플랫폼 설정

threat defense 디바이스의 플랫폼 설정은 값을 여러 디바이스 간에 공유하려고 할 수 있는 비 관련 기능을 구성합니다. 디바이스마다 다른 설정을 원한다고 해도 공유 정책을 생성하고 원하는 디바이스에 적용해야 합니다.

플랫폼 설정 소개

플랫폼 설정 정책은 시간 설정 및 외부 인증과 같이 구축의 다른 매니지드 디바이스와 유사할 가능성이 있는 매니지드 디바이스의 측면을 정의하는 기능 또는 파라미터의 공유 집합입니다.

공유 정책을 사용하면 여러 매니지드 디바이스를 한 번에 구성할 수 있으므로 구축 일관성을 유지하고 관리 작업을 간소화할 수 있습니다. 플랫폼 설정 정책을 변경하면 정책을 적용한 모든 매니지드

디바이스에 영향을 줍니다. 디바이스마다 다른 설정을 원한다고 해도 공유 정책을 생성하고 원하는 디바이스에 적용해야 합니다.

예를 들어, 조직의 보안 정책을 이용하려면 사용자가 로그인하는 경우 사용자 어플라이언스에 "무단 사용 금지" 메시지가 표시되어야 할 수 있습니다. 플랫폼 설정을 통해 플랫폼 설정 정책에서 로그인 배너를 한 번 설정할 수 있습니다.

또한 단일 management center의 플랫폼 설정 정책이 유용할 수도 있습니다. 예를 들어, 다양한 상황에서 사용하는 서로 다른 메일 릴레이 호스트가 있거나 다양한 액세스 목록을 테스트하려는 경우, 단일 정책을 수정하는 대신 여러 플랫폼 설정을 생성하여 전환할 수 있습니다.

플랫폼 설정 정책을 위한 요구 사항 및 사전 요건

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

네트워크 관리자

플랫폼 설정 정책 관리

플랫폼 설정 정책을 관리하려면 Platform Settings(플랫폼 설정) 페이지(**Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**)를 사용합니다. 이 페이지는 각 정책에 대한 디바이스 유형을 나타냅니다. Status(상태) 열에는 정책에 대한 장치 대상이 표시됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택합니다.

단계 **2** 기존 정책의 경우, **Copy(**복사**)** (), **Edit(**수정**)** () 또는 **Delete(**삭제**)** () 정책을 사용할 수 있습니다.

주의 대상 디바이스에 마지막으로 구축한 정책은 최신 상태가 아니더라도 삭제할 수 없습니다. 정책을 완전히 삭제하기 전에 다른 정책을 해당 대상에 구축하는 것이 좋습니다.

단계 **3** 새 정책을 생성하려면 **New Policy(**새 정책**)**를 클릭합니다.

a) 드롭다운 목록에서 디바이스 유형을 선택합니다.

- **Firepower Settings(Firepower** 설정**)**를 선택하여 매니지드 클래식 디바이스에 대한 공유 정책을 만듭니다.

- **Threat Defense Settings(Threat Defense** 설정**)**를 선택하여 threat defense 디바이스에 대한 공유 정책을 만듭니다.

b) 새 정책의 이름을 입력하고 선택적으로 설명을 입력합니다.
c) 선택적으로 정책을 적용할 **Available Devices(**사용 가능한 디바이스**)**를 선택하고 **Add to Policy(**정책에 추가**)**(또는 드래그 앤 드롭)를 클릭하여 선택한 디바이스를 추가합니다. **Search(**검색**)** 필드에 검색 문자열을 입력하여 디바이스 목록을 좁힐 수 있습니다.
d) **Save(**저장**)**를 클릭합니다.

시스템이 정책을 생성하고 편집을 위해 엽니다.

단계 **4** 정책의 대상 디바이스를 변경하려면 편집할 플랫폼 설정 정책 옆의 **Edit(**수정**)** ( )을 클릭합니다

a) **Policy Assignment(**정책 할당**)**를 클릭합니다.
b) 디바이스, 고가용성 쌍 또는 디바이스 그룹을 정책에 할당하려면 **Available Devices(**사용 가능한 디바이스**)** 목록에서 이를 선택하고 **Add to Policy(**정책에 추가**)**를 클릭합니다. 아니면 끌어서 놓을 수도 있습니다.
c) 디바이스 할당을 제거하려면 **Selected Devices(**선택한 디바이스**)** 목록의 디바이스, 고가용성 쌍 또는 디바이스 그룹 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.
d) **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

ARP 검사 설정

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 간에 허용됩니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다.

