center에 등록합니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} - FireSIGHT Management Center의 정규화된 호스트 이름 또는 IP 주소를 지정합니다. FireSIGHT Management Center의 주소를 직접 지정할 수 없으면 DONTRESOLVE를 사용합니다.
- *reg_key* - 디바이스를 FireSIGHT Management Center에 등록하기 위해 필요한 고유한 영숫자 등록 키입니다.
- *nat_id* - FireSIGHT Management Center와 디바이스 간 등록 프로세스 중에 사용되는 선택적인 영숫자 문자열입니다. 호스트 이름을 DONTRESOLVE로 설정하는 경우 반드시 필요합니다.

4단계 브라우저에서 HTTPS를 사용하고, 위에서 입력한 호스트 이름 또는 주소를 사용하여 FireSIGHT Management Center에 로그인합니다. 예: https://DC.example.com.

디바이스를 추가하려면 Device Management(**Devices > Device Management**) 페이지를 사용합니다. 자세한 내용은 온라인 도움말 또는 *FireSIGHT System User Guide*의 Managing Devices 장을 참조하십시오.

ASA FirePOWER 모듈에서 보안 정책 구성

ASA FirePOWER 모듈에서 보안 정책을 구성하려면 FireSIGHT Management Center를 사용합니다. 보안 정책은 모듈에서 제공하는 Next Generation IPS 필터링 및 애플리케이션 필터링 등의 서비스를 제어합니다. ASA FirePOWER CLI, ASA CLI 또는 ASDM에서는 정책을 구성할 수 없습니다.

FireSIGHT Management Center를 열려면 웹 브라우저를 사용하여 다음 URL을 엽니다.

https://*DC_address*

여기서 *DC_address*는 17-16 페이지의 FireSIGHT Management Center에 ASA FirePOWER 추가에서 정의한 관리자의 DNS 이름 또는 IP 주소입니다. 예: https://dc.example.com.

보안 정책 구성 방법에 대한 자세한 내용은 *FireSIGHT System User Guide* 또는 FireSIGHT Management Center의 온라인 도움말을 참조하십시오.

팁 ASDM의 ASA FirePOWER Status 대시보드에서 FireSIGHT Management Center를 열 수도 있습니다. **Home > ASA FirePOWER Status**를 선택하고 대시보드의 아래쪽에서 링크를 클릭합니다.

ASA FirePOWER 모듈로 트래픽 리디렉션

특정 트래픽을 식별하는 서비스 정책을 만들어 ASA FirePOWER 모듈로 트래픽을 리디렉션할 수 있습니다.

패시브("모니터 전용") 또는 인라인 배포에서 디바이스를 구성할 수 있습니다.

- 패시브 배포에서는 트래픽의 복사본이 디바이스로 전송되지만 ASA로 반환되지는 않습니다. 패시브 모드에서는 네트워크에 영향을 미치지 않은 채, 디바이스가 트래픽에 대해 무엇을 수행했는지를 알 수 있으며, 트래픽의 내용을 평가할 수 있습니다.
- 인라인 배포 시에는 실제 트래픽이 디바이스로 전송되며, 디바이스의 정책이 트래픽에 영향을 미칩니다. 원하지 않는 트래픽을 취소하고 정책에 의해 적용되는 다른 작업을 수행한 후 추가 처리 및 최종 전송을 위해 트래픽을 ASA로 반환합니다.

참고 ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수 없습니다. 보안 정책 유형은 하나만 허용됩니다. 다중 컨텍스트 모드에서는 일부 컨텍스트에 대해 모니터 전용 모드를 구성할 수 없고, 다른 컨텍스트에 대해 일반 인라인 모드를 구성할 수 없습니다.

시작하기 전에

- 트래픽을 IPS 또는 CX 모듈(ASA FirePOWER와 교체한 모듈)로 리디렉션하는 활성 서비스 정책이 있는 경우 이 정책을 먼저 제거한 후 ASA FirePOWER 서비스 정책을 구성해야 합니다.
- ASA 및 ASA FirePOWER에서 일관된 정책을 구성해야 합니다(FireSIGHT Management Center를 통해). 두 정책 모두 트래픽의 패시브 모드 또는 인라인 모드를 반영해야 합니다.
- 다중 컨텍스트 모드의 경우 각 보안 컨텍스트 내부에서 이 절차를 수행합니다.

절차

1단계 모듈로 전송할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map firepower_class_map
hostname(config-cmap)# match access-list firepower
```

다중 트래픽 클래스를 모듈로 전송하려면 보안 정책에서 사용할 다중 클래스 맵을 만들 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 이 절차의 시작 부분에 만든 클래스 맵을 확인합니다.

```
class name
```

예:

```
hostname(config-pmap)# class firepower_class_map
```

4단계 트래픽을 ASA FirePOWER 모듈로 전송합니다.

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

여기서 각 항목은 다음을 나타냅니다.

- **fail-close** 키워드는 ASA FirePOWER 모듈을 사용할 수 없는 경우 모든 트래픽을 차단하도록 ASA를 설정합니다.
- **fail-open** 키워드는 모듈을 사용할 수 없는 경우 검사 없이 모든 트래픽을 허용하도록 ASA를 설정합니다.
- 트래픽의 읽기 전용 복사본을 모듈로 전송하려면(즉, 패시브 모드) **monitor-only**를 지정합니다. 이 키워드를 포함하지 않으면 트래픽은 인라인 모드에서 전송됩니다. 자세한 내용은 17-3 페이지의 ASA FirePOWER 패시브(모니터 전용) 모드 섹션을 참조하십시오.

예:

```
hostname(config-pmap-c)# sfr fail-close
```

5단계 ASA FirePOWER 트래픽용 다중 클래스 맵을 만든 경우 정책에 대한 또 다른 클래스를 지정하고 **sfr** 리디렉션 작업을 적용할 수 있습니다.

클래스의 순서가 정책 맵에서 어떤 의미를 갖는지를 자세히 알아보려면 1-5 페이지의 서비스 정책 내에서의 기능 일치를 참조하십시오. 트래픽은 동일한 작업 유형에 대해 둘 이상의 클래스 맵과 일치할 수 없습니다.

6단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

ASA FirePOWER 모듈 관리

이 섹션에는 모듈 관리에 도움이 되는 절차가 포함되어 있습니다.

비밀번호 재설정

admin 사용자의 비밀번호를 잊어버린 경우 CLI 컨피그레이션 권한이 있는 다른 사용자 이름으로 로그인하여 비밀번호를 변경할 수 있습니다.

필요한 권한을 보유한 다른 사용자가 없는 경우 **session do** 명령을 사용하여 ASA에서 admin 비밀번호를 재설정할 수 있습니다.

팁 ASA hw-module 및 sw-module 명령의 password-reset 옵션은 ASA FirePOWER에서 작동하지 않습니다.

사용자 **admin**의 모듈 비밀번호를 기본값인 **Sourcefire**로 재설정하려면 다음 명령을 사용합니다. 하드웨어 모듈에는 **1**, 소프트웨어 모듈에는 **sfr**을 지정합니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

```
session {1 | sfr} do password-reset
```

예: **session sfr do password-reset**.

모듈 다시 로드 또는 재설정

모듈을 다시 로드하거나 재설정 후 다시 로드하려면 ASA CLI에서 다음 명령 중 하나를 입력합니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

- 하드웨어 모듈(ASA 5585-X):

  ```
  hw-module module 1 {reload | reset}
  ```

- 소프트웨어 모듈(ASA 5512-X~ASA 5555-X):

  ```
  sw-module module sfr {reload | reset}
  ```

모듈 종료

모듈 소프트웨어를 종료하면 컨피그레이션 데이터를 잃지 않은 채 모듈의 전원을 안전하게 끌 수 있습니다. 모듈을 정상적으로 종료하려면 ASA CLI에서 다음 명령 중 하나를 입력합니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

참고 ASA를 다시 로드하면 모듈이 자동으로 종료되지 않습니다. 따라서 ASA를 다시 로드하기 전에 모듈을 종료하는 것이 좋습니다.

- 하드웨어 모듈(ASA 5585-X):

  ```
  hw-module module 1 shutdown
  ```

- 소프트웨어 모듈(ASA 5512-X~ASA 5555-X):

  ```
  sw-module module sfr shutdown
  ```

(ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 이미지 제거

소프트웨어 모듈 이미지 및 관련 컨피그레이션을 제거할 수 있습니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

절차

1단계 소프트웨어 모듈 이미지 및 관련 컨피그레이션을 제거합니다.

```
hostname# sw-module module sfr uninstall

Module sfr will be uninstalled. This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module sfr? [confirm]
```

2단계 ASA를 다시 로드합니다. 새 모듈을 설치하려면 먼저 ASA를 다시 로드해야 합니다.

```
hostname# reload
```

(ASA 5512-X~ASA 5555-X) ASA에서 모듈에 대한 세션 시작

기본 네트워크 설정을 구성하고 모듈 관련 문제를 해결하려면 ASA FirePOWER CLI를 사용하십시오.

ASA에서 ASA FirePOWER 소프트웨어 모듈 CLI에 액세스하려면 ASA에서 세션을 시작할 수 있습니다. 모듈에 대한 세션을 시작하거나(텔넷 사용) 가상 콘솔 세션을 만들 수 있습니다. 제어 평면이 다운되어 텔넷 세션을 설정할 수 없는 경우 콘솔 세션이 유용할 수 있습니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 세션을 시작합니다.

텔넷 또는 콘솔 세션에서 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시됩니다. ASA FirePOWER에 구성된 어떤 사용자 이름으로도 로그인할 수 있습니다. 초기에 유일하게 구성된 사용자 이름은 **admin**입니다(항상 사용 가능). 초기 기본 사용자 이름은 전체 이미지의 경우 **Sourcefire,** 부트 이미지의 경우 **Admin123**입니다.

- 텔넷 세션:

  ```
  session sfr
  ```

  ASA FirePOWER CLI에 있을 때 종료 후 ASA CLI로 돌아가려면 모듈에서 로그아웃하기 위한 명령(**logout** 또는 **exit**)을 입력하고 **Ctrl-Shift-6, x**를 누릅니다.

- 콘솔 세션:

  ```
  session sfr console
  ```

  콘솔 세션을 종료하는 유일한 방법은 **Ctrl-Shift-6, x**를 누르는 것입니다. 모듈에서 로그아웃하면 모듈 로그인 프롬프트가 표시됩니다.

참고 터미널 서버에서는 **session sfr console** 명령을 사용하지 마십시오. 여기서 **Ctrl-Shift-6, x**는 터미널 서버 프롬프트로 돌아가기 위한 이스케이프 시퀀스입니다. **Ctrl-Shift-6, x**는 ASA FirePOWER 콘솔을 이스케이프하고 ASA 프롬프트로 돌아가기 위한 시퀀스이기도 합니다. 그러므로 이 상황에서 ASA FirePOWER 콘솔을 종료하려고 시도하면 대신 종료 후 터미널 서버 프롬프트에 이르게 됩니다. 터미널 서버를 ASA에 다시 연결하면 ASA FirePOWER 콘솔 세션은 여전히 활성 상태이므로, 종료 후 ASA 프롬프트로 돌아갈 수 없습니다. 콘솔을 ASA 프롬프트로 되돌리려면 직접 직렬 연결을 사용해야 합니다. 이러한 상황에서는 콘솔 명령 대신 **session sfr** 명령을 사용하십시오.

5585-X ASA FirePOWER 하드웨어 모듈 재이미지화

ASA 5585-X 어플라이언스에서 어떤 이유로든 ASA FirePOWER 하드웨어 모듈을 재이미지화해야 하는 경우 부트 이미지 및 시스템 소프트웨어 패키지를 순서대로 설치해야 합니다. 시스템이 작동하려면 두 패키지를 모두 설치해야 합니다. 정상적인 상황에서는 업그레이드 패키지를 설치하기 위해 시스템을 재이미지화할 필요가 없습니다.

부트 이미지를 설치하려면 모듈의 콘솔 포트에 로그인하여 ASA FirePOWER SSP의 Management-0 포트에서 이미지의 TFTP 부트를 수행해야 합니다. Management-0 포트는 첫 번째 슬롯의 SSP에 있으므로 Management1/0이라고도 하지만 rommon에서는 이를 Management-0 또는 Management0/1로 인식됩니다.

TFTP 부트를 수행하려면 다음과 같이 해야 합니다.

- 소프트웨어 이미지를 ASA FirePOWER에서 Management1/0 인터페이스를 통해 액세스할 수 있는 TFTP 서버에 둡니다.
- Management1/0을 네트워크에 연결합니다. 부트 이미지에 대해 TFTP 부트를 수행하려면 이 인터페이스를 사용해야 합니다.
- rommon 변수를 구성합니다. Esc 키를 눌러 rommon 변수를 구성할 수 있도록 자동 부팅을 중단합니다.

부트 이미지를 설치한 후 시스템 소프트웨어 패키지를 설치합니다. ASA FirePOWER에서 액세스할 수 있는 HTTP, HTTPS 또는 FTP 서버에 패키지를 두어야 합니다.

다음 절차에서는 부트 이미지를 설치한 다음 시스템 소프트웨어 패키지를 설치하는 방법에 대해 설명합니다.

절차

1단계 콘솔 포트에 연결합니다. ASA 제품에 포함된 콘솔 케이블을 사용하여 PC를 콘솔에 연결합니다(터미널 에뮬레이터 9600보드, 8 데이터 비트, 패리티 없음, 1 정지 비트, 흐름 제어 없음). 콘솔 케이블에 대한 자세한 내용은 ASA에 대한 하드웨어 가이드를 참조하십시오.

2단계 시스템을 다시 로드하려면 **system reboot** 명령을 입력합니다.

3단계 프롬프트가 표시되면 Esc 키를 눌러 부트에서 빠져나옵니다. 시스템 부팅을 위한 grub start가 표시되면 너무 오래 기다린 것입니다.

이 경우 rommon 프롬프트로 이동하게 됩니다.

4단계 rommon 프롬프트에서 **set**을 입력하고 다음 매개변수를 구성합니다.

- ADDRESS - 모듈의 관리 IP 주소입니다.
- SERVER - TFTP 서버의 IP 주소입니다.
- GATEWAY - TFTP 서버의 게이트웨이 주소입니다. TFTP 서버가 Management1/0에 직접 연결되어 있으면 TFTP 서버의 IP 주소를 사용하십시오. TFTP 서버 및 관리 주소가 동일한 서브넷에 있으면 게이트웨이를 구성하지 마십시오. 그렇지 않으면 TFTP 부트가 실패합니다.
- IMAGE - TFTP 서버의 부트 이미지 경로 및 이미지 이름입니다. 예를 들어 TFTP 서버에서 파일 위치가 /tftpboot/images/filename.img인 경우 IMAGE 값은 images/filename.img입니다.

예:

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
GATEWAY=10.5.1.1
IMAGE=asasfr-boot-5.3.1-26-54.img
```

5단계 **sync**를 입력하여 설정을 저장합니다.

6단계 **tftp**를 입력하여 다운로드 및 부팅을 시작합니다.

진행 상태를 나타내는 ! 표시가 나타납니다. 몇 분 후 부팅이 완료되면 로그인 프롬프트가 표시됩니다.

7단계 비밀번호 **Admin123**을 사용하여 **admin**으로 로그인합니다.

8단계 시스템 소프트웨어 패키지를 설치할 수 있도록 시스템을 구성하려면 **setup** 명령을 사용합니다.

다음에 대한 프롬프트가 표시됩니다. 관리 주소, 게이트웨이 및 DNS 정보는 구성을 위한 핵심 설정입니다.

- 호스트 이름 - 공백 없이 영숫자 최대 65자를 사용합니다. 하이픈은 허용됩니다.
- 네트워크 주소 - 고정 IPv4 또는 IPv6 주소를 사용하거나, DHCP(IPv4용) 또는 IPv6 무상태(stateless) 자동 컨피그레이션을 설정할 수 있습니다.
- DNS 정보 - 하나 이상의 DNS 서버를 지정해야 합니다. 도메인 이름 및 검색 도메인도 설정할 수 있습니다.
- NTP 정보 - NTP를 활성화하고, 시스템 시간 설정을 위해 NTP 서버를 구성할 수 있습니다.

9단계 **system install** 명령을 사용하여 시스템 소프트웨어 이미지를 설치합니다.

system install [**noconfirm**] *url*

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다.

설치가 완료되면 시스템이 다시 부팅됩니다. 애플리케이션 구성 요소가 설치되고 ASA FirePOWER 서비스가 시작될 때까지 10분 이상 기다립니다.

예:

```
asasfr-boot> system install http://asasfr-sys-5.3.1-54.pkg
```

10단계 부팅이 완료되면 사용자 이름 **admin** 및 비밀번호 **Sourcefire**로 로그인합니다.

표시되는 화면 컨피그레이션을 완료합니다.

먼저 EULA(최종 사용자 라이센스 계약)를 읽고 내용에 동의해야 합니다. 그런 다음 표시되는 프롬프트에 따라 admin 비밀번호를 변경하고, 관리 주소 및 DNS 설정을 변경합니다. IPv4 및 IPv6 관리 주소를 모두 구성할 수 있습니다.

11단계 **configure manager add** 명령을 사용하여, 이 디바이스를 관리할 FireSIGHT Management Center 어플라이언스를 지정합니다.

등록 키(registration key)를 제공해야 하는데, 이 키는 디바이스를 인벤토리에 추가할 때 FireSIGHT Management Center에서 사용하게 됩니다. 다음 예는 간단한 사례를 보여줍니다. NAT 경계가 있으면 명령이 달라집니다. 17-16 페이지의 FireSIGHT Management Center에 ASA FirePOWER 추가를 참조하십시오.

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

12단계 브라우저에서 HTTPS를 사용하고, 위에서 입력한 호스트 이름 또는 주소를 사용하여 FireSIGHT Management Center에 로그인합니다. 예: https://DC.example.com.

디바이스를 추가하려면 Device Management(**Devices > Device Management**) 페이지를 사용합니다. 자세한 내용은 *FireSIGHT System User Guide*의 Managing Devices 장 또는 FireSIGHT Management Center의 온라인 도움말을 참조하십시오.

시스템 소프트웨어 업그레이드

FireSIGHT Management Center를 사용하여 ASA FirePOWER 모듈에 업그레이드 이미지를 적용합니다. 업그레이드를 적용하기 전에 ASA에서 새 버전의 최소 필수 릴리스를 실행하고 있는지 확인합니다. 모듈을 업그레이드하기 전에 ASA를 업그레이드해야 할 수 있습니다.

업그레이드 적용에 대한 자세한 내용은 *FireSIGHT System User Guide* 또는 FireSIGHT Management Center의 온라인 도움말을 참조하십시오.

모듈 ASA FirePOWER 모니터링

다음 항목에서는 모듈 모니터링에 대한 지침을 제공합니다. ASA FirePOWER 관련 syslog 메시지에 대해서는 syslog 메시지 가이드를 참조하십시오. ASA FirePOWER syslog 메시지는 메시지 번호 434001부터 시작합니다.

- 17-24 페이지의 모듈 상태 표시
- 17-25 페이지의 모듈 통계 표시
- 17-26 페이지의 모듈 연결 모니터링

모듈 상태 표시

모듈 상태를 확인하려면 다음 명령 중 하나를 입력합니다.

- **show module** [**1** | **sfr**] [**details**]

  모듈 상태를 표시합니다. ASA FirePOWER 모듈과 관련된 상태를 보려면 1(하드웨어 모듈의 경우) 또는 sfr(소프트웨어 모듈의 경우) 키워드를 포함합니다. 모듈을 관리하는 디바이스의 주소를 비롯한 추가 정보를 보려면 details 키워드를 포함합니다.