ARP 감시 기능은 악의적인 사용자가 다른 호스트 또는 라우터로 위장(ARP 스푸핑이라고도 함)하는 것을 방지합니다. ARP 스푸핑은 "끼어들기" 공격을 활성화할 수 있습니다. 예를 들어, 호스트에서 ARP 요청을 게이트웨이 라우터에 전송할 경우 해당 게이트웨이 라우터는 게이트웨이 라우터 MAC 주소에 응답합니다. 그러나 공격자는 라우터 MAC 주소가 아닌 공격자 MAC 주소가 포함된 다른 ARP 응답을 호스트에 전송합니다. 이제 공격자는 라우터에 트래픽이 전달되기 전에 모든 호스트 트래픽을 가로챌 수 있게 됩니다.

ARP 감시 기능은 고정 ARP 테이블에 올바른 MAC 주소와 관련 IP 주소를 입력하기만 하면 공격자가 공격자 MAC 주소가 포함된 ARP 응답을 보낼 수 없도록 합니다.

ARP 감시를 활성화할 경우 위협 방지 디바이스에서는 MAC 주소, IP 주소, 모든 ARP 패킷의 소스 인터페이스를 ARP 테이블의 고정 항목과 비교하고 다음과 같은 조치를 취합니다.

- IP 주소, MAC 주소, 소스 인터페이스가 ARP 항목과 일치하면 패킷이 통과됩니다.

- MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 위협 방지 디바이스에서는 패킷을 누락시킵니다.
- ARP 패킷이 고정 ARP 테이블의 어느 항목과도 일치하지 않으면 위협 방지 디바이스를 설정하여 패킷을 모든 인터페이스로 전달(플러딩)하거나 패킷이 누락되도록 합니다.

참고 전용 진단 인터페이스는 이 파라미터가 플러딩을 실행하도록 설정된 경우에도 패킷을 플러딩하지 않습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **ARP Inspection(ARP** 검사**)**을 선택합니다.

단계 **3** ARP 검사 테이블에 항목을 추가합니다.

a) **Add(**추가**)**를 클릭하여 새 항목을 만들거나 항목이 이미 있는 경우 **Edit(**편집**)**를 클릭합니다.

b) 원하는 옵션을 선택합니다.

- **Inspect Enabled(**검사 활성화**)** - 선택한 인터페이스 및 영역에서 ARP 검사를 수행할 수 있습니다.
- **Flood Enabled(**플러드 활성화**)** - 정적 ARP 항목과 일치하지 않는 ARP 요청이 원래 인터페이스 또는 전용 관리 인터페이스 이외의 모든 인터페이스로 플러딩될지 여부입니다. 이는 기본 동작입니다.

  ARP 요청을 플러딩하도록 선택하지 않으면 정적 ARP 항목과 정확히 일치하는 요청만 허용됩니다.
- **Security Zones(**보안 영역**)** - 선택한 작업을 수행하는 인터페이스를 포함하는 영역을 추가합니다. 영역은 전환된 영역이어야 합니다. 영역에 없는 인터페이스의 경우 선택한 Selected Security Zone(보안 영역 목록) 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** 고정 ARP 항목 추가에 따라 고정 ARP 항목을 추가합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

배너 설정

사용자가 장치 명령줄 인터페이스(CLI)에 연결할 때 이를 표시하도록 메시지를 구성할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Banner(**배너**)**를 선택합니다.

단계 **3** 배너를 구성합니다.

다음은 배너에 대한 몇 가지 팁과 요구 사항입니다.

- ASCII 문자만 허용됩니다. 줄바꿈(Enter를 누름)을 사용할 수 있지만 탭은 사용할 수 없습니다.
- 변수 **$(hostname)** 또는 **$(domain)**를 포함하여 디바이스의 호스트네임 또는 도메인 이름을 동적으로 추가할 수 있습니다.
- 배너에 대한 절대적인 길이 제한은 없지만 배너 메시지를 처리할 수 있는 시스템 메모리가 충분하지 않으면 텔넷 또는 SSH 세션이 닫힙니다.
- 보안의 관점에서는 배너에서 무단 액세스를 방지하는 것이 중요합니다. 침입자를 초대하는 것처럼 보이는 "환영" 또는 "부탁"에 해당하는 단어를 사용하지 마십시오. 다음 배너는 무단 액세스에 대해 올바른 톤을 설정합니다.

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

DNS 구성

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. 서로 다른 트래픽 유형에 적용되는 두 가지 DNS 서버 설정(데이터 및 특수 관리 트래픽)이 있습니다. 데이터 트래픽에는 액세스 제어 규칙 및 원격 액세스 VPN과 같이 DNS 조회가 필요한 FQDN을 사용하는 모든 서비스가 포함됩니다. 특수 관리 트래픽에는 구성 및 데이터베이스 업데이트와 같은 관리 인터페이스에서 발생하는 트래픽이 포함됩니다. 이 절차는 데이터 DNS 서버에만 적용됩니다. 관리 DNS 설정은 CLI **configure network dns servers** 및 **configure network dns searchdomains** 명령을 참조하십시오.

DNS 서버 통신에 대한 올바른 인터페이스를 결정하기 위해 매니지드디바이스는 라우팅 조회를 사용하지만, 사용되는 라우팅 테이블은 DNS를 활성화하는 인터페이스에 따라 다릅니다. 자세한 내용은 아래 인터페이스 설정을 참조하십시오.

선택적으로 여러 DNS 서버 그룹을 구성하고 이를 사용하여 서로 다른 DNS 도메인을 확인할 수 있습니다. 예를 들어 인터넷 연결에 사용하기 위해 공용 DNS 서버를 사용하는 범용 기본 그룹이 있을 수 있습니다. 그런 다음 내부 트래픽(예: example.com 도메인의 시스템에 대한 연결)에 내부 DNS 서버를 사용하도록 별도의 그룹을 구성할 수 있습니다. 따라서 조직의 도메인 이름을 사용하는 FQDN에 대한 연결은 내부 DNS 서버를 사용하여 확인되는 반면, 공용 서버에 대한 연결은 외부 DNS 서버를 사용합니다. 이러한 확인은 데이터 DNS 확인을 사용하는 모든 기능(예: NAT 및 액세스 제어 규칙)에서 사용됩니다.

Trusted DNS Servers(신뢰할 수 있는 DNS 서버) 탭을 사용하여 DNS 스누핑에 대해 신뢰할 수 있는 DNS 서비스를 구성할 수 있습니다. DNS 스누핑은 첫 번째 패킷에서 애플리케이션을 탐지하기 위해 애플리케이션 도메인을 IP에 매핑하는 데 사용됩니다. 신뢰할 수 있는 DNS 서버를 구성하는 것 외에도 DNS 그룹, DHCP 풀, DHCP 릴레이 및 DHCP 클라이언트에 이미 구성된 서버를 신뢰할 수 있는 DNS 서버로 포함할 수 있습니다.

참고 애플리케이션 기반 PBR의 경우 신뢰할 수 있는 DNS 서버를 구성해야 합니다. 또한 도메인을 확인하여 애플리케이션을 탐지할 수 있도록 DNS 트래픽이 일반 텍스트 형식(암호화된 DNS는 지원되지 않음)으로 threat defense를 통과하는지 확인해야 합니다.

시작하기 전에

- 하나 이상의 DNS 서버 그룹을 만들었는지 확인합니다. 자세한 내용은 DNS 서버 그룹 개체 생성을 참고하십시오.
- DNS 서버에 연결할 인터페이스 개체를 생성했는지 확인하십시오.
- 매니지드 디바이스에 DNS 서버에 액세스하기 위한 적절한 정적 또는 동적 경로가 있는지 확인합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Threat Defense 정책을 생성하거나 수정합니다.

단계 **2** **DNS**를 클릭합니다.

단계 **3** **DNS Settings(DNS** 설정**)** 탭을 클릭합니다.