- **show module sfr recover**

  모듈 설치 시 사용된 부트 이미지의 위치를 표시합니다.

다음은 ASA FirePOWER 하드웨어 모듈이 설치된 ASA 5585-X에서 **show module** 명령을 실행한 샘플 출력입니다.

```
hostname# show module
Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
   1 ASA 5585-X FirePOWER Security Services Proce ASA5585-SSP-SFR10  JAF1510BLSA

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.10(0)8
   1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     5.3.1-44

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
   1 FirePOWER                      Up               5.3.1-44

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Up                 Up
```

다음 예는 소프트웨어 모듈의 세부사항을 보여줍니다. DC Addr은 이 디바이스를 관리하는 FireSIGHT Management Center의 주소입니다.

```
hostname# show module sfr details
Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              ASA5555
Hardware version:   N/A
Serial Number:      FCH1714J6HP
Firmware version:   N/A
Software version:   5.3.1-100
MAC Address Range:  bc16.6520.1dcb to bc16.6520.1dcb
App. name:          ASA FirePOWER
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       5.3.1-100
Data Plane Status:  Up
Status:             Up
DC addr:            10.89.133.202
Mgmt IP addr:       10.86.118.7
Mgmt Network mask:  255.255.252.0
Mgmt Gateway:       10.86.116.1
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

다음 예는 모듈 설치 시 **sw-module module sfr recover** 명령과 함께 사용된 ASA FirePOWER 부트 이미지의 위치를 보여줍니다.

```
hostname# show module sfr recover
Module sfr recover parameters...
Boot Recovery Image: No
Image File Path:     disk0:/asasfr-5500x-boot-5.3.1-44.img
```

모듈 통계 표시

각 서비스 정책에 대한 통계와 상태를 표시하려면 **sfr** 명령이 포함된 show service-policy sfr 명령을 사용합니다. 카운터를 지우려면 **clear service-policy**를 사용합니다.

다음 예는 ASA FirePOWER 서비스 정책과 현재 통계 및 모듈 상태를 보여줍니다.

```
ciscoasa# show service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: my-sfr-class
      SFR: card status Up, mode fail-close
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

다음 예는 모니터 전용 정책을 보여줍니다. 이 경우 패킷 입력 카운터는 증가하지만 패킷 출력 카운터는 0에 머물러 있는 것을 볼 수 있습니다. 이는 ASA로 다시 전달되는 트래픽이 없기 때문입니다.

```
hostname# show service-policy sfr
Global policy:
  Service-policy: global_policy
    Class-map: bypass
      SFR: card status Up, mode fail-open, monitor-only
        packet input 2626422041, packet output 0, drop 0, reset-drop 0, proxied 0
```

모듈 연결 모니터링

ASA FirePOWER 모듈을 통한 연결을 표시하려면 다음 명령 중 하나를 입력합니다.

- **show asp table classify domain sfr**

  ASA FirePOWER 모듈로 트래픽을 전송하기 위해 만든 NP 규칙을 표시합니다.

- **show asp drop**

  삭제된 패킷을 표시합니다. 패킷 유형에 대한 설명은 아래와 같습니다.

- **show conn**

  'X - inspected by service module' 플래그를 표시하여 연결이 모듈로 전달되는지를 보여줍니다.

show asp drop 명령은 ASA FirePOWER 모듈과 관련된 다음과 같은 삭제 이유를 포함할 수 있습니다.

프레임 삭제:

- sfr-bad-tlv-received - ASA가 Policy ID TLV 없이 FirePOWER에서 패킷을 수신할 때 발생합니다. 작업 필드에 Standby/Active 비트가 설정되지 않은 경우 이 TLV는 비 제어 패킷에 있어야 합니다.
- sfr-request - FirePOWER에 대한 정책 때문에 FirePOWER에서 프레임 삭제를 요청했습니다. FirePOWER는 작업을 Deny Source, Deny Destination 또는 Deny Pkt로 설정할 수 있습니다. 프레임이 삭제되지 않은 경우 흐름을 거부하는 모듈의 정책을 검토하십시오.
- sfr-fail-close - 카드가 작동되지 않고 구성된 정책이 'fail-close'(카드가 비작동 상태여도 패킷 통과를 허용하는 'fail-open'이 아니라)이므로 패킷이 삭제됩니다. 카드 상태를 점검하고 서비스를 다시 시작하거나 다시 부팅해보십시오.
- sfr-fail - 기존 흐름에 대해 FirePOWER 컨피그레이션이 제거되었고 FirePOWER를 통해 기존 흐름을 처리할 수 없으므로 삭제됩니다. 이 상황은 발생할 가능성이 매우 낮습니다.
- sfr-malformed-packet - FirePOWER의 패킷에 잘못된 헤더가 포함되어 있습니다. 예를 들면 헤더 길이가 정확하지 않을 수 있습니다.
- sfr-ha-request - 보안 어플라이언스가 FirePOWER HA 요청 패킷을 수신하지만 처리할 수 없어서 패킷이 삭제되면 이 카운터가 증가합니다.
- sfr-invalid-encap - 보안 어플라이언스가 잘못된 메시지 헤더가 포함된 FirePOWER 패킷을 수신하여 패킷이 삭제되면 이 카운터가 증가합니다.
- sfr-bad-handle-received - FirePOWER 모듈의 패킷에서 잘못된 흐름 핸들을 수신하여 흐름을 삭제합니다. FirePOWER 흐름에 대한 핸들이 흐름 기간 중에 변경되었으므로 이 카운터가 증가하고 흐름과 패킷이 ASA에서 삭제됩니다.
- sfr-rx-monitor-only - 보안 어플라이언스가 모니터 전용 모드에서 FirePOWER 패킷을 수신하여 패킷이 삭제되면 이 카운터가 증가합니다.

흐름 삭제:

- sfr-request - FirePOWER에서 흐름 종료를 요청했습니다. 작업 비트 0이 설정됩니다.
- reset-by-sfr - FirePOWER에서 흐름 종료 및 재설정을 요청했습니다. 작업 비트 1이 설정됩니다.
- sfr-fail-close - 카드가 작동하지 않으며 구성된 정책이 'fail-close'이므로 흐름이 종료되었습니다.

ASA FirePOWER 모듈의 예

다음 예는 모든 HTTP 트래픽을 ASA FirePOWER 모듈로 전환하고, 어떤 이유로든 모듈이 실패하면 모든 HTTP 트래픽을 차단합니다.

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

다음 예는 10.1.1.0 및 10.2.1.0 네트워크로 향하는 모든 IP 트래픽을 ASA FirePOWER 모듈로 전환하고, 어떤 이유로든 모듈이 실패하면 모든 트래픽을 허용합니다.

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

ASA FirePOWER 모듈의 기록

기능 이름	플랫폼 릴리스	기능 정보
ASA 5585-X(모든 모델)는 일치하는 ASA FirePOWER SSP 하드웨어 모듈을 지원합니다. ASA 5512-X~ASA 5555-X는 ASA FirePOWER 소프트웨어 모듈을 지원합니다.	ASA 9.2(2.4) ASA FirePOWER 5.3.1	ASA FirePOWER 모듈은 NGIPS(Next-Generation IPS), AVC(Application Visibility and Control), URL 필터링, AMP(Advanced Malware Protection)를 비롯한 차세대 방화벽 서비스를 제공합니다. 단일/다중 컨텍스트 모드 및 라우팅된/투명 모드에서 이 모듈을 사용할 수 있습니다. 추가 또는 수정된 명령: **capture interface asa_dataplane**, **debug sfr**, **hw-module module 1 reload**, **hw-module module 1 reset**, **hw-module module 1 shutdown**, **session do setup host ip, session do get-config, session do password-reset, session sfr, sfr, show asp table classify domain sfr**, **show capture**, **show conn**, **show module sfr**, **show service-policy, sw-module sfr**.

18 장

ASA CX 모듈

이 장에서는 ASA에서 실행되는 ASA CX 모듈을 구성하는 방법에 대해 설명합니다.

ASA CX 모듈

ASA CX 모듈을 사용하면 상황의 완전한 컨텍스트를 기반으로 보안을 적용할 수 있습니다. 이 컨텍스트에는 사용자의 신원(누가), 사용자가 액세스하려는 애플리케이션 또는 웹사이트(무엇을), 액세스 시도의 근원지(어디), 시도된 액세스 시간(언제) 및 액세스에 사용된 디바이스의 속성(어떻게)이 포함됩니다. ASA CX 모듈을 사용하면 흐름의 완전한 컨텍스트를 파악하여 세부적인 정책을 적용할 수 있습니다. 예를 들어 Facebook에 대한 액세스는 허용하되 Facebook의 게임에 대한 액세스는 거부하거나, 재무 관련 직원의 회사 기밀 데이터베이스에 대한 액세스는 허용하되 다른 직원의 액세스는 거부할 수 있습니다.

ASA CX 모듈이 ASA에서 작동하는 방식

ASA CX 모듈은 ASA에서 별도의 애플리케이션을 실행합니다. 모듈은 하드웨어 모듈(ASA 5585-X) 또는 소프트웨어 모듈(5512-X~5555-X)일 수 있습니다. 하드웨어 모듈인 경우 디바이스에는 별도의 관리 및 콘솔 포트, 그리고 ASA에서는 직접 사용하지만 모듈 자체에서는 사용하지 않는 추가 데이터 인터페이스가 포함됩니다.

디바이스를 일반 인라인 모드에서 구성할 수도 있고, 데모용인 경우 모니터 전용(monitor-only) 모드에서 구성할 수도 있습니다.

- 인라인 배포 시에는 실제 트래픽이 디바이스로 전송되며, 디바이스의 정책이 트래픽에 영향을 미칩니다. 원하지 않는 트래픽을 취소하고 정책에 의해 적용되는 다른 작업을 수행한 후 추가 처리 및 최종 전송을 위해 트래픽을 ASA로 반환합니다.
- 모니터 전용 배포에서는 트래픽의 복사본이 디바이스로 전송되지만 ASA로 반환되지는 않습니다. 모니터 전용 모드에서는 네트워크에 영향을 미치지 않은 채, 디바이스가 트래픽에 어떤 작업을 수행할지를 알아볼 수 있습니다. 모니터 전용 서비스 정책 또는 트래픽 포워딩 인터페이스를 사용하여 이 모드를 구성할 수 있습니다. 모니터 전용 모드의 지침 및 제한은 18-6 페이지의 ASA CX 지침을 참조하십시오.

다음 섹션에서는 이러한 모드에 대해 좀 더 자세히 설명합니다.

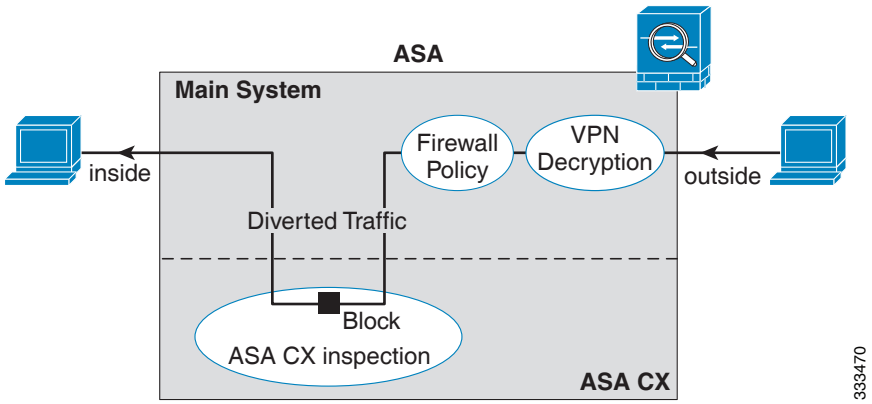
ASA CX 일반 인라인 모드

일반 인라인 모드에서는 트래픽이 ASA CX 모듈로 전달되기 전에 방화벽 점검을 거치게 됩니다. ASA에서 ASA CX 검사를 통해 트래픽을 식별할 경우, ASA 및 ASA CX 모듈에서 트래픽이 다음과 같이 흐릅니다.

1. 트래픽이 ASA로 들어갑니다.
2. 들어오는 VPN 트래픽이 암호 해독됩니다.
3. 방화벽 정책이 적용됩니다.
4. 트래픽이 ASA CX 모듈로 전송됩니다.
5. ASA CX 모듈이 보안 정책을 트래픽에 적용하고 적절한 작업을 수행합니다.
6. 유효한 트래픽은 ASA로 다시 전송됩니다. ASA CX 모듈은 자체 보안 정책에 따라 일부 트래픽을 차단할 수 있으며, 그러한 트래픽은 전달되지 못합니다.
7. 나가는 VPN 트래픽이 암호화됩니다.
8. 트래픽이 ASA를 빠져나갑니다.

다음 그림은 ASA CX 모듈 사용 시 트래픽 흐름을 보여줍니다. 이 예에서 ASA CX 모듈은 특정 애플리케이션에 대해 허용되지 않는 트래픽을 자동으로 차단합니다. 다른 모든 트래픽은 ASA를 통해 전달됩니다.

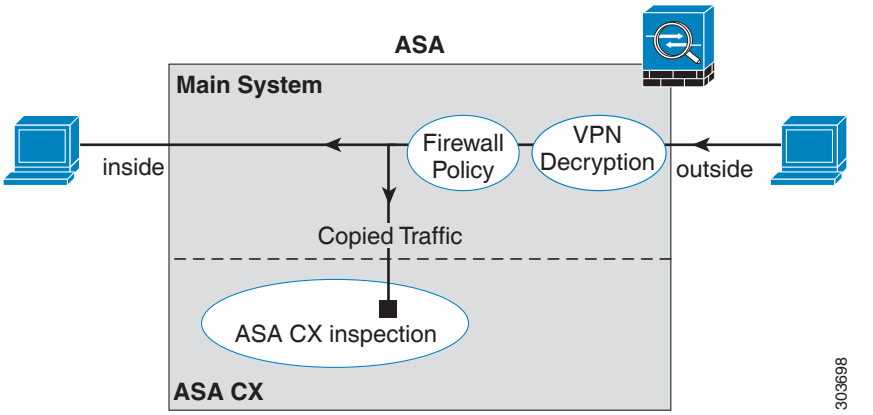
그림 18-1 ASA에서 ASA CX 모듈 트래픽 흐름



모니터 전용 모드의 서비스 정책

테스트 및 데모용으로 읽기 전용 트래픽을 ASA CX 모듈로 전송하도록 ASA를 구성할 수 있습니다. 그러면 ASA 트래픽 흐름에 영향을 미치지 않은 채 모듈이 트래픽을 어떻게 검사하는지 확인할 수 있습니다. 이 모드에서 ASA CX 모듈은 정상적으로 트래픽을 검사하고, 정책 결정을 내리고, 이벤트를 생성합니다. 그러나 패킷이 읽기 전용 복사본이므로 모듈 작업이 실제 트래픽에 영향을 미치지는 않습니다. 대신, 검사 후 모듈이 복사본을 삭제합니다. 다음 그림은 모니터 전용 모드의 ASA CX 모듈을 보여줍니다.

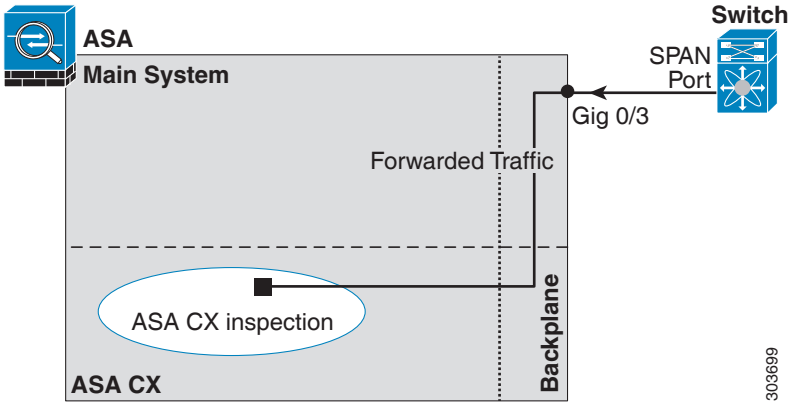
그림 18-2 ASA CX 모니터 전용



모니터 전용 모드의 트래픽 포워딩 인터페이스

ASA 인터페이스를 트래픽 포워딩 인터페이스로 구성할 수도 있습니다. 이 경우 수신된 모든 트래픽은 ASA 프로세싱 없이 ASA CX 모듈로 직접 전달됩니다. 테스트 및 데모용의 경우 트래픽 포워딩을 사용하면 별도의 복잡한 ASA 프로세싱이 제거됩니다. 트래픽 포워딩은 모니터 전용 모드에서만 지원되므로 ASA CX 모듈은 트래픽을 검사한 후 취소합니다. 다음 그림은 트래픽 포워딩을 위해 구성된 ASA GigabitEthernet 0/3 인터페이스를 보여줍니다. ASA CX 모듈이 네트워크 트래픽을 모두 검사할 수 있도록 해당 인터페이스는 스위치 SPAN 포트에 연결됩니다.

그림 18-3 ASA CX 트래픽 포워딩



ASA CX 관리 액세스

ASA CX 모듈을 관리하기 위한 두 개의 액세스 레이어, 즉 초기 컨피그레이션(및 후속 문제 해결) 레이어와 정책 관리 레이어가 있습니다.

- 18-4 페이지의 초기 컨피그레이션
- 18-5 페이지의 정책 컨피그레이션 및 관리

초기 컨피그레이션

초기 컨피그레이션에서 **setup** 명령을 실행하고 기타 선택적인 설정을 구성하려면 ASA CX 모듈에서 CLI를 사용해야 합니다.

CLI에 액세스하려면 다음 방법을 사용할 수 있습니다.

- ASA 5585-X:
  - ASA CX 콘솔 포트 - ASA CX 콘솔 포트는 별도의 외부 콘솔 포트입니다.
  - SSH를 사용하는 ASA CX Management 1/0 인터페이스 - 기본 IP 주소(192.168.8.8)에 연결하거나, ASDM을 사용하여 관리 IP 주소를 변경한 다음 SSH를 사용하여 연결할 수 있습니다. ASA CX 관리 인터페이스는 별도의 외부 기가비트 이더넷 인터페이스입니다.

참고 **session** 명령을 사용하여 ASA 백플레인을 통해 ASA CX 하드웨어 모듈 CLI에 액세스할 수 없습니다.

- ASA 5512-X~ASA 5555-X:
  - 백플레인을 통한 ASA 세션 - ASA에 CLI 액세스가 가능한 경우 모듈에 대한 세션을 시작하고 모듈 CLI에 액세스할 수 있습니다.
  - SSH를 사용하는 ASA CX Management 0/0 인터페이스 - 기본 IP 주소(192.168.1.2)에 연결하거나, ASDM을 사용하여 관리 IP 주소를 변경한 다음 SSH를 사용하여 연결할 수 있습니다. 이러한 모델은 ASA CX 모듈을 소프트웨어 모듈로서 실행합니다. ASA CX 관리 인터페이스는 Management 0/0 인터페이스를 ASA와 공유합니다. ASA 및 ASA CX 모듈에 대해 별도의 MAC 주소와 IP 주소가 지원됩니다. ASA CX 운영 체제 내에서 ASA CX IP 주소를 구성해야 합니다(CLI 또는 ASDM 사용). 그러나 물리적 특성(예: 인터페이스 활성화)은 ASA에서 구성됩니다. 이 인터페이스를 ASA CX 전용 인터페이스로 지정하려면 ASA 인터페이스 컨피그레이션(특히 인터페이스 이름)을 제거할 수 있습니다. 이 인터페이스는 관리 전용입니다.