단계 **4** **Enable DNS name resolution by device(**디바이스로 **DNS** 이름 확인 활성화**)**를 선택합니다.

단계 **5** DNS 서버 그룹을 구성합니다.

a) DNS 서버 그룹 목록에서 다음 중 하나를 수행합니다.

- 목록에 그룹을 추가하려면 **Add(**추가**)**를 클릭합니다. 기존 서버 그룹 목록 내에 30개의 필터 도메인이 구성되어 있으면 다른 그룹을 추가할 수 없습니다.

- 그룹에 대한 설정을 편집하려면 그룹 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.
- 그룹을 제거하려면 그룹 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다. 그룹을 제거해도 DNS 서버 그룹 개체는 삭제되지 않으며 단순히 이 목록에서 제거됩니다.

b) 그룹을 추가하거나 수정할 때 다음 설정을 구성하고 **OK(**확인**)**를 클릭합니다.

- **Select DNS Group(DNS** 그룹 선택**)** - 기존 DNS 서버 그룹 개체를 선택하거나 +를 클릭하여 새 개체를 만듭니다.
- **Make as default(**기본값으로 설정**)** - 이 그룹을 기본 그룹으로 설정하려면 이 옵션을 선택합니다. 다른 그룹의 필터와 일치하지 않는 모든 DNS 확인 요청은 이 그룹의 서버를 사용하여 확인됩니다.
- **Filter Domains(**도메인 필터링**)** - 기본 그룹이 아닌 그룹에만 해당하는 쉼표로 구분된 도메인 이름 목록(예: example.com,example2.com)입니다. 공백이 있으면 안 됩니다.

  이 그룹은 이러한 도메인에 대한 DNS 확인에만 사용됩니다. 이 DNS 플랫폼 설정 정책에 추가된 모든 그룹에 최대 30개의 개별 도메인을 입력할 수 있습니다. 각 이름은 최대 127자입니다.

  이러한 필터 도메인은 그룹의 기본 도메인 이름과 관련이 없습니다. 필터 목록은 기본 도메인과 다를 수 있습니다.

단계 **6** (선택 사항) **Expiry Entry Timer(**만료 입력 타이머**)** 및 **Poll Timer(**폴링 타이머**)** 값을 분 단위로 입력합니다.

이러한 옵션은 네트워크 개체에 지정된 FQDN에만 적용됩니다. 이는 다른 기능에 사용되는 FQDN에는 적용되지 않습니다.

- **Expire Entry Timer(**항목 만료 타이머**)**는 DNS 항목에 대한 최소 TTL (Time-To-Live)을 분 단위로 지정합니다. 만료 타이머가 항목의 TTL보다 긴 경우 TTL은 만료 항목 시간 값으로 증가합니다. TTL이 만료 타이머보다 길면 만료 입력 시간 값이 무시됩니다. 이 경우 TTL에 추가 시간이 추가되지 않습니다. 만료되면 DNS 조회 테이블에서 항목이 제거됩니다. 항목 제거 시 테이블을 다시 컴파일해야 하므로 자주 제거하면 디바이스의 처리 부하가 증가할 수 있습니다. 일부 DNS 항목은 매우 짧은 TTL(3초 정도)을 가질 수 있으므로 이 설정을 사용하여 TTL을 가상으로 늘릴 수 있습니다. 기본값은 1분입니다(즉, 모든 확인의 최소 TTL은 1 분). 범위는 1~65535분입니다.

  7.0 이하 버전을 실행하는 시스템의 경우 만료 시간이 실제로 TTL에 추가됩니다. 최소값을 지정하지 않습니다.

- **Poll Timer(**폴링 타이머**)**는 네트워크 개체에 정의된 FQDN을 확인하기 위해 디바이스가 DNS 서버를 쿼리한 후 시간 제한을 지정합니다. FQDN은 폴링 타이머가 만료된 때와 확인된 IP 엔트리의 TTL이 만료된 때 중 더 빠른 시점에 정기적으로 확인됩니다.

단계 **7** 모든 인터페이스 또는 특정 인터페이스에서 DNS 조회를 활성화합니다. 이러한 선택은 사용되는 라우팅 테이블에도 영향을 미칩니다.

인터페이스에서 DNS 조회를 활성화하는 것은 조회를 위해 소스 인터페이스를 지정하는 것과 다릅니다. threat defense는 항상 경로 조회를 사용하여 소스 인터페이스를 결정합니다.

- 인터페이스를 선택하지 않음 - 관리 및 관리 전용 인터페이스를 포함하여 모든 인터페이스에서 DNS 조회를 활성화합니다. threat defense는 데이터 라우팅 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- 특정 인터페이스가 선택되었지만 진단 인터페이스를 통한 **DNS** 조회도 활성화 옵션은 선택되지 않음 - 지정된 인터페이스에서 DNS 조회를 활성화합니다. threat defense는 데이터 라우팅 테이블만 확인합니다.
- 선택한 특정 인터페이스와 진단 인터페이스를 통한 **DNS** 조회도 활성화 옵션 - 지정된 인터페이스 및 진단 인터페이스에서 DNS 조회를 활성화합니다. threat defense는 데이터 라우팅 테이블을 확인하며, 경로가 없으면 관리 전용 라우팅 테이블로 폴백됩니다.
- **Enable DNS Lookup via diagnostic**인터페이스옵션만 - 진단에서 DNS 조회를 활성화합니다. threat defense는 관리 전용 라우팅 테이블만 확인합니다.**Devices(**디바이스**)Device Management(**디바이스 관리**) edit device(**디바이스 수정**)Interfaces(**인터페이스**)** 페이지에서 진단 인터페이스의 IP 주소를 설정해야 합니다.

단계 **8** 신뢰할 수 있는 DNS 서버를 구성하려면 **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 탭을 클릭합니다.

단계 **9** 기본적으로 DHCP 풀, DHCP 릴레이, DHCP 클라이언트 또는 DNS 서버 그룹에 구성된 기존 DNS 서버는 신뢰할 수 있는 DNS 서버로 포함됩니다. 이 중 하나라도 제외하려면 해당 확인란의 선택을 취소합니다.

단계 **10** 신뢰할 수 있는 DNS 서버를 추가하려면 **Specify DNS Servers(DNS** 서버 지정**)** 아래에서 **Edit(**편집**)**를 클릭합니다.

단계 **11** **Select DNS Servers(DNS** 서버 선택**)** 대화 상자에서 호스트 개체를 신뢰할 수 있는 DNS 서버로 선택하거나 신뢰할 수 있는 DNS 서버의 IP 주소를 직접 지정합니다.

a) 기존 호스트 개체를 선택하려면 **Available Host Objects(**사용 가능한 호스트 개체**)** 아래에서 필요한 호스트 개체를 선택하고 **Add(**추가**)**를 클릭하여 **Selected DNS Servers(**선택한 **DNS** 서버**)**에 포함합니다. 호스트 개체 추가에 대한 자세한 내용은 네트워크 개체 생성의 내용을 참조하십시오.

b) 신뢰할 수 있는 DNS 서버의 IP 주소(IPv4 또는 IPv6)를 직접 제공하려면 지정된 텍스트 필드에 주소를 입력하고 **Add(**추가**)**를 클릭하여 **Selected DNS Servers(**선택한 **DNS** 서버**)**에 포함합니다.

c) **Save(**저장**)**를 클릭합니다. 추가된 DNS 서버가 **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 페이지에 표시됩니다.

참고 정책당 최대 12개의 DNS 서버를 구성할 수 있습니다.

단계 **12** (선택 사항) 호스트 이름 또는 IP 주소를 사용하여 추가된 DNS 서버를 검색하려면 **Specify DNS Servers(DNS** 서버 지정**)** 아래의 검색 필드를 사용합니다.

단계 **13** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

액세스 제어 규칙에 FQDN 개체를 사용하려면 액세스 제어 규칙에 할당할 수 있는 FQDN 네트워크 개체를 만듭니다. 자세한 내용은 네트워크 개체 생성 섹션을 참조하십시오.

SSH에 대한 외부 인증 설정

참고 이 작업을 수행하려면 관리자 권한이 있어야 합니다.