정책 컨피그레이션 및 관리

초기 컨피그레이션을 수행한 후 Cisco PRSM(Prime Security Manager)을 사용하여 ASA CX 정책을 구성합니다. PRSM은 ASA CX 컨피그레이션 인터페이스의 이름이자 동시에 ASA CX 디바이스를 구성하기 위한 별도 제품의 이름(Cisco Prime Security Manager)입니다.

그런 다음 ASDM, ASA CLI 또는 PRSM(다중 디바이스 모드)을 사용하여 ASA CX 모듈로 트래픽을 전송하기 위한 ASA 정책을 구성합니다.

능동적 인증을 위한 인증 프록시

액세스 정책에 사용할 사용자 ID 정보를 수집하기 위해 ASA CX에서 ID 정책을 구성할 수 있습니다. 시스템에서는 사용자 ID를 능동적으로(사용자 이름과 비밀번호 자격 증명을 입력하라는 메시지를 표시하여) 또는 수동적으로(AD 에이전트 또는 Cisco CDA(Context Directory Agent)가 수집한 정보를 검색하여) 수집할 수 있습니다.

능동적 인증을 사용하려면 인증 프록시 역할을 하도록 ASA를 구성해야 합니다. ASA CX 모듈은 인증 요청을 ASA 인터페이스 IP 주소/프록시 포트로 리디렉션합니다. 기본 포트는 885지만 다른 포트를 구성할 수 있습니다.

능동적 인증을 활성화하려면 18-16 페이지의 ASA CX 서비스 정책 만들기에서 설명한 대로 ASA CX에 대한 트래픽을 리디렉션하는 서비스 정책의 일부로서 인증 프록시를 활성화할 수 있습니다.

ASA 기능과의 호환성

ASA에는 HTTP 검사를 비롯한 많은 고급 애플리케이션 검사 기능이 포함되어 있습니다. 그러나 ASA CX 모듈은 ASA에서 제공하는 것보다 더 향상된 HTTP 검사 기능은 물론, 애플리케이션 사용량 모니터링과 제어 등 애플리케이션에 대한 추가 기능도 제공합니다.

ASA CX 모듈 기능을 충분히 활용하려면 ASA CX 모듈로 전송하는 트래픽에 대한 다음 지침을 참조하십시오.

- HTTP 트래픽에 대해 ASA 검사를 구성하지 마십시오.
- Cloud Web Security(ScanSafe) 검사를 구성하지 마십시오. 동일한 트래픽에 대해 ASA CX 작업과 Cloud Web Security 검사를 모두 구성하면 ASA에서는 ASA CX 작업만 수행합니다.
- 기본 검사를 비롯하여 ASA에서 수행하는 기타 애플리케이션 검사는 ASA CX 모듈과 호환됩니다.
- MUS(Mobile User Security) 서버를 활성화하지 마십시오. ASA CX 모듈과 호환되지 않습니다.
- ASA 클러스터링을 활성화하지 마십시오. ASA CX 모듈과 호환되지 않습니다.

ASA CX 모듈의 라이센싱 요구 사항

ASA CX 모듈과 PRSM에는 추가 라이센스가 필요합니다. 이러한 라이센스는 ASA의 컨텍스트보다는 모듈 자체에 설치해야 합니다. ASA 자체에는 추가 라이센스가 필요하지 않습니다. 자세한 내용은 ASA CX 설명서를 참조하십시오.

ASA CX 전제 조건

PRSM을 사용하여 ASA를 구성하려면 안전한 통신을 위해 ASA에 인증서를 설치해야 합니다. 기본적으로 ASA는 자체 서명 인증서를 생성합니다. 그러나 이 인증서의 경우 게시자가 알려지지 않았기 때문에 브라우저에 인증서를 확인하라는 메시지가 표시될 수 있습니다. 브라우저에 이러한 메시지가 표시되지 않게 하려면 알려진 CA(인증 기관)의 인증서를 설치할 수 있습니다. CA의 인증서를 요청하는 경우 인증서 유형은 서버 인증 인증서 및 클라이언트 인증 인증서여야 합니다. 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

ASA CX 지침

컨텍스트 모드 지침

ASA CX 9.1(3)부터 다중 컨텍스트 모드가 지원됩니다.

그러나 ASA CX 모듈 자체(PRSM에서 구성)는 단일 컨텍스트 모드 디바이스입니다. ASA에서 오는 컨텍스트별 트래픽은 공통된 ASA CX 정책을 기준으로 점검을 거치게 됩니다. 각 컨텍스트에는 고유한 네트워크가 포함되어 있으므로 다중 컨텍스트에서는 동일한 IP 주소를 사용할 수 없습니다.

방화벽 모드 지침

투명 및 라우팅된 방화벽 모드에서 지원됩니다. 트래픽 포워딩 인터페이스는 투명 모드에서만 지원됩니다.

장애 조치 지침

장애 조치를 직접 지원하지 않습니다. ASA가 장애 조치되면 기존 ASA CX 흐름은 새로운 ASA로 전송되지만, 트래픽은 ASA CX의 검사를 거치지 않고 ASA를 통과할 수 있습니다. ASA CX 모듈은 새로운 ASA에서 수신한 새 흐름에만 작동합니다.

ASA 클러스터링 지침

클러스터링은 지원되지 않습니다.

IPv6 지침

- IPv6을 지원합니다.
- (9.1(1) 이하) NAT 64를 지원하지 않습니다. 9.1(2) 이상에서는 NAT 64가 지원됩니다.

모델 지침

- ASA 5585-X 및 5512-X~ASA 5555-X에서만 지원됩니다. 자세한 내용은 *Cisco ASA Compatibility Matrix*를 참조하십시오.

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

- 5512-X~ASA 5555-X의 경우 Cisco SSD(Solid State Drive)를 설치해야 합니다. 자세한 내용은 ASA 5500-X 하드웨어 지침을 참조하십시오.

모니터 전용 모드 지침:

모니터 전용 모드는 모듈의 일반적인 운영 모드가 아니며 데모용으로만 사용해야 합니다.

- ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수 없습니다. 보안 정책 유형은 하나만 허용됩니다. 다중 컨텍스트 모드에서는 일부 컨텍스트에 대해 모니터 전용 모드를 구성할 수 없고, 다른 컨텍스트에 대해 일반 인라인 모드를 구성할 수 없습니다.
- 모니터 전용 모드에서는 다음 기능이 지원되지 않습니다.
  - 거부 정책
  - 능동적 인증
  - 암호 해독 정책
- ASA CX는 모니터 전용 모드에서 패킷 버퍼링을 수행하지 않으며, 이벤트는 best-effort 기준으로 생성됩니다. 예를 들어 일부 이벤트(예: 패킷 경계를 넘는 긴 URL)는 버퍼링 부족의 영향을 받을 수 있습니다.
- 모드가 일치하도록 ASA 정책 및 ASA CX를 구성해야 합니다(둘 다 모니터 전용 모드이거나 둘 다 일반 인라인 모드).

트래픽 포워딩 인터페이스를 위한 추가 지침:

- ASA는 투명 모드여야 합니다.
- 트래픽 포워딩 인터페이스로 최대 4개의 인터페이스를 구성할 수 있습니다. 기타 ASA 인터페이스는 정상적으로 사용할 수 있습니다.
- 트래픽 포워딩 인터페이스는 VLAN 또는 BVI가 아닌 물리적 인터페이스여야 합니다. 물리적 인터페이스에는 VLAN을 연결할 수 없습니다.
- 트래픽 포워딩 인터페이스는 ASA 트래픽에 사용할 수 없습니다. 이러한 인터페이스는 명명할 수 없으며, 장애 조치 또는 관리 전용 등 ASA 기능을 구성할 수 없습니다.
- ASA CX 트래픽용 서비스 정책과 트래픽 포워딩 인터페이스를 둘 다 구성할 수는 없습니다.

추가 지침 및 제한

- 18-5 페이지의 ASA 기능과의 호환성 섹션을 참조하십시오.
- 하드웨어 모듈에 설치된 소프트웨어 유형을 변경할 수 없습니다. ASA CX 모듈을 구매하면 나중에 여기에 다른 소프트웨어를 설치할 수 없습니다.

ASA CX의 기본값

다음 표에는 ASA CX 모듈의 기본 설정이 나열되어 있습니다.

표 18-1 기본 네트워크 매개변수

매개변수	기본값
관리 IP 주소	ASA 5585-X: Management 1/0 192.168.8.8/24 ASA 5512-X~ASA 5555-X: Management 0/0 192.168.1.2/24
게이트웨이	ASA 5585-X: 192.168.8.1/24 ASA 5512-X~ASA 5555-X: 192.168.1.1/24
SSH 또는 세션 사용자 이름	admin
비밀번호	Admin123

ASA CX 모듈 구성

ASA CX 모듈 컨피그레이션은 ASA CX 모듈에서 ASA CX 보안 정책을 컨피그레이션하고 ASA CX 모듈에 트래픽을 전송하도록 ASA를 구성하는 프로세스입니다. ASA CX 모듈을 구성하려면 다음 단계를 수행하십시오.

1단계 18-8 페이지의 ASA CX 관리 인터페이스 연결. ASA CX 관리 인터페이스 및 선택적으로 콘솔 인터페이스를 연결합니다.

2단계 18-11 페이지의 (ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 설치 또는 재이미지화.

3단계 18-13 페이지의 (ASA 5585-X) ASA CX 관리 IP 주소 변경(필요한 경우). 초기 SSH 액세스에 필요할 수 있습니다.

4단계 18-14 페이지의 기본 ASA CX 설정 구성. ASA CX 모듈에서 수행합니다.

5단계 18-15 페이지의 ASA CX 모듈에서 보안 정책 구성.

6단계 (선택 사항) 18-16 페이지의 인증 프록시 포트 구성

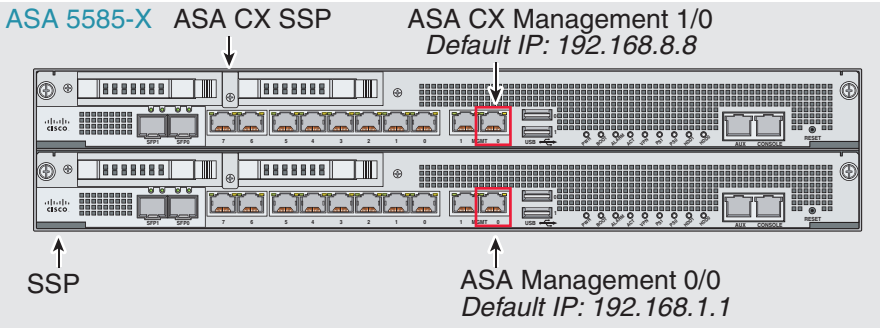
7단계 18-16 페이지의 ASA CX 모듈로 트래픽 리디렉션.

ASA CX 관리 인터페이스 연결

ASA CX 관리 인터페이스는 ASA CX 모듈에 대한 관리 액세스를 제공하는 것 외에도 시그니처 업데이트 등을 위해 HTTP 프록시 서버 또는 DNS 서버와 인터넷에 액세스해야 합니다. 이 섹션에서는 권장 네트워크 컨피그레이션에 대해 설명합니다. 네트워크는 환경에 따라 다를 수 있습니다.

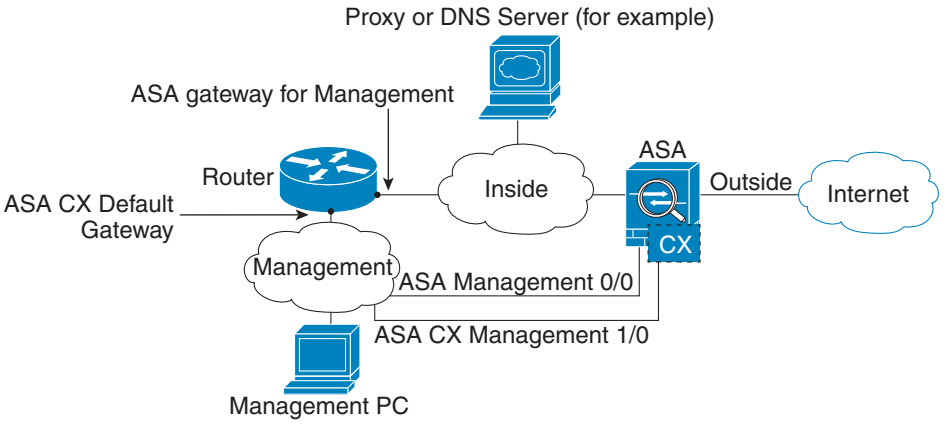
ASA 5585-X(하드웨어 모듈)

ASA CX 모듈에는 ASA에서 오는 별도의 관리 및 콘솔 인터페이스가 포함되어 있습니다. 초기 설정 시 기본 IP 주소(192.168.8.8/24)를 사용하여 SSH로 ASA CX Management 1/0 인터페이스에 연결할 수 있습니다. 기본 IP 주소를 사용할 수 없는 경우, SSH를 사용하기 위해 콘솔 포트 또는 ASDM을 사용하여 관리 IP 주소를 변경할 수 있습니다.



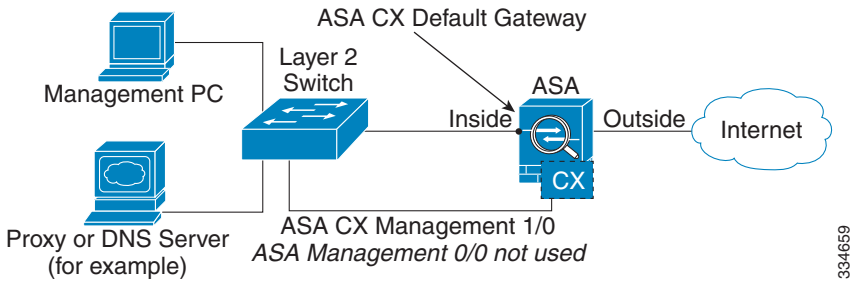
내부 라우터가 있는 경우

내부 라우터가 있으면 관리 네트워크(ASA Management 0/0 및 ASA CX Management 1/0 인터페이스를 모두 포함할 수 있음)와 인터넷 액세스용 ASA 내부 네트워크 간에 라우팅할 수 있습니다. 또한 내부 라우터를 통해 관리 네트워크에 도달하려면 ASA에서 경로를 추가해야 합니다.



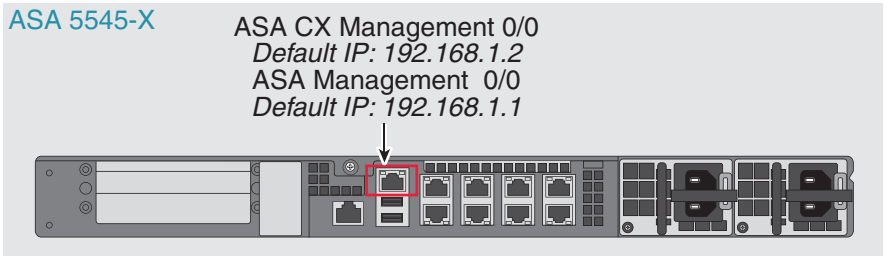
내부 라우터가 없는 경우

하나의 내부 네트워크만 있는 경우 별도의 관리 네트워크를 둘 수 없습니다. 네트워크 간 라우팅을 위해 내부 라우터가 필요하기 때문입니다. 이 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. ASA CX 모듈은 ASA와 분리된 디바이스이므로 내부 인터페이스와 동일한 네트워크에 오도록 ASA CX Management 1/0 주소를 구성할 수 있습니다.



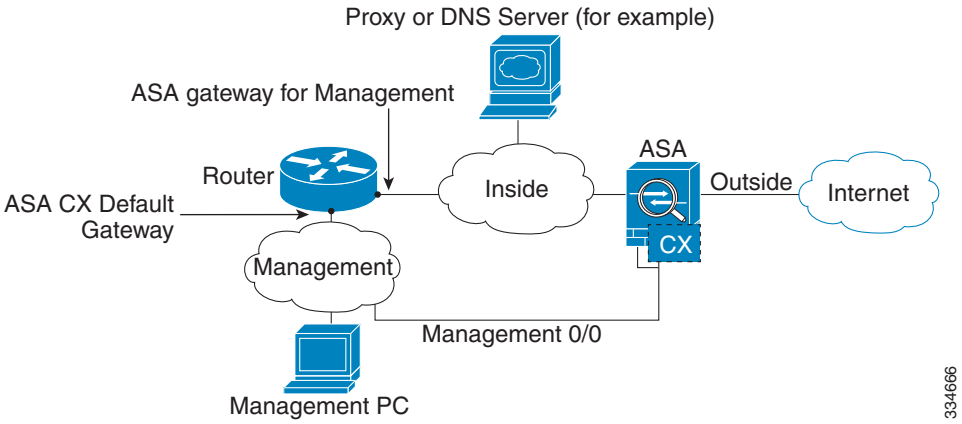
ASA 5512-X~ASA 5555-X(소프트웨어 모듈)

이러한 모듈은 ASA CX 모듈을 소프트웨어 모듈로서 실행하며, ASA CX 관리 인터페이스는 Management 0/0 인터페이스를 ASA와 공유합니다. 초기 설정 시 SSH로 ASA CX 기본 IP 주소(192.168.1.2/24)에 연결할 수 있습니다. 기본 IP 주소를 사용할 수 없는 경우, SSH를 사용할 수 있도록 ASDM을 사용하여 관리 IP 주소를 변경하거나 백플레인을 통해 ASA CX에 대한 세션을 시작할 수 있습니다.



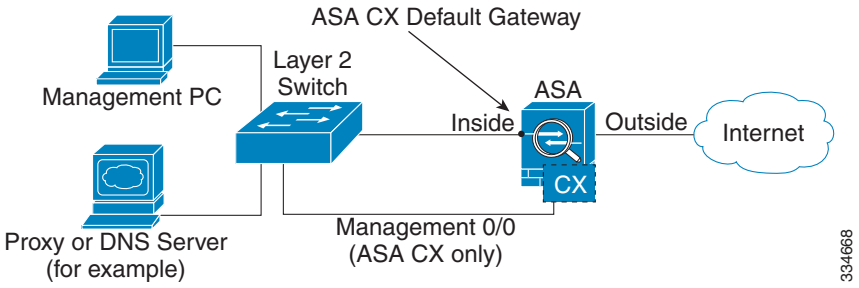
내부 라우터가 있는 경우

내부 라우터가 있으면 Management 0/0 네트워크(ASA 및 ASA CX 관리 IP 주소를 모두 포함)와 인터넷 액세스용 내부 네트워크 간에 라우팅할 수 있습니다. 또한 내부 라우터를 통해 관리 네트워크에 도달하려면 ASA에서 경로를 추가해야 합니다.



내부 라우터가 없는 경우

하나의 내부 네트워크만 있는 경우 별도의 관리 네트워크를 둘 수 없습니다. 이 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. ASA에서 구성한 이름을 Management 0/0 인터페이스에서 제거하더라도 해당 인터페이스에 대해 ASA CX IP 주소를 구성할 수 있습니다. ASA CX 모듈은 기본적으로 ASA와 분리된 디바이스이므로 내부 인터페이스와 동일한 네트워크에 오도록 ASA CX 관리 주소를 구성할 수 *있습니다.*



참고 ASA에서 구성한 이름을 Management 0/0에서 제거해야 합니다. ASA에서 구성한 경우 ASA CX 주소는 ASA와 동일한 네트워크에 있어야 합니다. 그러면 기타 ASA 인터페이스에서 이미 구성된 모든 네트워크가 제외됩니다. 이름이 구성되지 않은 경우 ASA CX 주소는 어떤 네트워크에든 둘 수 있습니다(예: ASA 내부 네트워크).

(ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 설치 또는 재이미지화

ASA CX 모듈과 함께 ASA를 구매하면 모듈 소프트웨어 및 필수 SSD(Solid State Drive)가 사전 설치되어 바로 사용할 수 있는 상태가 됩니다. ASA CX를 기존 ASA에 추가하거나 SSD를 교체해야 할 경우 ASA CX 부트 소프트웨어를 설치하고 다음 절차에 따라 SSD의 파티션을 만들어야 합니다. SSD를 물리적으로 설치하려면 ASA 하드웨어 가이드를 참조하십시오.

모듈 재이미지화 절차도 동일합니다. 단, ASA CX 모듈을 먼저 제거해야 합니다. SSD를 교체하는 경우 시스템을 재이미지화하게 됩니다.

참고 ASA 5585-X 하드웨어 모듈의 경우 ASA CX 모듈 내에서 이미지를 설치 또는 업그레이드해야 합니다. 자세한 내용은 ASA CX 모듈 설명서를 참조하십시오.

시작하기 전에

- 플래시의 빈 공간(disk0)은 최소 3GB + 부트 소프트웨어 크기가 되어야 합니다.
- 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.
- 실행 중인 다른 소프트웨어 모듈은 종료해야 합니다. 디바이스는 한 번에 하나의 소프트웨어 모듈을 실행할 수 있습니다. ASA CLI에서 수행해야 합니다. 예를 들어 다음 명령은 IPS 소프트웨어 모듈을 종료하고 제거한 다음 ASA를 다시 로드합니다.

```
hostname# sw-module module ips shutdown
hostname# sw-module module ips uninstall
hostname# reload
```

참고 트래픽을 IPS 모듈로 리디렉션하는 활성 서비스 정책이 있는 경우 해당 정책을 제거해야 합니다. 글로벌 정책이면 **no service-policy** *ips_policy* **global**을 사용하면 됩니다. CLI 또는 ASDM을 사용하여 정책을 제거할 수 있습니다.

- 모듈을 재이미지화할 때 동일한 종료 및 제거 명령을 사용하여 이전 이미지를 제거합니다. 예: **sw-module module cxsc uninstall**.
- ASA CX 부트 이미지 및 시스템 소프트웨어 패키지는 모두 Cisco.com에서 다운로드합니다. http://software.cisco.com/download/type.html?mdfid=284325223&flowid=34503

절차

1단계 부트 이미지를 디바이스로 다운로드합니다. 시스템 소프트웨어를 전송하지 마십시오. 나중에 SSD로 다운로드됩니다. 다음 옵션을 이용할 수 있습니다.

- ASDM - 먼저 부트 이미지를 워크스테이션으로 다운로드하거나 FTP, TFTP, HTTP, HTTPS, SMB 또는 SCP 서버에 둡니다. ASDM에서 **Tools > File Management**를 선택한 다음 적절한 **File Transfer** 명령, **Between Local PC and Flash** 또는 **Between Remote Server and Flash**를 선택합니다. 부트 소프트웨어를 ASA의 disk0으로 전송합니다.
- ASA CLI - 먼저 부트 이미지를 TFTP, FTP, HTTP 또는 HTTPS 서버에 둔 다음 **copy** 명령을 사용하여 플래시로 다운로드합니다. 다음 예에서는 TFTP를 사용합니다. <TFTP Server>를 각자의 서버 IP 주소 또는 호스트 이름으로 교체하십시오.

```
ciscoasa# copy tftp://<TFTP SERVER>/asacx-5500x-boot-9.3.1.1-112.img
disk0:/asacx-5500x-boot-9.3.1.1-112.img
```

2단계 Cisco.com의 ASA CX 시스템 소프트웨어를 ASA CX 관리 인터페이스에서 액세스할 수 있는 HTTP, HTTPS 또는 FTP 서버로 다운로드합니다.

3단계 다음 명령을 입력하여 ASA CX 모듈 부트 이미지 위치를 ASA disk0으로 설정합니다.

```
hostname# sw-module module cxsc recover configure image disk0:file_path
```

참고 "ERROR: Another service (ips) is running, only one service is allowed to run at any time"과 같은 메시지가 표시되면 이미 다른 소프트웨어 모듈이 구성되어 있다는 의미입니다. 위의 전제 조건 섹션에서 설명한 대로 새 모듈을 설치하려면 기존 모듈을 종료하고 제거해야 합니다.

예:

```
hostname# sw-module module cxsc recover configure image
disk0:asacx-5500x-boot-9.3.1.1-112.img
```

4단계 다음 명령을 입력하여 ASA CX 부트 이미지를 로드합니다.

```
hostname# sw-module module cxsc recover boot
```

5단계 ASA CX 모듈이 부팅할 때까지 약 5분 정도 기다린 후 현재 실행 중인 ASA CX 부트 이미지에 대한 콘솔 세션을 시작합니다. 기본 사용자 이름은 **admin**이고 기본 비밀번호는 **Admin123**입니다.

```
hostname# session cxsc console
Establishing console session with slot 1
Opening console session with module cxsc.
Connected to module cxsc. Escape character sequence is 'CTRL-SHIFT-6 then x'.
cxsc login: admin
Password: Admin123
```

팁 모듈 부팅이 완료되면, ttyS1을 통해 연결할 수 없다는 메시지와 함께 **session** 명령이 실패합니다. 기다렸다가 다시 시도하십시오.

6단계 SSD의 파티션을 만듭니다.

```
asacx-boot> partition
....
Partition Successfully Completed
```

7단계 18-14 페이지의 기본 ASA CX 설정 구성에 따라 **setup** 명령을 사용하여 기본적인 네트워크 설정을 수행한 다음(아직 ASA CX CLI를 종료하지 않음) 이 절차로 돌아와 소프트웨어 이미지를 설치합니다.

8단계 **system install** 명령을 사용하여 시스템 소프트웨어 이미지를 설치합니다.

system install [**noconfirm**] *url*

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다. HTTP, HTTPS 또는 FTP URL을 사용합니다. 사용자 이름과 비밀번호가 필요한 경우 입력하라는 메시지가 표시됩니다.

설치가 완료되면 시스템이 다시 부팅하며 콘솔 세션이 종료됩니다. 애플리케이션 구성 요소가 설치되고 ASA CX 서비스가 시작될 때까지 10분 이상 기다립니다. (**show module cxsc**가 출력되면 모든 프로세스가 완료된 것입니다.)

다음 명령은 asacx-sys-9.3.1.1-112.pkg 시스템 소프트웨어를 설치합니다.

```
asacx-boot> system install https://upgrades.example.com/packages/asacx-sys-9.3.1.1-112.pkg

Username: buffy
Password: angelforever
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA CX 9.3.1.1-112 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [n]: Y
Warning: Please do not interrupt the process or turn off the system. Doing so might leave
system in unusable state.
Upgrading
Stopping all the services ...
Starting upgrade process ...
Reboot is required to complete the upgrade. Press Enter to reboot the system.
```

(ASA 5585-X) ASA CX 관리 IP 주소 변경

기본 관리 IP 주소(192.168.8.8)를 사용할 수 없는 경우 ASA에서 관리 IP 주소를 설정할 수 있습니다. 관리 IP 주소를 설정하면 SSH를 사용하여 ASA CX 모듈에 액세스하고 초기 설정을 수행할 수 있습니다.

참고 소프트웨어 모듈의 경우 ASA CLI에서 세션을 시작하고 ASA CX CLI에 액세스하여 설정을 수행할 수 있습니다. 그런 다음 설정 과정에서 ASA CX 관리 IP 주소를 설정할 수 있습니다. 18-14 페이지의 기본 ASA CX 설정 구성 섹션을 참조하십시오.

ASA를 통해 관리 IP 주소를 변경하려면 다음 중 하나를 수행하십시오. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

- CLI에서 다음 명령을 사용하여 ASA CX 관리 IP 주소, 마스크 및 게이트웨이를 설정합니다.

  session 1 do setup host ip *ip_address*/*mask*,*gateway_ip*

  예: **session 1 do setup host ip 10.1.1.2/24,10.1.1.1**.

- (단일 컨텍스트 모드 전용) ASDM에서 **Wizards > Startup Wizard**를 선택하고 마법사의 과정에 따라 ASA CX Basic Configuration으로 이동합니다. 여기서 IP 주소, 마스크 및 기본 게이트웨이를 설정할 수 있습니다. 기본 포트가 적절하지 않으면 다른 인증 프록시 포트를 설정할 수도 있습니다.

기본 ASA CX 설정 구성

보안 정책을 구성하려면 우선 ASA CX 모듈에서 기본 네트워크 설정 및 기타 매개변수를 구성해야 합니다. 이러한 설정을 구성하기 위한 유일한 방법은 ASA CX CLI를 이용하는 것입니다.

절차

1단계 다음 중 하나를 수행합니다.

- (모든 모델) SSH를 사용하여 ASA CX 관리 IP 주소에 연결합니다.
- (ASA 5512-X~ASA 5555-X) ASA CLI에서 모듈에 대한 콘솔 세션을 엽니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 세션을 시작합니다.

  hostname# **session cxsc console**

2단계 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다. 이 절차를 수행하면서 비밀번호를 변경할 수 있습니다.

3단계 다음 명령을 입력합니다.

asacx> **setup**

예:

```
asacx> setup
Welcome to Cisco Prime Security Manager Setup
[hit Ctrl-C to abort]
Default values are inside [ ]
```

설정 마법사 과정 전체에서 프롬프트가 표시됩니다. 다음 예는 마법사 전체의 일반적인 과정을 보여줍니다. 프롬프트에서 **N** 대신 **Y**를 입력하면 몇 가지 추가 설정을 구성할 수 있습니다. 다음 예는 IPv4 및 IPv6 고정 주소를 구성하는 방법을 보여줍니다. 고정 IPv6 주소를 구성할지를 묻는 질문에 **N**이라고 대답하면 IPv6 무상태(stateless) 자동 컨피그레이션을 수행할 수 있습니다.

```
Enter a hostname [asacx]: asa-cx-host
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n)[N]: N
Enter an IPv4 address [192.168.8.8]: 10.89.31.65
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 10.89.31.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: Y
Enter an IPv6 address: 2001:DB8:0:CD30::1234/64
Enter the gateway: 2001:DB8:0:CD30::1
Enter the primary DNS server IP address [ ]: 10.89.47.11
Do you want to configure Secondary DNS Server? (y/n) [N]: N
Do you want to configure Local Domain Name? (y/n) [N] Y
```

```
Enter the local domain name: example.com
Do you want to configure Search domains? (y/n) [N] Y
Enter the comma separated list for search domains: example.com
Do you want to enable the NTP service?(y/n) [N]: Y
Enter the NTP servers separated by commas: 1.ntp.example.com, 2.ntp.example.com
```

4단계 최종 프롬프트를 완료하면 설정 요약이 표시됩니다. 요약에서 값이 올바른지 확인하고, 변경된 컨피그레이션을 적용하려면 **Y**를 입력합니다. 변경 사항을 취소하려면 **N**을 입력합니다.

예:

```
Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Done.
Generating self-signed certificate, the web server will be restarted after that
...
Done.
Press ENTER to continue...
asacx>
```

참고 호스트 이름을 변경하는 경우 로그아웃한 후 다시 로그인하기 전에는 새 이름이 표시되지 않습니다.

5단계 NTP를 사용하지 않는 경우 시간 설정을 구성합니다. 기본 시간대는 UTC입니다. 현재 설정을 보려면 **show time** 명령을 사용하십시오. 시간 설정을 변경하려면 다음 명령을 사용할 수 있습니다.

```
asacx> config timezone
asacx> config time
```

6단계 다음 명령을 입력하여 admin 비밀번호를 변경합니다.

```
asacx> config passwd
```

예:

```
asacx> config passwd
The password must be at least 8 characters long and must contain
at least one uppercase letter (A-Z), at least one lowercase letter
(a-z) and at least one digit (0-9).
Enter password: Farscape1
Confirm password: Farscape1
SUCCESS: Password changed for user admin
```

7단계 **exit** 명령을 입력하여 로그아웃합니다.

ASA CX 모듈에서 보안 정책 구성

ASA CX 모듈에서 보안 정책을 구성하려면 PRSM을 사용합니다. 보안 정책은 모듈이 제공하는 서비스를 제어합니다. ASA CX CLI, ASA CLI 또는 ASDM에서는 정책을 구성할 수 없습니다.

PRSM은 ASA CX 컨피그레이션 인터페이스의 이름이자 동시에 ASA CX 디바이스를 구성하기 위한 별도 제품의 이름(Cisco Prime Security Manager)입니다. 컨피그레이션 인터페이스에 액세스하는 방법과 인터페이스 사용 방법은 동일합니다. PRSM을 사용하여 ASA CX 보안 정책을 구성하는 방법에 대한 자세한 내용은 ASA CX/PRSM 사용자 가이드 또는 온라인 도움말을 참조하십시오.

PRSM을 열려면 웹 브라우저를 사용하여 다음 URL을 엽니다.

https://*management_address*

여기서 *management_address*는 ASA CX 관리 인터페이스 또는 PRSM 서버의 DNS 이름 또는 IP 주소입니다. 예: https://asacx.example.com.

인증 프록시 포트 구성

ASA CX 정책에서 능동적 인증을 사용하는 경우 ASA는 포트 885를 인증 프록시 포트로 사용합니다. 885를 사용할 수 없으면 다른 포트를 구성할 수 있지만, 기본이 아닌 포트는 1024보다 높아야 합니다. 인증 프록시에 대한 자세한 내용은 18-5 페이지의 능동적 인증을 위한 인증 프록시을 참조하십시오.

다중 컨텍스트 모드의 경우 각 보안 컨텍스트 내부에서 포트를 변경합니다.

인증 프록시 포트를 변경하려면 다음 명령을 입력합니다.

```
cxsc auth-proxy port port
```

예: **cxsc auth-proxy port 5000**.

ASA CX 모듈로 트래픽 리디렉션

특정 트래픽을 식별하는 서비스 정책을 만들어 ASA CX 모듈로 트래픽을 리디렉션할 수 있습니다. 데모용인 경우에만 서비스 정책에 대해 모니터 전용 모드를 활성화할 수 있습니다. 이 경우 트래픽의 복사본이 ASA CX 모듈로 전달되고 원래 트래픽은 영향을 받지 않습니다.

또 다른 데모용 옵션은 모니터 전용 모드에서 서비스 정책 대신 트래픽 포워딩 인터페이스를 구성하는 것입니다. 트래픽 포워딩 인터페이스는 ASA를 우회하여 모든 트래픽을 ASA CX 모듈로 직접 전송합니다.

- 18-16 페이지의 ASA CX 서비스 정책 만들기
- 18-18 페이지의 트래픽 포워딩 인터페이스 구성(모니터 전용 모드)

ASA CX 서비스 정책 만들기

특정 트래픽을 식별하는 서비스 정책을 만들어 ASA CX 모듈로 트래픽을 리디렉션할 수 있습니다.

참고 ASA CX 리디렉션은 양방향입니다. 따라서 한 인터페이스용 서비스 정책을 구성하면 해당 인터페이스의 호스트 및 리디렉션이 구성되지 않은 인터페이스의 호스트 간에 연결이 생성됩니다. 그러면 비 ASA CX 인터페이스에서 시작된 트래픽을 포함하여 두 호스트 간의 모든 트래픽이 ASA CX 모듈로 전송됩니다. 그러나 ASA는 서비스 정책이 적용된 인터페이스에서만 인증 프록시를 수행합니다. 인증 프록시는 인그레스(ingress) 트래픽에만 적용되기 때문입니다.

시작하기 전에

- 이 절차를 사용하여 ASA에서 인증 프록시를 활성화하려는 경우 ASA CX 모듈에서 인증을 위한 디렉토리 영역도 구성해야 합니다. 자세한 내용은 ASA 사용 설명서를 참조하십시오.
- 트래픽을 IPS 모듈(ASA CX와 교체한 모듈)로 리디렉션하는 활성 서비스 정책이 있는 경우 이 정책을 먼저 제거한 후 ASA CX 서비스 정책을 구성해야 합니다.
- 모드가 일치하도록 ASA 정책 및 ASA CX를 구성해야 합니다(둘 다 모니터 전용 모드이거나 둘 다 일반 인라인 모드).

- 다중 컨텍스트 모드의 경우 각 보안 컨텍스트 내부에서 이 절차를 수행합니다.
- 다중 디바이스 모드에서 PRSM을 사용할 경우 아래에서 설명한 대로, ASDM 또는 ASA CLI를 사용하는 대신 PRSM 내에서 ASA CX 모듈로 트래픽을 전송할 수 있도록 ASA 정책을 구성할 수 있습니다. 그러나 PRSM의 경우 ASA 서비스 정책을 구성할 때 몇 가지 제한이 있습니다. 자세한 내용은 ASA CX 사용 설명서를 참조하십시오.

절차

1단계 모듈로 전송할 트래픽을 식별하기 위한 L3/L4 클래스 맵을 만듭니다.

```
class-map name
match parameter
```

예:

```
hostname(config)# class-map cx_class
hostname(config-cmap)# match access-list cx_traffic
```

다중 트래픽 클래스를 모듈로 전송하려면 보안 정책에서 사용할 다중 클래스 맵을 만들 수 있습니다.

매칭 명령문에 대한 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵)을 참조하십시오.

2단계 클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

```
policy-map name
```

예:

```
hostname(config)# policy-map global_policy
```

기본 컨피그레이션에서 global_policy 정책 맵은 모든 인터페이스에 전체적으로 할당됩니다. global_policy를 편집하려면 정책 이름으로 global_policy를 입력합니다.

3단계 이 절차의 시작 부분에 만든 클래스 맵을 확인합니다.

```
class name
```

예:

```
hostname(config-pmap)# class cx_class
```

4단계 트래픽을 ASA CX 모듈로 전송합니다.

```
cxsc {fail-close | fail-open} [auth-proxy | monitor-only]
```

여기서 각 항목은 다음을 나타냅니다.

- **fail-close** 키워드는 ASA CX 모듈을 사용할 수 없는 경우 모든 트래픽을 차단하도록 ASA를 설정합니다.
- **fail-open** 키워드는 모듈을 사용할 수 없는 경우 검사 없이 모든 트래픽을 허용하도록 ASA를 설정합니다.
- 선택 사항인 **auth-proxy** 키워드는 능동적 인증 시 필요한 인증 프록시를 활성화합니다.
- 데모용인 경우에만, 트래픽의 읽기 전용 복사본을 ASA CX 모듈로 전송하도록 **monitor-only**를 지정합니다. 모든 클래스 및 정책을 모니터 전용 모드 또는 일반 인라인 모드로 구성해야 합니다. 동일한 ASA에서 두 모드를 혼합할 수 없습니다.

예:

```
hostname(config-pmap-c)# cxsc fail-close auth-proxy
```

5단계 ASA CX 트래픽용 다중 클래스 맵을 만든 경우 정책에 대한 또 다른 클래스를 지정하고 **cxsc** 리디렉션 작업을 적용할 수 있습니다.