관리 사용자에 대한 외부 인증을 활성화하는 경우, 외부 인증 객체에 지정된 대로 threat defense에서 LDAP 또는 RADIUS 서버로 사용자 자격 증명을 확인합니다.

외부 인증 객체 공유

외부 인증 개체는 management center 및 threat defense 디바이스가 사용할 수 있습니다. management center 및 디바이스 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다. threat defense에서는 RADIUS 서버에서 사용자를 정의하는 것을 지원하지만, management center에서는 외부 인증 객체에 사용자 목록을 미리 정의해야 합니다. threat defense에 대해 사전 정의된 목록 방법을 사용하도록 선택할 수 있지만, RADIUS 서버에서 사용자를 정의하려면 threat defense 및 management center에 대해 별도의 객체를 만들어야 합니다.

참고 시간 제한 범위는 threat defense와 management center가 다르므로 개체를 공유할 때는 threat defense의 더 적은 시간 제한 범위(LDAP의 경우 1~30초, RADIUS의 경우 1~300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 threat defense 외부 인증 설정이 작동하지 않습니다.

외부 인증 객체를 디바이스에 할당

management center의 경우, 외부 인증 개체를 **System(**시스템**)** > **User(**사용자**)** > **External Authentication(**외부 인증**)**에서 직접 활성화합니다. 이 설정은 management center 사용에만 영향을 주며 매니지드 디바이스 사용에 대해 활성화할 필요는 없습니다. threat defense 디바이스의 경우, 디바이스에 구축하는 플랫폼 설정에서 외부 인증 객체를 활성화해야 합니다. CAC 인증이 활성화된 LDAP 객체는 CLI 액세스에도 사용할 수 없습니다.

Threat Defense 지원되는 필드

외부 인증 개체에서 필드 하위 집합만 threat defense SSH 액세스에 사용됩니다. 다른 필드를 입력하는 경우, 해당 필드는 무시됩니다. 이 개체를 management center에 사용하는 경우 해당 필드가 사용됩니다. 이 절차는 threat defense에 대한 지원되는 필드만 적용합니다. 다른 필드는 Cisco Secure Firewall Management Center 관리 가이드에서 *Management Center*에 대한 외부 인증 구성을 참조하십시오.

사용자 이름

사용자 이름은 Linux에서 유효한 사용자 이름이어야 하며 소문자로 된 영숫자에 마침표(.) 또는 하이픈(-)을 사용해야 합니다. at 기호(@) 및 사선(/) 등 다른 특수 문자는 지원되지 않습니다. 외부 인증에 대한 관리자 사용자를 추가할 수 없습니다. 외부 사용자만 외부 인증 객체의 일부로 management center에서 추가할 수 있습니다. CLI에서는 추가할 수 없습니다. 내부 사용자는 management center가 아닌 CLI에서만 추가할 수 있습니다.

내부 사용자에 대해 **configure user add** 명령을 사용하여 동일한 사용자 이름을 구성한 경우, threat defense가 우선 내부 사용자에 대해 비밀번호를 확인하고 실패한 경우 LDAP 서버를 확인합니다. 참

고로 외부 사용자와 이름이 같은 내부 사용자를 나중에 추가할 수 없습니다. 기존 내부 사용자만 지원됩니다. RADIUS 서버에 정의된 사용자의 경우 권한 수준을 모든 내부 사용자와 동일하게 설정해야합니다. 그렇지 않으면 외부 사용자 비밀번호를 사용하여 로그인할 수 없습니다.

권한 레벨

LDAP 사용자는 항상 Config(구성) 권한을 갖습니다. RADIUS 사용자는 Config(구성) 또는 Basic(기본) 사용자로 정의할 수 있습니다.