클래스의 순서가 정책 맵에서 어떤 의미를 갖는지를 자세히 알아보려면 1-5 페이지의 서비스 정책 내에서의 기능 일치를 참조하십시오. 트래픽은 동일한 작업 유형에 대해 둘 이상의 클래스 맵과 일치할 수 없습니다.

6단계 기존 서비스 정책(예: global_policy라는 기본 글로벌 정책)을 편집하는 경우 모두 완료된 것입니다. 그렇지 않은 경우 하나 이상의 인터페이스에 대한 정책 맵을 활성화합니다.

service-policy *policymap_name* {**global** | **interface** *interface_name*}

예:

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

global 키워드는 모든 인터페이스에 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

트래픽 포워딩 인터페이스 구성(모니터 전용 모드)

데모용인 경우에만 트래픽 포워딩 인터페이스를 구성할 수 있습니다. 이 경우 모든 트래픽이 ASA CX 모듈로 직접 전달됩니다. 일반 ASA CX 작동에 대해서는 18-16 페이지의 ASA CX 서비스 정책 만들기를 참조하십시오.

자세한 내용은 18-4 페이지의 모니터 전용 모드의 트래픽 포워딩 인터페이스 섹션을 참조하십시오. 트래픽 포워딩 인터페이스와 관련된 지침 및 제한은 18-6 페이지의 ASA CX 지침을 참조하십시오.

시작하기 전에

- 모드가 일치하도록 ASA 정책 및 ASA CX를 구성해야 합니다(둘 다 모니터 전용 모드).
- 다중 컨텍스트 모드의 경우 각 보안 컨텍스트 내부에서 이 절차를 수행합니다.

절차

1단계 트래픽 포워딩을 사용하려는 물리적 인터페이스에 대해 인터페이스 컨피그레이션 모드로 들어갑니다.

interface *physical_interface*

예:

```
hostname(config)# interface gigabitethernet 0/5
```

2단계 인터페이스에 대해 구성된 이름을 제거합니다. 이 인터페이스가 ASA 컨피그레이션에서 사용된 경우 해당 컨피그레이션이 제거됩니다. 명명된 인터페이스에서는 트래픽 포워딩을 구성할 수 없습니다.

no nameif

3단계 트래픽 포워딩을 활성화합니다.

traffic-forward cxsc monitor-only

4단계 인터페이스를 활성화합니다.

```
no shutdown
```

추가 인터페이스에 대해 반복합니다.

예

다음 예에서는 GigabitEthernet 0/5 a 트래픽 포워딩 인터페이스를 만듭니다.

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

ASA CX 모듈 관리

이 섹션에는 모듈 관리에 도움이 되는 절차가 포함되어 있습니다.

비밀번호 재설정

모듈 비밀번호를 기본값으로 재설정할 수 있습니다. 사용자 **admin**에 대한 기본 비밀번호는 **Admin123**입니다. 비밀번호를 재설정한 후 모듈 애플리케이션을 사용하여 고유한 값으로 변경해야 합니다.

모듈 비밀번호를 재설정하면 모듈이 재부팅됩니다. 모듈이 재부팅되는 동안에는 서비스를 사용할 수 없습니다.

모듈 비밀번호를 기본값으로 재설정하려면 다음 방법 중 하나를 사용합니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

- (CLI) 하드웨어 모듈(ASA 5585-X):

  ```
  hw-module module 1 password-reset
  ```

- (CLI) 소프트웨어 모듈(ASA 5512-X~ASA 5555-X):

  ```
  sw-module module cxsc password-reset
  ```

모듈 다시 로드 또는 재설정

모듈을 다시 로드하거나 재설정 후 다시 로드하려면 ASA CLI에서 다음 명령 중 하나를 입력합니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

- 하드웨어 모듈(ASA 5585-X):

  hw-module module 1 {**reload** | **reset**}

- 소프트웨어 모듈(ASA 5512-X~ASA 5555-X):

  sw-module module cxsc {**reload** | **reset**}

모듈 종료

모듈 소프트웨어를 종료하면 컨피그레이션 데이터를 잃지 않은 채 모듈의 전원을 안전하게 끌 수 있습니다. 모듈을 정상적으로 종료하려면 ASA CLI에서 다음 명령 중 하나를 입력합니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

참고 ASA를 다시 로드하면 모듈이 자동으로 종료되지 않습니다. 따라서 ASA를 다시 로드하기 전에 모듈을 종료하는 것이 좋습니다.

- 하드웨어 모듈(ASA 5585-X):

  hw-module module 1 shutdown

- 소프트웨어 모듈(ASA 5512-X~ASA 5555-X):

  sw-module module cxsc shutdown

(ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 이미지 제거

소프트웨어 모듈 이미지 및 관련 컨피그레이션을 제거할 수 있습니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

절차

1단계 소프트웨어 모듈 이미지 및 관련 컨피그레이션을 제거합니다.

```
hostname# sw-module module cxsc uninstall

Module cxsc will be uninstalled. This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module cxsc? [confirm]
```

2단계 ASA를 다시 로드합니다. 새 모듈을 설치하려면 먼저 ASA를 다시 로드해야 합니다.

```
hostname# reload
```

(ASA 5512-X~ASA 5555-X) ASA에서 모듈에 대한 세션 시작

기본 네트워크 설정을 구성하고 모듈 관련 문제를 해결하려면 ASA CX CLI를 사용하십시오.

ASA에서 ASA CX 소프트웨어 모듈 CLI에 액세스하려면 ASA에서 세션을 시작할 수 있습니다. 모듈에 대한 세션을 시작하거나(텔넷 사용) 가상 콘솔 세션을 만들 수 있습니다. 제어 평면이 다운되어 텔넷 세션을 설정할 수 없는 경우 콘솔 세션이 유용할 수 있습니다. 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 세션을 시작합니다.

텔넷 또는 콘솔 세션에서 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시됩니다. **admin** 사용자 이름 및 비밀번호(기본값은 **Admin123**)를 사용합니다.

- 텔넷 세션:

  ```
  session cxsc
  ```

  ASA CX CLI에서 종료 후 ASA CLI로 돌아가려면 **exit** 명령을 사용하거나 **Ctrl-Shift-6, x**를 누릅니다.

- 콘솔 세션:

  ```
  session cxsc console
  ```

  콘솔 세션을 종료하는 유일한 방법은 **Ctrl-Shift-6, x**를 누르는 것입니다. 모듈에서 로그아웃하면 모듈 로그인 프롬프트가 표시됩니다.

참고 터미널 서버에서는 **session cxsc console** 명령을 사용하지 마십시오. 여기서 **Ctrl-Shift-6, x**는 터미널 서버 프롬프트로 돌아가기 위한 이스케이프 시퀀스입니다. **Ctrl-Shift-6, x**는 ASA CX 콘솔을 이스케이프하고 ASA 프롬프트로 돌아가기 위한 시퀀스이기도 합니다. 그러므로 이 상황에서 ASA CX 콘솔을 종료하려고 시도하면 대신 종료 후 터미널 서버 프롬프트에 이르게 됩니다. 터미널 서버를 ASA에 다시 연결하면 ASA CX 콘솔 세션은 여전히 활성 상태이므로, 종료 후 ASA 프롬프트로 돌아갈 수 없습니다. 콘솔을 ASA 프롬프트로 되돌리려면 직접 직렬 연결을 사용해야 합니다. 이러한 상황에서는 콘솔 명령 대신 **session cxsc** 명령을 사용하십시오.

ASA CX 모듈 모니터링

다음 항목에서는 모듈 모니터링에 대한 지침을 제공합니다. ASA CX 관련 syslog 메시지에 대해서는 syslog 메시지 가이드를 참조하십시오. ASA CX syslog 메시지는 메시지 번호 429001부터 시작합니다.

- 18-21 페이지의 모듈 상태 표시
- 18-22 페이지의 모듈 통계 표시
- 18-23 페이지의 모듈 연결 모니터링

모듈 상태 표시

모듈 상태를 확인하려면 다음 명령 중 하나를 입력합니다.

- **show module** [**1** | **cxsc**] [**details**]

  모듈 상태를 표시합니다. ASA CX 모듈과 관련된 상태를 보려면 1(하드웨어 모듈의 경우) 또는 cxsc(소프트웨어 모듈의 경우) 키워드를 포함합니다. 모듈을 관리하는 디바이스의 주소를 비롯한 추가 정보를 보려면 details 키워드를 포함합니다.

- **show module cxsc recover**

  모듈 설치 시 사용된 부트 이미지의 위치를 표시합니다.

다음은 ASA CX SSP가 설치된 ASA에서 **show module** 명령을 실행한 샘플 출력입니다.

```
hostname# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1507AMKE
  1 ASA 5585-X CX Security Services Processor-10 ASA5585-SSP-CX10   JAF1510BLSA

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1100 to 5475.d05b.110b  1.0          2.0(7)0      100.7(6)78
  1 5475.d05b.2450 to 5475.d05b.245b  1.0          2.0(13)0     0.6.1

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 ASA CX Security Module         Up               0.6.1

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

모듈 통계 표시

각 서비스 정책에 대한 통계와 상태를 표시하려면 **cxsc** 명령이 포함된 **show service-policy cxsc** 명령을 사용합니다. 카운터를 지우려면 **clear service-policy**를 사용합니다.

다음은 **show service-policy** 명령의 샘플 출력으로, ASA CX 정책과 현재 통계는 물론 인증 프록시가 비활성화되었을 때의 모듈 상태도 보여줍니다.

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: global_policy
    Class-map: bypass
      CXSC: card status Up, mode fail-open, auth-proxy disabled
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

다음은 **show service-policy** 명령의 샘플 출력으로, ASA CX 정책과 현재 통계는 물론 인증 프록시가 활성화되었을 때의 모듈 상태도 보여줍니다. 이 경우 proxied 카운터도 증가합니다.

```
hostname# show service-policy cxsc
Global policy:
  Service-policy: pmap
    Class-map: class-default
      Default Queueing      Set connection policy: random-sequence-number disable
        drop 0
      CXSC: card status Up, mode fail-open, auth-proxy enabled
        packet input 7724, packet output 7701, drop 0, reset-drop 0, proxied 10
```

모듈 연결 모니터링

ASA CX 모듈을 통한 연결을 표시하려면 다음 명령 중 하나를 입력합니다.

- **show asp table classify domain cxsc**

  ASA CX 모듈로 트래픽을 전송하기 위해 만든 NP 규칙을 표시합니다.

- **show asp table classify domain cxsc-auth-proxy**

  ASA CX 모듈용 인증 프록시를 위해 만든 NP 규칙을 표시합니다. 하나의 규칙을 표시하는 다음 샘플 출력에서 목적지 "port=2000"은 **cxsc auth-proxy port 2000** 명령으로 구성된 auth-proxy 포트이고 목적지 "ip/id=192.168.0.100"은 ASA 인터페이스 IP 주소입니다.

```
hostname# show asp table classify domain cxsc-auth-proxy
Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

- **show asp drop**

  삭제된 패킷을 표시합니다. 패킷 유형에 대한 설명은 아래와 같습니다.

- **show asp event dp-cp cxsc-msg**

  이 출력은 dp-cp 큐에 있는 ASA CX 모듈 메시지의 수를 보여줍니다. ASA CX 모듈에서 온 VPN 쿼리만 dp-cp로 전송됩니다.

- **show conn**

  'X - inspected by service module' 플래그를 표시하여 연결이 모듈로 전달되는지를 보여줍니다.

show asp drop 명령은 ASA CX 모듈과 관련된 다음과 같은 삭제 이유를 포함할 수 있습니다.

프레임 삭제:

- cxsc-bad-tlv-received - ASA가 Policy ID TLV 없이 CXSC에서 패킷을 수신할 때 발생합니다. 작업 필드에 Standby Active 비트가 설정되지 않은 경우 이 TLV는 비 제어 패킷에 있어야 합니다.
- cxsc-request - CXSC에 대한 정책 때문에 CXSC에서 프레임 삭제를 요청했습니다. CXSC는 작업을 Deny Source, Deny Destination 또는 Deny Pkt로 설정할 수 있습니다.
- cxsc-fail-close - 카드가 작동되지 않고 구성된 정책이 'fail-close'(카드가 비작동 상태여도 패킷 통과를 허용하는 'fail-open'이 아니라)이므로 패킷이 삭제됩니다.
- cxsc-fail - 기존 흐름에 대해 CXSC 컨피그레이션이 제거되었고 CXSC를 통해 기존 흐름을 처리할 수 없으므로 삭제됩니다. 이 상황은 발생할 가능성이 매우 낮습니다.
- cxsc-malformed-packet - CXSC의 패킷에 잘못된 헤더가 포함되어 있습니다. 예를 들면 헤더 길이가 정확하지 않을 수 있습니다.

흐름 삭제:

- cxsc-request - CXSC에서 흐름 종료를 요청했습니다. 작업 비트 0이 설정됩니다.
- reset-by-cxsc - CXSC에서 흐름 종료 및 재설정을 요청했습니다. 작업 비트 1이 설정됩니다.
- cxsc-fail-close - 카드가 작동하지 않으며 구성된 정책이 'fail-close'이므로 흐름이 종료되었습니다.

인증 프록시 관련 문제 해결

인증 프록시 기능 사용에 문제가 있는 경우 다음 단계를 수행하여 컨피그레이션 및 연결 문제를 해결하십시오.

참고 두 개의 ASA 인터페이스에 있는 호스트가 연결되어 있는데 ASA CX 서비스 정책이 그중 하나에 대해서만 구성되어 있으면 비 ASA CX 인터페이스에서 시작된 트래픽을 포함하여 두 호스트 간 모든 트래픽이 ASA CX 모듈로 전송됩니다(이 기능은 양방향임). 그러나 ASA는 서비스 정책이 적용된 인터페이스에서만 인증 프록시를 수행합니다. 이 기능은 인그레스(ingress) 전용이기 때문입니다.

절차

1단계 컨피그레이션을 확인합니다.

- ASA에서 **show asp table classify domain cxsc-auth-proxy** 명령의 출력을 검토하고 설치된 규칙이 있는지, 그러한 규칙이 정확한지를 확인합니다.
- PRSM에서 디렉토리 영역이 올바른 자격 증명으로 생성되었는지를 확인하고 연결을 테스트하여 인증 서버에 도달할 수 있는지를 확인합니다. 또한 정책 객체가 인증에 맞게 구성되었는지도 확인합니다.

2단계 **show service-policy cxsc** 명령의 출력을 검토하여 프록시 처리된 패킷이 있는지 확인합니다.

3단계 백플레인에서 패킷 캡처를 수행하고(**capture** *name* **interface asa_dataplane**), 트래픽이 올바르게 구성된 포트에서 리디렉션되는지 확인합니다. 구성된 포트를 점검하려면 **show running-config cxsc** 명령 또는 **show asp table classify domain cxsc-auth-proxy** 명령을 사용할 수 있습니다.

예

포트 2000이 일관성 있게 사용되는지 확인합니다.

1. 인증 프록시 포트를 점검합니다.

```
hostname# show running-config cxsc
cxsc auth-proxy port 2000
```

2. 인증 프록시 규칙을 점검합니다.

```
hostname# show asp table classify domain cxsc-auth-proxy

Input Table
in  id=0x7ffed86cc470, priority=121, domain=cxsc-auth-proxy, deny=false
    hits=0, user_data=0x7ffed86ca220, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=192.168.0.100, mask=255.255.255.255, port=2000, dscp=0x0
    input_ifc=inside, output_ifc=identity
```

3. 패킷 캡처에서 리디렉션 요청은 목적지 포트 2000으로 이동해야 합니다.

ASA CX 모듈의 예

다음 예는 모든 HTTP 트래픽을 ASA CX 모듈로 전환하고, 어떤 이유로든 ASA CX 모듈 카드가 실패하면 모든 HTTP 트래픽을 차단합니다.

```
hostname(config)# access-list ASACX permit tcp any any eq port 80
hostname(config)# class-map my-cx-class
hostname(config-cmap)# match access-list ASACX
hostname(config-cmap)# policy-map my-cx-policy
hostname(config-pmap)# class my-cx-class
hostname(config-pmap-c)# cxsc fail-close auth-proxy
hostname(config-pmap-c)# service-policy my-cx-policy global
```

다음 예는 10.1.1.0 및 10.2.1.0 네트워크로 향하는 모든 IP 트래픽을 ASA CX 모듈로 전환하고, 어떤 이유로든 ASA CX 모듈이 실패하면 모든 트래픽을 허용합니다.

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

ASA CX 모듈의 기록

기능 이름	플랫폼 릴리스	설명
SSP-10 및 -20의 ASA 5585-X에서 ASA CX SSP-10 및 -20 지원	ASA 8.4(4.1) ASA CX 9.0(1)	ASA CX 모듈을 사용하면 상황의 완전한 컨텍스트를 기반으로 보안을 적용할 수 있습니다. 이 컨텍스트에는 사용자의 신원(누가), 사용자가 액세스하려는 애플리케이션 또는 웹사이트(무엇을), 액세스 시도의 근원지(어디), 시도된 액세스 시간(언제) 및 액세스에 사용된 디바이스의 속성(어떻게)이 포함됩니다. ASA CX 모듈을 사용하면 흐름의 완전한 컨텍스트를 파악하여 세부적인 정책을 적용할 수 있습니다. 예를 들어 Facebook에 대한 액세스는 허용하되 Facebook의 게임에 대한 액세스는 거부하거나, 재무 관련 직원의 회사 기밀 데이터베이스에 대한 액세스는 허용하되 다른 직원의 액세스는 거부할 수 있습니다. 추가 및 수정된 명령: **capture**, **cxsc**, **cxsc auth-proxy**, **debug cxsc**, **hw-module module password-reset**, **hw-module module reload**, **hw-module module reset**, **hw-module module shutdown**, **session do setup host ip, session do get-config, session do password-reset, show asp table classify domain cxsc**, **show asp table classify domain cxsc-auth-proxy**, **show capture**, **show conn**, **show module**, **show service-policy**.

기능 이름	플랫폼 릴리스	설명
ASA 5512-X~ASA 5555-X 에서 ASA CX SSP 지원	ASA 9.1(1) ASA CX 9.1(1)	ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X 및 ASA 5555-X에 대해 ASA CX SSP 소프트웨어 모듈 지원을 추가했습니다. 수정된 명령: **session cxsc**, **show module cxsc**, **sw-module cxsc**.
데모용 모니터 전용 모드	ASA 9.1(2) ASA CX 9.1(2)	데모용인 경우에만 서비스 정책에 대해 모니터 전용 모드를 활성화할 수 있습니다. 이 경우 트래픽의 복사본이 ASA CX 모듈로 전달되고 원래 트래픽은 영향을 받지 않습니다. 또 다른 데모용 옵션은 모니터 전용 모드에서 서비스 정책 대신 트래픽 포워딩 인터페이스를 구성하는 것입니다. 트래픽 포워딩 인터페이스는 ASA를 우회하여 모든 트래픽을 ASA CX 모듈로 직접 전송합니다. 수정 또는 추가된 명령: **cxsc** {**fail-close** | **fail-open**} **monitor-only**, **traffic-forward cxsc monitor-only**.
ASA CX 모듈에서 NAT 64 지원	ASA 9.1(2) ASA CX 9.1(2)	이제 NAT 64를 ASA CX 모듈과 함께 사용할 수 있습니다. 수정된 명령이 없습니다.
SSP-40 및 -60의 ASA 5585-X에서 ASA CX SSP-40 및 -60 지원	ASA 9.1(3) ASA CX 9.2(1)	ASA CX SSP-40 및 -60 모듈을 일치하는 수준의 SSP-40 및 -60의 ASA 5585-X와 함께 사용할 수 있습니다. 수정된 명령이 없습니다.
ASA CX 모듈에서 다중 컨텍스트 모드 지원	ASA 9.1(3) ASA CX 9.2(1)	이제 ASA에서 컨텍스트 단위로 ASA CX 서비스 정책을 구성할 수 있습니다. **참고** 컨텍스트 단위로 ASA 서비스 정책을 구성할 수 있지만 ASA CX 모듈 자체(PRSM에서 구성)는 단일 컨텍스트 모드 디바이스입니다. ASA에서 오는 컨텍스트별 트래픽은 공통된 ASA CX 정책을 기준으로 점검을 거치게 됩니다. 수정된 명령이 없습니다.

기능 이름	플랫폼 릴리스	설명
ASA CX 백플레인에서 캡처된 패킷 필터링	ASA 9.1(3) ASA CX 9.2(1)	이제 **match** 또는 **access-list** 키워드와 함께 **capture interface asa_dataplane** 명령을 사용하여 ASA CX 백플레인에서 캡처된 패킷을 필터링할 수 있습니다. ASA CX 모듈 관련 제어 트래픽은 access-list 또는 match 필터링의 영향을 받지 않습니다. ASA는 모든 제어 트래픽을 캡처합니다. 다중 컨텍스트 모드에서 컨텍스트 단위로 패킷 캡처를 구성합니다. 다중 컨텍스트 모드의 모든 제어 트래픽은 시스템 실행 공간으로만 이동합니다. 제어 트래픽은 access-list 또는 match를 사용하여 필터링할 수 없으므로 시스템 실행 공간에서는 이러한 옵션을 사용할 수 없습니다. 수정된 명령: **capture interface asa_dataplane**.

ASA IPS 모듈

이 장에서는 ASA IPS 모듈의 구성 방법에 대해 설명합니다. ASA IPS 모듈은 ASA 모델에 따라 하드웨어 모듈일 수도 있고 소프트웨어 모듈일 수도 있습니다. ASA 모델에 대해 지원되는 ASA IPS 모듈의 리스트는 *Cisco ASA Compatibility Matrix*를 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

ASA IPS 모듈에 대한 정보

ASA IPS 모듈은 완전한 기능을 갖춘 사전 대응형 침입 방지 서비스를 제공하여 웜과 네트워크 바이러스 등 악성 트래픽이 네트워크에 영향을 미치기 전에 차단하는 고급 IPS 소프트웨어를 실행합니다.

ASA IPS 모듈이 ASA에서 작동하는 방식

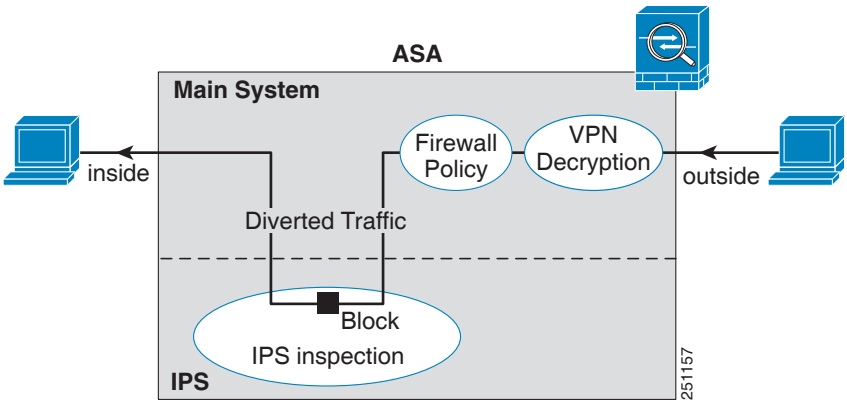
ASA IPS 모듈은 ASA에서 별도의 애플리케이션을 실행합니다. ASA IPS 모듈에는 외부 관리 인터페이스가 포함되어 있으므로, 이를 통해 ASA IPS 모듈에 직접 연결할 수 있습니다. 관리 인터페이스가 없는 경우 ASA 인터페이스를 통해 ASA IPS 모듈에 연결할 수 있습니다. ASA 5585-X의 ASA IPS SSP에는 ASA에 대한 추가적인 포트 밀도를 제공하는 데이터 인터페이스가 포함되어 있습니다. 그러나 ASA의 전체적인 처리량은 증가하지 않습니다.

트래픽은 ASA IPS 모듈로 전달되기 전에 방화벽 점검을 거치게 됩니다. ASA에서 IPS 검사를 통해 트래픽을 식별할 경우, ASA 및 ASA IPS 모듈에서 트래픽이 다음과 같이 흐릅니다. **참고**: 이 예는 "인라인 모드"에 대한 것입니다. "프로미스큐어스(promiscuous) 모드"에 대한 정보는 19-3 페이지의 운영 모드를 참조하십시오. 프로미스큐어스 모드에서는 ASA가 ASA IPS 모듈에 트래픽의 복사본만 전송합니다.

1. 트래픽이 ASA로 들어갑니다.
2. 들어오는 VPN 트래픽이 암호 해독됩니다.
3. 방화벽 정책이 적용됩니다.
4. 트래픽이 ASA IPS 모듈로 전송됩니다.
5. ASA IPS 모듈이 보안 정책을 트래픽에 적용하고 적절한 작업을 수행합니다.
6. 유효한 트래픽은 ASA로 다시 전송됩니다. ASA IPS 모듈은 자체 보안 정책에 따라 일부 트래픽을 차단할 수 있으며, 그러한 트래픽은 전달되지 않습니다.
7. 나가는 VPN 트래픽이 암호화됩니다.
8. 트래픽이 ASA를 빠져나갑니다.

그림 19-1은 인라인 모드에서 ASA IPS 모듈을 실행할 때의 트래픽 흐름을 보여줍니다. 이 예에서 ASA IPS 모듈은 공격으로 식별되는 트래픽을 자동으로 차단합니다. 다른 모든 트래픽은 ASA를 통해 전달됩니다.

그림 19-1 ASA에서 ASA IPS 모듈 트래픽 흐름: 인라인 모드

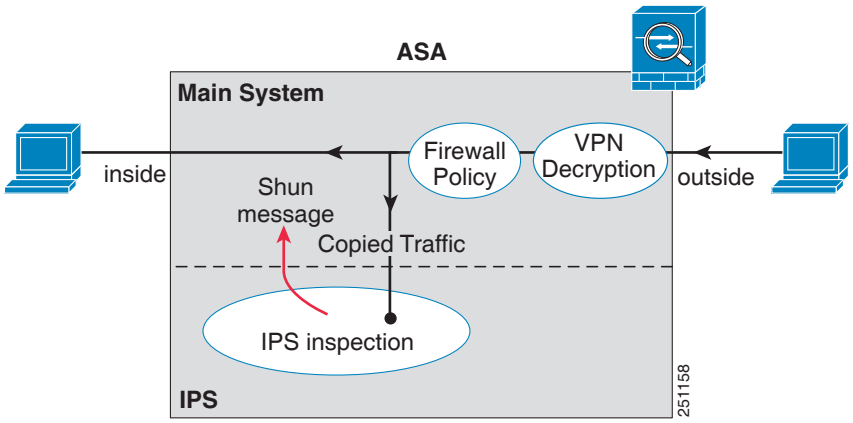


운영 모드

다음 모드 중 하나를 사용하여 ASA IPS 모듈에 트래픽을 전송할 수 있습니다.

- 인라인(inline) 모드 - 이 모드는 ASA IPS 모듈을 트래픽 흐름에 직접 배치합니다(그림 19-1 참조). IPS 검사를 위해 분류된 트래픽은 ASA IPS 모듈에서 먼저 검사를 통과하지 않으면 ASA로 계속 나아갈 수 없습니다. 검사를 위해 분류된 모든 패킷은 분석을 거친 후 통과가 허용되므로 이 모드가 가장 안전합니다. 또한 ASA IPS 모듈은 패킷 단위로 차단 정책을 구현할 수 있습니다. 그러나 이 모드는 처리량에 영향을 미칠 수 있습니다.
- 프로미스큐어스(promiscuous) 모드 - 이 모드는 트래픽의 복제 스트림을 ASA IPS 모듈로 전송합니다. 이 모드는 덜 안전하지만 트래픽 처리량에 거의 영향을 미치지 않습니다. 인라인 모드와는 달리 프로미스큐어스 모드에서는 ASA IPS 모듈이 트래픽을 차단하려면 ASA에 트래픽을 차단하도록 지시하거나 ASA에서 연결을 재설정해야 합니다. 또한 ASA IPS 모듈이 트래픽을 분석하는 동안 소량의 트래픽은 ASA IPS 모듈이 차단하기 전에 ASA를 통과할 수도 있습니다. 그림 19-2는 프로미스큐어스 모드의 ASA IPS 모듈을 보여줍니다. 이 예에서 ASA IPS 모듈은 위협으로 식별한 트래픽에 대한 차단 메시지를 ASA에 전송합니다.

그림 19-2 ASA의 ASA IPS 모듈 트래픽 흐름: 프로미스큐어스 모드



가상 센서 사용

IPS 소프트웨어 버전 6.0 이상을 실행하는 ASA IPS 모듈은 여러 가상 센서를 실행할 수 있는데, 이는 ASA IPS 모듈에서 여러 보안 정책을 구성할 수 있음을 의미합니다. 각 ASA 보안 컨텍스트 또는 단일 모드 ASA를 하나 이상의 가상 센서에 할당할 수도 있고, 동일한 가상 센서에 여러 보안 컨텍스트를 할당할 수도 있습니다. 지원되는 최대 센서 수를 포함하여 가상 센서에 대한 자세한 내용은 IPS 설명서를 참조하십시오.

그림 19-3은 하나의 가상 컨텍스트가 하나의 가상 센서와 쌍을 이룬 경우(인라인 모드) 및 두 개의 가상 컨텍스트가 동일한 가상 센서를 공유하는 경우를 보여줍니다.

그림 19-3 보안 컨텍스트 및 가상 센서

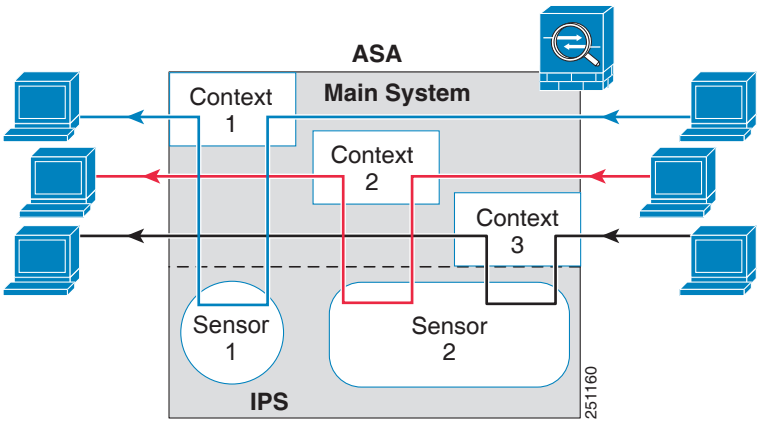
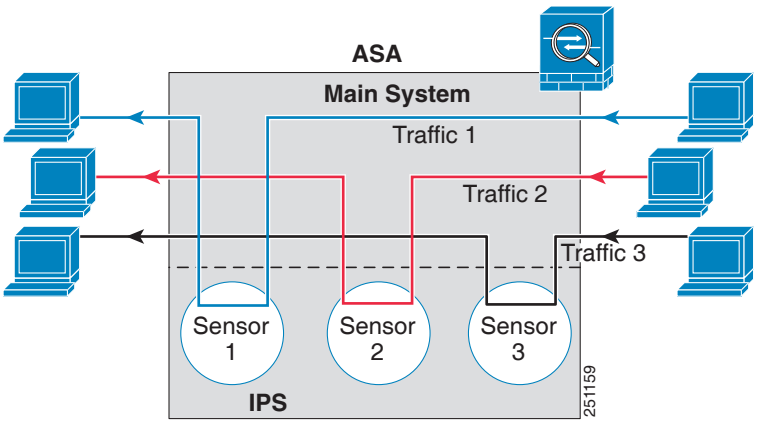


그림 19-4는 단일 모드 ASA가 여러 가상 센서와 쌍을 이룬 경우를 보여줍니다(인라인 모드). 정의된 각 트래픽 흐름은 각기 다른 센서로 이동합니다.

그림 19-4 여러 가상 센서가 있는ASA 단일 모드



관리 액세스에 대한 정보

다음 방법을 사용하여 IPS 애플리케이션을 관리할 수 있습니다.

- ASA에서 모듈에 대한 세션 시작 - ASA에 CLI 액세스가 가능한 경우 모듈에 대한 세션을 시작하고 모듈 CLI에 액세스할 수 있습니다. 19-10 페이지의 ASA에서 모듈에 대한 세션 시작 섹션을 참조하십시오.
- ASDM 또는 SSH를 사용하여 IPS 관리 인터페이스에 연결 - ASA에서 ASDM을 실행하면 IPS 애플리케이션을 구성할 수 있도록 관리 스테이션이 모듈 관리 인터페이스에 연결됩니다. SSH의 경우 모듈 관리 인터페이스에서 모듈 CLI에 직접 액세스할 수 있습니다. (텔넷 액세스의 경우 모듈 애플리케이션에서 추가 컨피그레이션이 필요합니다). 모듈 관리 인터페이스는 syslog 메시지를 전송하거나 모듈 애플리케이션의 업데이트(예: 시그니처 데이터베이스 업데이트)를 허용하는 데에도 사용할 수 있습니다.

관리 인터페이스에 대한 다음 정보를 참조하십시오.

- ASA 5585-X - IPS 관리 인터페이스는 별도의 외부 기가비트 이더넷 인터페이스입니다.
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X - 이러한 모델은 ASA IPS 모듈을 소프트웨어 모듈로 실행합니다. IPS 관리 인터페이스는 Management 0/0 인터페이스를 ASA와 공유합니다. ASA 및 ASA IPS 모듈에 대해 별도의 MAC 주소와 IP 주소가 지원됩니다. IPS 운영 체제 내에서 IPS IP 주소를 컨피그레이션해야 합니다(CLI 또는 ASDM 사용). 그러나 물리적 특성(예: 인터페이스 활성화)은 ASA에서 구성됩니다. 이 인터페이스를 IPS 전용 인터페이스로 지정하려면 ASA 인터페이스 컨피그레이션(특히 인터페이스 이름)을 제거할 수 있습니다. 이 인터페이스는 관리 전용입니다.

ASA IPS 모듈의 라이센싱 요구 사항

다음 표에서는 이 기능의 라이센싱 요구 사항을 보여줍니다.

모델	라이센스 요구 사항
ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	IPS 모듈 라이센스. **참고** IPS 모듈 라이센스를 사용하면 ASA에서 IPS 소프트웨어 모듈을 실행할 수 있습니다. IPS 시그니처 서브스크립션도 별도로 구매해야 합니다. 장애 조치의 경우 유닛당 서브스크립션을 구매해야 합니다. IPS 시그니처 지원을 받으려면 IPS가 미리 설치된 ASA를 구매해야 합니다(부품 번호에 "IPS" 포함됨). 결합된 장애 조치 클러스터 라이센스에서는 비 IPS 유닛과 IPS 유닛을 페어링할 수 없습니다. 예를 들어ASA 5515-X의 IPS 버전(부품 번호 ASA5515-IPS-K9)을 구매하고 비 IPS 버전(부품 번호 ASA5515-K9)과 장애 조치 페어링을 시도하면, 다른 유닛에서 IPS 모듈 라이센스를 상속받았더라도 ASA5515-K9 유닛에 대해 IPS 시그니처 업데이트를 얻을 수 없습니다.
ASA 5585-X	기본 라이센스
모든 다른 모델	지원되지 않음.

지침 및 제한

이 섹션에서는 이 기능의 지침 및 제한에 대해 소개합니다.

모델 지침

- 어떤 모델이 어떤 모듈을 지원하는가에 대한 자세한 내용은 *Cisco ASA Compatibility Matrix*를 참조하십시오.

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

추가 지침

- ASA 및 IPS 모듈의 총 처리량은 ASA의 단독 처리량보다 낮습니다.
  - ASA 5512-X~ASA 5555-X - http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-700608.html 참조
  - ASA 5585-X - http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-617018.html 참조

- 모듈에 설치된 소프트웨어 유형을 변경할 수 없습니다. ASA IPS 모듈을 구매하는 경우 나중에 다른 소프트웨어를 설치할 수 없습니다.

기본 설정

표 19-1에는 ASA IPS 모듈에 대한 기본 설정이 나열됩니다.

표 19-1 기본 네트워크 매개변수

매개변수	기본값
관리 IP 주소	192.168.1.2/24
게이트웨이	192.168.1.1/24(기본 ASA 관리 IP 주소)
아이디	cisco
비밀번호	cisco

참고 ASA의 기본 관리 IP 주소는 192.168.1.1/24입니다.

ASA IPS 모듈 구성

이 섹션에서는 ASA IPS 모듈의 구성 방법에 대해 설명합니다.

- 19-6 페이지의 ASA IPS 모듈의 작업 흐름
- 19-7 페이지의 ASA IPS 관리 인터페이스 연결
- 19-10 페이지의 ASA에서 모듈에 대한 세션 시작
- 19-12 페이지의 기본 IPS 모듈 네트워크 설정 구성
- 19-11 페이지의 (ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 부팅
- 19-12 페이지의 ASA IPS 모듈에서 보안 정책 구성
- 19-13 페이지의 보안 컨텍스트에 가상 센서 할당
- 19-15 페이지의 ASA IPS 모듈로 트래픽 전환

ASA IPS 모듈의 작업 흐름

ASA IPS 모듈 컨피그레이션은 ASA IPS 모듈에서 IPS 보안 정책을 컨피그레이션하고 ASA IPS 모듈에 트래픽을 전송하도록 ASA를 구성하는 프로세스입니다. ASA IPS 모듈을 구성하려면 다음 단계를 수행하십시오.

1단계 ASA IPS 관리 인터페이스를 연결합니다. 19-7 페이지의 ASA IPS 관리 인터페이스 연결 섹션을 참조하십시오.

2단계 모듈에 대한 세션을 시작합니다. 백플레인을 통해 IPS CLI에 액세스합니다.19-10 페이지의 ASA에서 모듈에 대한 세션 시작 섹션을 참조하십시오.

3단계 (ASA 5512-X~ASA 5555-X, 필요할 수 있음) 소프트웨어 모듈을 설치합니다. 19-11 페이지의 (ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 부팅 섹션을 참조하십시오.

4단계 ASAIPS 모듈에 대한 기본 네트워크 설정을 구성합니다. 19-12 페이지의 기본 IPS 모듈 네트워크 설정 구성 섹션을 참조하십시오.

5단계 모듈에서 검사 및 보호 정책을 구성합니다. 이러한 정책에서는 트래픽을 어떻게 검사할지, 침입이 탐지되었을 때 무엇을 할지 등을 결정합니다. 19-12 페이지의 ASA IPS 모듈에서 보안 정책 구성 섹션을 참조하십시오.

6단계 (선택 사항) ASA의 다중 컨텍스트 모드에서 각 컨텍스트에 대해 사용할 수 있는 IPS 가상 센서를 지정합니다(가상 센서를 구성한 경우). 19-13 페이지의 보안 컨텍스트에 가상 센서 할당 섹션을 참조하십시오.