시작하기 전에

- SSH 액세스는 관리 인터페이스에서 기본적으로 활성화됩니다. 데이터 인터페이스에서 SSH 액세스를 활성화하려면 보안 셸 설정, 22 페이지 섹션을 참조하십시오. SSH는 진단 인터페이스에서 지원되지 않습니다.
- 기대치를 적절하게 설정하려면 RADIUS 사용자를 다음 동작에 알려주십시오.
  - 외부 사용자가 처음 로그인하면 threat defense에서는 필수 구조를 생성합니다. 하지만 이와 동시에 사용자 세션을 생성할 수는 없습니다. 세션을 시작하려면 사용자는 다시 인증하기만 하면 됩니다. 사용자에게는 다음과 같은 메시지가 표시됩니다. "New external username identified(새 외부 사용자 이름이 식별됨). Please log in again to start a session(세션을 시작하려면 다시 로그인하십시오)."
  - 이와 마찬가지로 Service-Type(서비스 유형) 권한 부여가 마지막 로그인 후 변경된 경우, 사용자는 다시 인증해야 합니다. 사용자에게는 다음과 같은 메시지가 표시됩니다. "Your authorization privilege has changed(귀하의 권한 부여 권한이 변경되었습니다). Please log in again to start a session(세션을 시작하려면 다시 로그인하십시오)."

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **3** **Manage External Authentication Server(**외부 인증 서버 관리**)** 링크를 클릭합니다.

System(시스템**)** > **Users(**사용자**)** > **External Authentication(**외부 인증**)**을 클릭하여 External Authentication(외부 인증) 화면을 열 수도 있습니다.

단계 **4** LDAP 인증 개체를 구성합니다.

a) **Add External Authentication Object(**외부 인증 객체 추가**)**를 클릭합니다.
b) **Authentication Method(**인증 방법**)**을 **LDAP**로 설정합니다.
c) **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.
d) 드롭다운 목록에서 **Server Type(**서버 유형**)**을 선택합니다.
e) **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

참고 TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

f) (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

g) (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

h) **LDAP-Specific Parameters(LDAP** 전용 파라미터**)**를 입력합니다.

- **Base DN(**기본 **DN)** - 액세스하려는 LDAP 디렉토리의 기본 DN을 입력합니다. 예를 들어, 예시 회사의 보안 조직에서 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다. 아니면 **Fetch DN(DN** 가져오기**)**을 클릭하고, 드롭다운 목록에서 적절한 기본 고유 이름을 선택합니다.
- (선택 사항) **Base Filter(**기본 필터**)** - 예를 들어 디렉터리 트리의 사용자 개체에 `physicalDeliveryOfficeName` 속성이 있고 뉴욕 사무실의 사용자는 그 속성 값이 `NewYork`인 경우 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.
- **User Name(**사용자 이름**)** - LDAP 서버를 찾아볼 수 있는 충분한 자격 증명이 있는 사용자의 고유 이름을 입력합니다. 예를 들어 OpenLDAP 서버에 연결하려는 경우, 해당 사용자 개체에 `uid` 속성이 있으며 예시 회사 보안 부서 관리자 개체의 `uid`값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.
- **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** - 사용자의 비밀번호를 입력하고 확인합니다.
- (선택 사항) **Show Advanced Options(**고급 옵션 표시**)** - 다음 고급 옵션을 구성합니다.
  - **Encryption(**암호화**)- None (**해당 없음**)**, **TLS**또는 **SSL**을 클릭 합니다.

    참고 포트를 지정한 다음 암호화 방식을 변경할 경우, 그 방법에 대해서는 포트가 기본값으로 재설정됩니다. **None(**해당 없음**)** 또는 **TLS**인 경우, 포트는 기본값인 389로 재설정됩니다. SSL 암호화를 선택할 경우 포트는 636로 재설정됩니다.

  - **SSL Certificate Upload Path(SSL** 인증서 업로드 경로**)**—SSL 또는 TLS 암호화인 경우, **Choose File(**파일 선택**)**을 클릭하여 인증서를 선택해야 합니다.
  - (사용되지 않음) **User Name Template(**사용자 이름 템플릿**)** - threat defense에서 사용되지 않습니다.
  - **Timeout(**시간 초과**)**—백업 연결로 전환하기 전 시간(초)을 입력합니다. 기본값은 30입니다.