7단계 ASA에서 ASA IPS 모듈로 전환할 트래픽을 식별합니다. 19-15 페이지의 ASA IPS 모듈로 트래픽 전환 섹션을 참조하십시오.

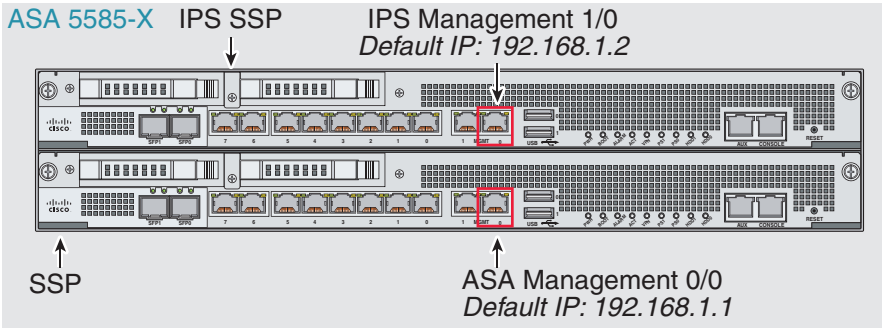
ASA IPS 관리 인터페이스 연결

IPS 관리 인터페이스는 IPS 모듈에 대한 관리 액세스를 제공하는 것 외에도 글로벌 상관관계, 시그니처 업데이트 및 라이센스 요청 등을 다운로드할 수 있도록 HTTP 프록시 서버 또는 DNS 서버와 인터넷에 액세스해야 합니다. 이 섹션에서는 권장 네트워크 컨피그레이션에 대해 설명합니다. 네트워크는 환경에 따라 다를 수 있습니다.

- 19-7 페이지의 ASA 5585-X(하드웨어 모듈)
- 19-8 페이지의 ASA 5512-X~ASA 5555-X(소프트웨어 모듈)

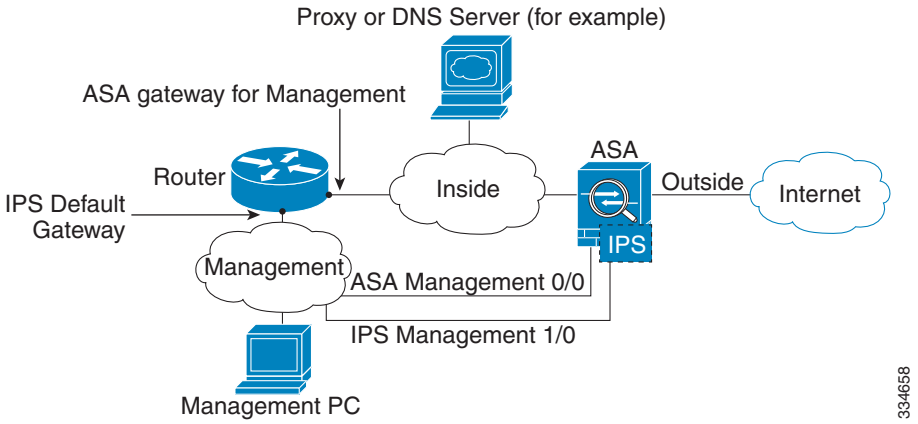
ASA 5585-X(하드웨어 모듈)

IPS 모듈에는 ASA에서 제공하는 별도의 관리 인터페이스가 포함되어 있습니다.



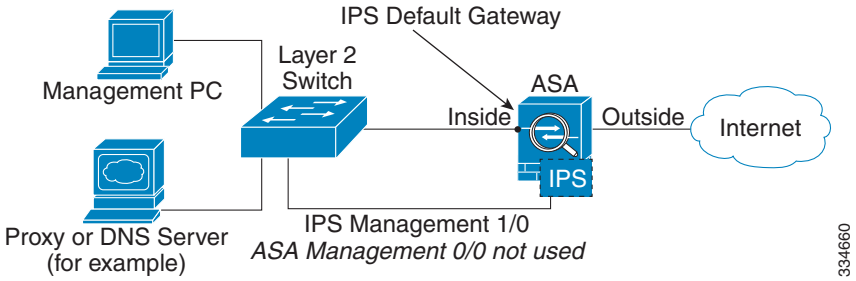
내부 라우터가 있는 경우

내부 라우터가 있으면 관리 네트워크(ASA Management 0/0 및 IPS Management 1/0 인터페이스를 모두 포함할 수 있음)와 ASA 내부 네트워크 간에 라우팅할 수 있습니다. 또한 내부 라우터를 통해 관리 네트워크에 도달하려면 ASA에서 경로를 추가해야 합니다.



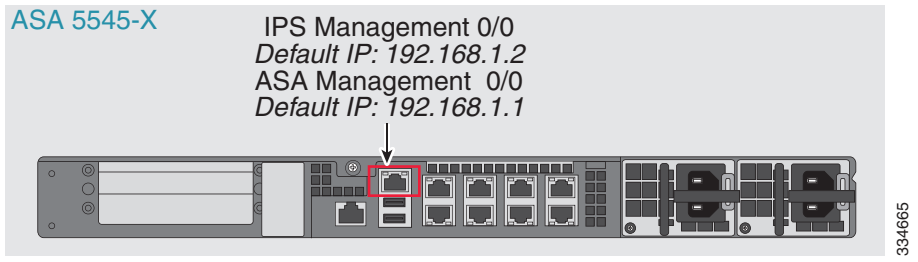
내부 라우터가 없는 경우

하나의 내부 네트워크만 있는 경우 별도의 관리 네트워크를 둘 수 없습니다. 네트워크 간 라우팅을 위해 내부 라우터가 필요하기 때문입니다. 이 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. IPS 모듈은 ASA와 분리된 디바이스이므로 내부 인터페이스와 동일한 네트워크에 오도록 IPS Management 1/0 주소를 구성할 수 있습니다.



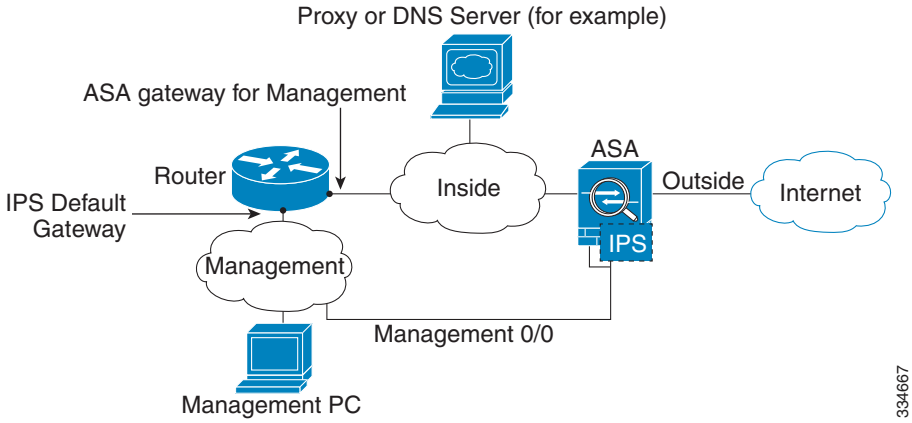
ASA 5512-X~ASA 5555-X(소프트웨어 모듈)

이러한 모듈은 IPS 모듈을 소프트웨어 모듈로서 실행하며, IPS 관리 인터페이스는 Management 0/0 인터페이스를 ASA와 공유합니다.



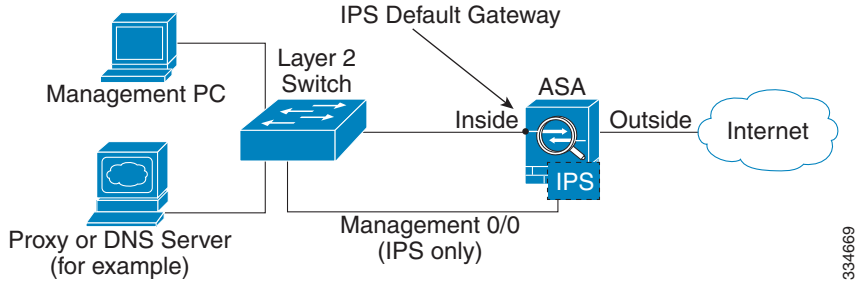
내부 라우터가 있는 경우

내부 라우터가 있으면 Management 0/0 네트워크(ASA 및 IPS IP 관리 IP 주소를 모두 포함)와 내부 네트워크 간에 라우팅할 수 있습니다. 또한 내부 라우터를 통해 관리 네트워크에 도달하려면 ASA에서 경로를 추가해야 합니다.



내부 라우터가 없는 경우

하나의 내부 네트워크만 있는 경우 별도의 관리 네트워크를 둘 수 없습니다. 이 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. ASA에서 구성한 이름을 Management 0/0 인터페이스에서 제거하더라도 해당 인터페이스에 대해 IPS IP 주소를 구성할 수 있습니다. IPS 모듈은 기본적으로 ASA와 분리된 디바이스이므로 내부 인터페이스와 동일한 네트워크에 오도록 IPS 관리 주소를 구성할 수 *있습니다.*



참고 ASA에서 구성한 이름을 Management 0/0에서 제거해야 합니다. ASA에서 구성한 경우 IPS 주소는 ASA와 동일한 네트워크에 있어야 합니다. 그러면 기타 ASA 인터페이스에서 이미 구성된 모든 네트워크가 제외됩니다. 이름이 구성되지 않은 경우 IPS 주소는 어떤 네트워크에든 둘 수 있습니다(예: ASA 내부 네트워크).

향후 작업

- 기본 네트워크 설정을 구성합니다. 19-12 페이지의 기본 IPS 모듈 네트워크 설정 구성 섹션을 참조하십시오.

ASA에서 모듈에 대한 세션 시작

ASA에서 IPS 모듈 CLI에 액세스하려면 ASA에서 세션을 시작할 수 있습니다. 소프트웨어 모듈의 경우 모듈에 대한 세션을 시작하거나(텔넷 사용) 가상 콘솔 세션을 만들 수 있습니다. 제어 평면이 다운되어 텔넷 세션을 설정할 수 없는 경우 콘솔 세션이 유용할 수 있습니다.

자세한 단계

명령	목적

텔넷 세션.
하드웨어 모듈(예: ASA 5585-X):
session 1
소프트웨어 모듈(예: ASA 5545-X):
session ips
 	
예:
`hostname# session 1`
 	
`Opening command session with slot 1.`
`Connected to slot 1. Escape character sequence is 'CTRL-^X'.`
 	
`sensor login: cisco`
`Password: cisco`
	텔넷을 사용하여 모듈에 액세스합니다. 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시됩니다. 기본 사용자 이름은 **cisco**이고 기본 비밀번호는 **cisco**입니다.
	참고 모듈에 처음 로그인하는 경우 기본 비밀번호를 변경하라는 프롬프트가 표시됩니다. 비밀번호는 최소 8자여야 하며 사전의 단어는 사용할 수 없습니다.

콘솔 세션(소프트웨어 모듈 전용).
session ips console
 	
예:
`hostname# session ips console`
 	
`Establishing console session with slot 1`
`Opening console session with module ips.`
`Connected to module ips. Escape character sequence is 'CTRL-SHIFT-6 then x'.`
 	
`sensor login: cisco`
`Password: cisco`
	모듈 콘솔에 액세스합니다. 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시됩니다. 기본 사용자 이름은 **cisco**이고 기본 비밀번호는 **cisco**입니다.
	참고 터미널 서버에서는 이 명령을 사용하지 마십시오. 여기서 **Ctrl-Shift-6, x**는 터미널 서버 프롬프트로 돌아가기 위한 이스케이프 시퀀스입니다. **Ctrl-Shift-6, x**는 IPS 콘솔을 이스케이프하고 ASA 프롬프트로 돌아가기 위한 시퀀스이기도 합니다. 그러므로 이 상황에서 IPS 콘솔을 종료하려고 시도하면 대신 종료 후 터미널 서버 프롬프트에 이르게 됩니다. 터미널 서버를 ASA에 다시 연결하면 IPS 콘솔 세션은 여전히 활성 상태이므로, 종료 후 ASA 프롬프트로 돌아갈 수 없습니다. 콘솔을 ASA 프롬프트로 되돌리려면 직접 직렬 연결을 사용해야 합니다.
	
	대신 **session ips** 명령을 사용합니다.

(ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 부팅

일반적으로 ASA는 Disk0에 IPS 모듈 소프트웨어가 포함된 상태로 제공됩니다. 모듈을 실행하고 있지 않거나 기존 ASA에 IPS 모듈을 추가하려는 경우 모듈 소프트웨어를 부팅해야 합니다. 모듈이 실행되고 있지 않으면 해당 모듈에 대한 세션을 시작할 수 없거나.

자세한 단계

1단계 다음 중 하나를 수행합니다.

- IPS가 사전 설치된 새로운 ASA - 플래시 메모리에서 IPS 모듈 소프트웨어 파일 이름을 보려면 다음을 입력하거나 **Tools > File Management**

  ```
  hostname# dir disk0:
  ```

  예를 들면 IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip와 같은 파일 이름을 찾아볼 수 있습니다. 파일 이름을 메모하십시오. 이 절차의 뒷부분에 이 파일 이름이 필요합니다.

- 새로운 IPS가 설치된 기존 ASA - Cisco.com에서 TFTP 서버나 IPS 소프트웨어를 다운로드합니다. Cisco.com 로그인이 있는 경우 다음 웹사이트에서 소프트웨어를 다운로드할 수 있습니다.

  http://www.cisco.com/cisco/software/navigator.html?mdfid=282164240

  ASA에 소프트웨어를 복사합니다.

  ```
  hostname# copy tftp://server/file_path disk0:/file_path
  ```

  기타 다운로드 서버 유형은 일반 운영 컨피그레이션 가이드를 참조하십시오.

  파일 이름을 메모하십시오. 이 절차의 뒷부분에 이 파일 이름이 필요합니다.

2단계 disk0에서 IPS 모듈 소프트웨어 위치를 설정하려면 다음 명령을 입력하고를 클릭합니다.

```
hostname# sw-module module ips recover configure image disk0:file_path
```

예를 들어 1단계 예제의 파일 이름을 사용하여 다음을 입력합니다.

```
hostname# sw-module module ips recover configure image
disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

3단계 IPS 모듈 소프트웨어를 설치 및 로드하려면 다음 명령을 입력하고를 클릭합니다.

```
hostname# sw-module module ips recover boot
```

4단계 이미지 전송 및 모듈 다시 시작 진행 상황을 확인하려면 다음 명령을 입력하고를 클릭합니다.

```
hostname# show module ips details
```

출력의 Status 필드는 모듈의 운영 상태를 나타냅니다. 정상적으로 운영되는 모듈은 "Up" 상태가 표시됩니다. ASA가 모듈에 애플리케이션 이미지를 전송하는 동안에는 출력의 Status 필드에 "Recover"가 표시됩니다. ASA가 이미지 전송을 완료하고 모듈을 다시 시작하면 새로 전송된 이미지가 실행됩니다.

기본 IPS 모듈 네트워크 설정 구성

모드에서는 ASA에서 모듈에 대한 세션을 시작하고 **setup** 명령을 사용하여 기본 설정을 구성합니다.

참고 (ASA 5512-X~ASA 5555-X) 모듈에 대한 세션을 시작할 수 없거나 IPS 모듈이 실행되고 있지 않은 것입니다. 19-11 페이지의 (ASA 5512-X~ASA 5555-X) 소프트웨어 모듈 부팅을 참조하고, 모듈을 설치한 후 이 절차를 반복하십시오.

자세한 단계

	명령	목적
1단계	19-10 페이지의 ASA에서 모듈에 대한 세션 시작에 따라 IPS 모듈에 대한 세션을 시작합니다.	
2단계	**setup** 예: `sensor# setup`	ASA IPS 모듈의 초기 컨피그레이션을 위한 설정 유틸리티를 실행합니다. 기본 설정을 위한 프롬프트가 표시됩니다. 기본 게이트웨이에는 업스트림 라우터의 IP 주소를 지정합니다. 네트워크 요구 사항을 알아보려면 19-7 페이지의 ASA IPS 관리 인터페이스 연결을 참조하십시오. ASA 관리 IP 주소의 기본 설정은 작동하지 않습니다.

ASA IPS 모듈에서 보안 정책 구성

이 섹션에서는 ASA IPS 모듈 애플리케이션의 구성 방법에 대해 설명합니다.

자세한 단계

1단계 다음 방법 중 하나를 사용하여 ASA IPS 모듈 CLI에 액세스합니다.

- ASA에서 ASA IPS 모듈에 대한 세션을 시작합니다. 19-10 페이지의 ASA에서 모듈에 대한 세션 시작 섹션을 참조하십시오.
- SSH를 사용하여 IPS 관리 인터페이스에 연결합니다. 변경하지 않은 경우 기본 관리 IP 주소는 192.168.1.2입니다. 기본 사용자 이름은 **cisco**이고 기본 비밀번호는 **cisco**입니다. 관리 인터페이스에 대한 자세한 내용은 19-4 페이지의 관리 액세스에 대한 정보를 참조하십시오.

2단계 IPS 설명서에 따라 IPS 보안 정책을 구성합니다.

IPS와 관련된 모든 문서에 액세스하려면 다음 페이지를 방문하십시오.
http://www.cisco.com/c/en/us/support/security/ips-4200-series-sensors/products-documentation-roadmaps-list.html

3단계 가상 센서를 구성하는 경우 센서 중 하나를 기본값으로 지정합니다. ASA의 컨피그레이션에 가상 센서 이름이 지정되지 않으면 기본 센서가 사용됩니다.

4단계 ASA IPS 모듈 구성을 완료했으면 다음 명령을 입력하여 IPS 소프트웨어를 종료합니다.

```
sensor# exit
```

ASA에서 ASA IPS에 대한 세션을 시작한 경우 ASA 프롬프트로 돌아가게 됩니다.

향후 작업

- 다중 컨텍스트 모드의 ASA에 대한 자세한 내용은 19-13 페이지의 보안 컨텍스트에 가상 센서 할당을 참조하십시오.
- 단일 컨텍스트 모드의 ASA에 대한 자세한 내용은 19-15 페이지의 ASA IPS 모듈로 트래픽 전환을 참조하십시오.

보안 컨텍스트에 가상 센서 할당

ASA가 다중 컨텍스트 모드에 있는 경우 하나 이상의 IPS 가상 센서를 각 컨텍스트에 할당할 수 있습니다. 그러면 ASA IPS 모듈로 트래픽을 전송하도록 컨텍스트를 구성할 때, 할당된 센서를 컨텍스트에 지정할 수 있습니다. 컨텍스트에 할당하지 않은 센서는 지정할 수 없습니다. 컨텍스트에 센서를 할당하지 않은 경우 ASA IPS 모듈에 대해 구성된 기본 센서가 사용됩니다. 여러 컨텍스트에 동일한 센서를 할당할 수 있습니다.

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

사전 요구 사항

컨텍스트 구성에 대한 자세한 내용은 일반 운영 컨피그레이션 가이드를 참조하십시오.

자세한 단계

	명령	목적

1단계	**context** *name*
	
	예:
	`hostname(config)# context admin`
	`hostname(config-ctx)#`
		구성할 컨텍스트를 식별합니다. 시스템 실행 공간에서 이 명령을 입력합니다.

	명령	목적
2단계	**allocate-ips** *sensor_name* [*mapped_name*] [**default**] 예: hostname(config-ctx)# allocate-ips sensor1 highsec	컨텍스트에 할당할 각 센서에 대해 이 명령을 입력합니다. *sensor_name* 인수는 ASA IPS 모듈에 구성된 센서 이름입니다. ASA IPS 모듈에 구성된 센서를 보려면 **allocate-ips ?**를 입력합니다. 사용 가능한 모든 센서가 나열됩니다. **show ips** 명령을 입력할 수도 있습니다. 시스템 실행 공간에서 **show ips** 명령을 실행하면 사용 가능한 모든 센서가 나열됩니다. 이 명령을 컨텍스트에서 입력할 경우 이미 컨텍스트에 할당된 센서가 표시됩니다. 아직 ASA IPS 모듈에 존재하지 않는 센서 이름을 지정하면 오류 메시지가 표시되지만 **allocate-ips** 명령은 있는 그대로 입력됩니다. ASA IPS 모듈에서 해당 이름의 센서를 만들 때까지 컨텍스트는 해당 센서가 다운 상태라고 간주합니다. 컨텍스트 내에서 실제 센서 이름 대신 센서 이름의 별칭을 사용하려면 *mapped_name* 인수를 사용합니다. 매핑된 이름을 지정하지 않으면 컨텍스트 내에서 센서 이름이 사용됩니다. 보안을 위해, 컨텍스트에서 어떤 센서가 사용되고 있는지를 컨텍스트 관리자에게 알리고 싶지 않을 수 있습니다. 또는 컨텍스트 컨피그레이션을 일반화하고자 할 수도 있습니다. 예를 들어, 모든 컨텍스트에서 "sensor1"과 "sensor2"라는 센서를 사용하도록 하려면 context A에서는 "highsec"과 "lowsec" 센서를 sensor1과 sensor2에 매핑하고, context B에서는 "medsec"과 "lowsec" 센서를 sensor1과 sensor2에 매핑할 수 있습니다. **default** 키워드는 컨텍스트당 하나의 센서를 기본 센서로 설정합니다. 컨텍스트 컨피그레이션에서 센서 이름을 지정하지 않으면 컨텍스트는 이 기본 센서를 사용합니다. 컨텍스트당 기본 센서를 하나만 구성할 수 있습니다. 기본 센서를 변경하려면 **no allocate-ips** *sensor_name* 명령을 입력하여 현재 센서를 제거한 후 새 기본 센서를 할당할 수 있습니다. 기본 센서를 지정하지 않고 컨텍스트 컨피그레이션에 센서 이름이 포함되어 있지 않으면, ASA IPS 모듈에서 지정한 기본 센서가 트래픽에 사용됩니다.
3단계	**changeto context** *context_name* 예: hostname# changeto context customer1 hostname/customer1#	19-15 페이지의 ASA IPS 모듈로 트래픽 전환에서 설명한 대로 IPS 보안 정책을 구성할 수 있도록 컨텍스트로 전환합니다.

예

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

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
```

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

hostname(config-ctx)# changeto context A
...
```

향후 작업

19-15 페이지의 ASA IPS 모듈로 트래픽 전환에서 설명한 대로 IPS 보안 정책을 구성할 수 있도록 각 컨텍스트로 전환합니다.

ASA IPS 모듈로 트래픽 전환

이 섹션에서는 ASA에서 ASA IPS 모듈로 전환되는 트래픽에 대해 설명합니다.

사전 요구 사항

다중 컨텍스트 모드의 각 컨텍스트 실행 공간에서 다음 단계를 수행합니다. 컨텍스트로 전환하려면 Configuration > Device List 창에 **changeto context** *context_name* 명령을.

자세한 단계

	명령	목적
1단계	**class-map** *name* 예: hostname(config)# class-map ips_class	ASA IPS 모듈로 전송할 트래픽을 식별하기 위한 클래스 맵을 만듭니다. 다중 트래픽 클래스를 ASA IPS 모듈로 전송하려면 보안 정책에서 사용할 다중 클래스 맵을 만들 수 있습니다.
2단계	**match** *parameter* 예: hostname(config-cmap)# match access-list ips_traffic	클래스 맵에서 트래픽을 지정합니다. 자세한 내용은 1-13 페이지의 트래픽 식별(Layer 3/4 클래스 맵) 섹션을 참조하십시오.
3단계	**policy-map** *name* 예: hostname(config)# policy-map ips_policy	클래스 맵 트래픽으로 사용할 작업을 설정하는 정책 맵을 추가하거나 편집합니다.

	명령	목적
4단계	**class** *name* 예: hostname(config-pmap)# class ips_class	1단계에서 생성한 클래스 맵을 식별합니다.
5단계	**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] 예: hostname(config-pmap-c)# ips promiscuous fail-close	트래픽을 ASA IPS 모듈로 전송해야 함을 지정합니다. **inline** 및 **promiscuous** 키워드는 ASA IPS 모듈의 운영 모드를 제어합니다. 자세한 내용은 19-3 페이지의 운영 모드를 참조하십시오. **fail-close** 키워드는 ASA IPS 모듈을 사용할 수 없는 경우 모든 트래픽을 차단하도록 ASA를 설정합니다. **fail-open** 키워드는 ASA IPS 모듈을 사용할 수 없는 경우 검사 없이 모든 트래픽을 허용하도록 ASA를 설정합니다. 가상 센서를 사용하려면 **sensor** *sensor_name* 인수를 사용하여 센서 이름을 지정할 수 있습니다. 사용 가능한 센서 이름을 보려면 **ips** {**inline**|**promiscuous**} {**fail-close**|**fail-open**} **sensor ?** 명령을 입력합니다. 사용 가능한 센서가 나열됩니다. **show ips** 명령을 사용할 수도 있습니다. ASA에서 다중 컨텍스트 모드를 사용하는 경우 컨텍스트에 할당한 센서만 지정할 수 있습니다(19-13 페이지의 보안 컨텍스트에 가상 센서 할당 참조). 컨텍스트에서 구성한 경우 *mapped_name*을 사용합니다. 센서 이름을 지정하지 않으면 기본 센서가 트래픽에 사용됩니다. 다중 컨텍스트 모드에서는 컨텍스트에 대한 기본 센서를 지정할 수 있습니다. 단일 모드인 경우 또는 다중 모드에서 기본 센서를 지정하지 않은 경우 ASA IPS 모듈에 설정된 기본 센서가 트래픽에 사용됩니다. 아직 ASA IPS 모듈에 존재하지 않는 이름을 입력하면 오류 메시지가 표시되고 명령이 거부됩니다.
6단계	(선택 사항) **class** *name2* 예: hostname(config-pmap)# class ips_class2	IPS 트래픽용 다중 클래스 맵을 만든 경우 정책에 대한 또 다른 클래스를 지정할 수 있습니다. 클래스의 순서가 정책 맵에서 어떤 의미를 갖는지를 자세히 알아보려면 1-5 페이지의 서비스 정책 내에서의 기능 일치를 참조하십시오. 트래픽은 동일한 작업 유형에 대해 둘 이상의 클래스 맵과 일치할 수 없습니다. 따라서 network A는 sensorA로 이동하고 다른 모든 트래픽은 sensorB로 이동하도록 지정하려면, network A에 대해 **class** 명령을 입력한 후 모든 트래픽에 대해 **class** 명령을 입력해야 합니다. 이렇게 하지 않으면 network A를 비롯한 모든 트래픽이 첫 번째 **class** 명령을 통해 일치가 확인된 후 sensorB로 전송됩니다.

	명령	목적
7단계	(선택 사항) **ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] 예: hostname(config-pmap-c)# ips promiscuous fail-close	트래픽의 두 번째 클래스를 ASA IPS 모듈로 전송해야 함을 지정합니다. 이 단계를 반복하여 필요한 만큼 클래스를 추가합니다.
8단계	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} 예: hostname(config)# service-policy tcp_bypass_policy outside	하나 이상의 인터페이스에서 정책 맵을 활성화합니다. **global**은 모든 인터페이스에서 정책 맵을 적용하고, **interface**는 하나의 인터페이스에 정책을 적용합니다. 글로벌 정책은 하나만 허용됩니다. 특정 인터페이스에 서비스 정책을 적용함으로써 해당 인터페이스에서 글로벌 정책을 재지정할 수 있습니다. 각 인터페이스에 정책 맵을 하나만 적용할 수 있습니다.

ASA IPS 모듈 관리

이 섹션에는 모듈 복구 또는 문제 해결에 도움이 되는 절차가 포함되어 있습니다.

- 19-17 페이지의 모듈에서 이미지 설치 및 부팅
- 19-19 페이지의 모듈 종료
- 19-19 페이지의 소프트웨어 모듈 이미지 제거
- 19-20 페이지의 비밀번호 재설정
- 19-20 페이지의 모듈 다시 로드 또는 재설정

모듈에서 이미지 설치 및 부팅

모듈이 실패하여 모듈 애플리케이션 이미지를 실행할 수 없으면 TFTP 서버(하드웨어 모듈의 경우) 또는 로컬 디스크(소프트웨어 모듈의 경우)에서 모듈에 새 이미지를 다시 설치할 수 있습니다.

참고 이미지를 설치하기 위해 모듈 소프트웨어 내에서 **upgrade** 명령을 사용하지 마십시오.

사전 요구 사항

- 하드웨어 모듈 - 지정한 TFTP 서버가 최대 60MB 크기의 파일을 전송할 수 있는지 확인합니다.

  참고 네트워크 및 이미지 크기에 따라 이 프로세스를 완료하는 데 약 15분 정도 걸릴 수 있습니다.

- 소프트웨어 모듈 - 이 절차를 완료하기 전에 이미지를 ASA 내부 플래시(disk0)에 복사합니다.

참고 IPS 소프트웨어를 disk0으로 다운로드하기 전에 여유 플래시 메모리가 50% 이상인지 확인합니다. IPS를 설치할 때 내부 플래시 메모리의 50%가 해당 파일 시스템에 예약됩니다.

자세한 단계

	명령	목적

1단계	하드웨어 모듈(예: ASA 5585-X):
	hw-module module 1 recover configure
	소프트웨어 모듈(예: ASA 5545-X):
	sw-module module ips recover configure image disk0:*file_path*
	예:
	`hostname# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		새 이미지의 위치를 지정합니다.
		하드웨어 모듈의 경우 - TFTP 서버의 URL, 관리 인터페이스 IP 주소 및 넷마스크, 게이트웨이 주소 등에 대한 프롬프트가 표시됩니다. 이러한 네트워크 매개변수는 ROMMON에서 구성합니다. 모듈 애플리케이션에서 구성한 네트워크 매개변수는 ROMMON에서 사용할 수 없으므로 여기서 별도로 설정해야 합니다.
		소프트웨어 모듈의 경우 - 로컬 디스크에 있는 이미지의 위치를 지정합니다.
		show module {1 | ips} recover 명령을 사용하여 복구 컨피그레이션을 볼 수 있습니다.
		다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 명령을 입력합니다.

2단계	하드웨어 모듈: **hw-module module 1 recover boot** 소프트웨어 모듈: **sw-module module ips recover boot** **예:** `hostname# hw-module module 1 recover boot`	IPS 모듈 소프트웨어를 설치 및 부팅합니다.
3단계	하드웨어 모듈: **show module 1 details** 소프트웨어 모듈: **show module ips details** **예:** `hostname# show module 1 details`	이미지 전송 및 모듈 다시 시작 프로세스의 진행 상황을 점검합니다. 출력의 Status 필드는 모듈의 운영 상태를 나타냅니다. 정상적으로 운영되는 모듈은 "Up" 상태가 표시됩니다. ASA가 모듈에 애플리케이션 이미지를 전송하는 동안에는 출력의 Status 필드에 "Recover"가 표시됩니다. ASA가 이미지 전송을 완료하고 모듈을 다시 시작하면 새로 전송된 이미지가 실행됩니다.

모듈 종료

모듈 소프트웨어를 종료하면 컨피그레이션 데이터를 잃지 않은 채 모듈의 전원을 안전하게 끌 수 있습니다. **참고**: ASA를 다시 로드하면 모듈이 자동으로 종료되지 않습니다. 따라서 ASA를 다시 로드하기 전에 모듈을 종료하는 것이 좋습니다. 모듈을 정상적으로 종료하려면 ASA CLI에서 다음 단계를 수행하십시오.

자세한 단계

명령	목적
하드웨어 모듈(예: ASA 5585-X): **hw-module module 1 shutdown** 소프트웨어 모듈(예: ASA 5545-X): **sw-module module ips shutdown** **예:** `hostname# hw-module module 1 shutdown`	모듈을 종료합니다.

소프트웨어 모듈 이미지 제거

소프트웨어 모듈 이미지 및 관련 컨피그레이션을 제거하려면 다음 단계를 수행하십시오.

자세한 단계

	명령	목적

1단계	**sw-module module ips uninstall**
	
	예:
	`hostname# sw-module module ips uninstall`
	`Module ips will be uninstalled. This will completely remove the`
	`disk image associated with the sw-module including any configuration`
	`that existed within it.`
	
	`Uninstall module <id>? [confirm]`
		소프트웨어 모듈 이미지 및 관련 컨피그레이션을 영구 제거합니다.

2단계	**reload** **예:** `hostname# reload`	ASA를 다시 로드합니다. 새 모듈 유형을 설치하려면 먼저 ASA를 다시 로드해야 합니다.

비밀번호 재설정

모듈 비밀번호를 기본값으로 재설정할 수 있습니다. 사용자 **cisco**에 대한 기본 비밀번호는 **cisco**입니다. 비밀번호를 재설정한 후 모듈 애플리케이션을 사용하여 고유한 값으로 변경해야 합니다.

모듈 비밀번호를 재설정하면 모듈이 재부팅됩니다. 모듈이 재부팅되는 동안에는 서비스를 사용할 수 없습니다.

모듈 비밀번호를 기본값 cisco로 재설정하려면 다음 단계를 수행하십시오.

자세한 단계

명령	목적
하드웨어 모듈(예: ASA 5585-X): **hw-module module 1 password-reset** 소프트웨어 모듈(예: ASA 5545-X): **sw-module module ips password-reset** **예:** `hostname# hw-module module 1 password-reset`	사용자 **cisco**에 대한 모듈 비밀번호를 **cisco**로 재설정합니다.

모듈 다시 로드 또는 재설정

모듈을 다시 로드 또는 재설정하려면 ASA CLI에서 다음 명령 중 하나를 입력합니다.

자세한 단계

명령	목적
하드웨어 모듈(예: ASA 5585-X): **hw-module module 1 reload** 소프트웨어 모듈(예: ASA 5545-X): **sw-module module ips reload** **예:** `hostname# hw-module module 1 reload`	모듈 소프트웨어를 다시 로드합니다.
하드웨어 모듈: **hw-module module 1 reset** 소프트웨어 모듈: **sw-module module ips reset** **예:** `hostname# hw-module module 1 reset`	재설정을 수행한 후 모듈을 다시 로드합니다.

ASA IPS 모듈 모니터링

모듈 상태를 확인하려면 다음 명령 중 하나를 입력합니다.

명령	목적
show module	상태를 표시합니다.
show module {**1** | **ips**} **details**	추가 상태 정보를 표시합니다. 하드웨어 모듈에는 **1**, 소프트웨어 모듈에는 **ips**를 지정합니다.
show module {**1** | **ips**} **recover**	이미지를 모듈로 전송하기 위한 네트워크 매개변수를 표시합니다. 하드웨어 모듈에는 **1**, 소프트웨어 모듈에는 **ips**를 지정합니다.

예

다음은 SSC가 설치된 ASA에 대한 추가 정보를 제공하는 **show module details** 명령을 실행한 샘플 출력입니다.

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Card-5
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc: Not Applicable
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

다음은 IPS SSP 소프트웨어 모듈이 설치된 ASA 5525-X에서 **show module ips** 명령을 실행한 샘플 출력입니다.

```
hostname# show module ips
Mod Card Type                                    Model           Serial No.
--- -------------------------------------------- ------------------------------
ips IPS 5525 Intrusion Protection System         IPS5525         FCH1504V03P

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
ips 503d.e59c.6f89 to 503d.e59c.6f89  N/A          N/A          7.1(1.160)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------------------------------------
ips IPS                            Up               7.1(1.160)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up
```

```
Mod License Name      License Status  Time Remaining
--- ----------------- --------------- ---------------
ips IPS Module        Enabled         7 days
```

ASA IPS 모듈의 컨피그레이션 예

다음 예는 프로미스큐어스(promiscuous) 모드에서 모든 IP 트래픽을 ASA IPS 모듈로 전환하고, 어떤 이유로든 ASA IPS 모듈 카드가 실패하면 모든 IP 트래픽을 차단합니다.

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

다음 예는 인라인 모드에서 10.1.1.0 및 10.2.1.0 네트워크로 향하는 모든 IP 트래픽을 AIP SSM으로 전환하고, 어떤 이유로든 AIP SSM이 실패하면 모든 트래픽을 허용합니다. my-ips-class 트래픽에는 sensor1이 사용되고 my-ips-class2 트래픽에는 sensor2가 사용됩니다.

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

ASA IPS 모듈의 기능 기록

표 19-2에는 각 기능 변경 사항 및 그것이 구현된 플랫폼 릴리스가 나열되어 있습니다.

표 19-2 ASA IPS 모듈의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
AIP SSM	7.0(1)	ASA 5510, 5520 및 5540에 대한 AIP SSM 지원을 추가했습니다. 추가된 명령: **ips**.
가상 센서(ASA 5510 이상)	8.0(2)	가상 센서 지원이 추가되었습니다. 가상 센서를 사용하면 ASA IPS 모듈에서 여러 보안 정책을 구성할 수 있습니다. 추가된 명령: **allocate-ips**.

표 19-2 ASA IPS 모듈의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
ASA 5505용 AIP SSC	8.2(1)	ASA 5505에 대한 AIP SSC 지원을 추가했습니다. 추가된 명령: **allow-ssc-mgmt**, **hw-module module ip** 및 **hw-module module allow-ip**.
ASA 5585-X에 대한 ASA IPS SSP-10, -20, -40 및 -60 지원	8.2(5)/ 8.4(2)	ASA 5585-X에 대한 ASA IPS SSP-10, -20, -40 및 -60 지원을 추가했습니다. ASA IPS SSP를 설치할 때 일치 수준 SSP를 하나만 사용할 수 있습니다(예: SSP-10과 ASA IPS SSP-10). **참고** ASA 5585-X는 버전 8.3에서 지원되지 않습니다.
SSP-40 및 SSP-60에 대한 Dual SSP 지원	8.4(2)	SSP-40 및 SSP-60의 경우 동일한 섀시에서 동일한 수준의 SSP 두 개를 사용할 수 있습니다. SSP을 수준을 혼합해서 사용할 수는 없습니다. 예를 들어 SSP-40과 SSP-60을 함께 사용하는 것은 지원되지 않습니다. 각 SSP는 별도의 컨피그레이션 및 관리와 함께 독립된 디바이스로서 작동합니다. 필요한 경우 두 개의 SSP를 장애 조치 쌍으로 사용할 수 있습니다. **참고** 섀시에서 두 개의 SSP를 사용하는 경우에는 VPN이 지원되지 않습니다. 그러나 VPN이 비활성화되지는 않았습니다. 수정된 명령: **show module**, **show inventory**, **show environment**.
ASA 5512-X~ASA 5555-X에 대한 ASA IPS SSP 지원	8.6(1)	ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X 및 ASA 5555-X에 대해 ASA IPS SSP 소프트웨어 모듈 지원을 추가했습니다. 추가 또는 수정된 명령: **session**, **show module**, **sw-module**.