    참고 시간 초과 범위는 threat defense와 management center에 따라 다르므로 개체를 공유하는 경우 threat defense의 더 작은 시간 초과 범위 (1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 threat defense 외부 인증 설정이 작동하지 않습니다.

i) (선택 사항) 사용자 고유 유형 이외의 셸 액세스 속성을 사용하려는 경우 **CLI Access Attribute(CLI 액세스 속성)**를 입력합니다. 예를 들어 Microsoft Active Directory Server에서 `sAMAccountName` 셸 액세스 속성을 사용하여 셸 액세스 사용자를 가져오려면 `sAMAccountName`을 **CLI Access Attribute(CLI 액세스 속성)**필드에 입력합니다.

j) **Shell Access Filter(셸 액세스 필터)**를 설정합니다.

다음 방법 중 하나를 선택합니다.

- 인증 설정을 구성할 때 지정한 것과 동일한 필터를 사용하려면 **Same as Base Filter(기본 필터와 동일)**를 선택합니다.
- 속성 값에 따라 관리자 사용자 엔트리를 검색하려면 속성 이름, 비교 연산자, 필터로 사용할 속성 값을 괄호로 묶어 입력합니다. 예를 들어 모든 네트워크 관리자에게 `manager` 속성이 있고 그 값이 `shell`이라면 `(manager=shell)`이라는 기본 필터를 설정할 수 있습니다.

LDAP 서버의 이름은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

k) **Save(저장)**를 클릭합니다.

단계 **5** LDAP의 경우 LDAP 서버에서 사용자를 나중에 추가 또는 삭제하는 경우, 사용자 목록을 새로 고침하고 Platform Settings(플랫폼 설정)을 재구축해야 합니다.

a) **System** > **Users** > **External Authentication**(시스템 사용자 외부 인증)을 선택합니다.

b) LDAP 서버 옆에 **Refresh(새로 고침)**( )를 클릭합니다.

사용자 목록을 변경하는 경우, 디바이스에 대한 구성 변경을 구축하라는 메시지가 표시됩니다. Firepower Theat Defense 플랫폼 설정에서도 "Out-of-Date on *x* targeted devices."이라고 표시됩니다.

c) 구성 변경사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

단계 **6** RADIUS 인증 개체를 구성합니다.

a) Service-Type 속성을 사용하여 RADIUS 서버에서 사용자를 정의합니다.

다음은 Service-Type 속성에 대해 지원되는 값입니다.

- Administrator(관리자) (6) - CLI에 대한 Config 액세스 권한을 제공합니다. 이러한 사용자는 CLI에서 모든 명령을 사용할 수 있습니다.
- NAS Prompt(NAS 프롬프트) (7) 또는 6 이외의 모든 레벨 - CLI에 대한 기본 액세스 권한을 제공합니다. 이러한 사용자는 모니터링 및 문제 해결을 위해 **show** 명령 같은 읽기 전용 명령을 사용할 수 있습니다.

이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)

- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

또는 외부 인증 객체에서 사용자를 미리 정의할 수 있습니다(6.j, 13 페이지 단계 참조). threat defense, management center에 동일한 RADUIS 서버를 사용하는 한편 Service-Type(서비스-유형) 속성 방법을 threat defense에 사용하려는 경우, 동일한 RADIUS 서버를 식별하는 두 개의 외부 인증 개체를 생성합니다. 한 개체는 사전 정의된 **CLI Access Filter(CLI** 액세스 필터**)** 사용자(management center 사용)를 포함하며, 나머지 한 개체는 **CLI Access Filter(CLI** 액세스 필터**)**를 공란으로 둡니다(threat defense에 사용).

b) management center에서 **Add External Authentication Object(**외부 인증 객체 추가**)**를 클릭합니다.

c) **Authentication Method(**인증 방법**)**을 **RADIUS**로 설정합니다.

d) **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

e) **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

참고 TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

f) (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

g) **RADIUS Secret Key(RADIUS** 비밀 키**)**를 입력합니다.

h) (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

i) **RADIUS-Specific Parameters(RADUIS** 특정 파라미터**)**를 입력합니다.

- **Timeout (Seconds)(**시간 초과**)(**초**)**—백업 연결로 전환하기 전 시간(초)을 입력합니다. 기본값은 30입니다.
- **Retries(**재시도**)** - 백업 연결로 넘어가기 전에 기본 서버 연결을 시도하는 횟수를 입력합니다. 기본값은 3입니다.

j) (선택 사항) RADIUS 정의 사용자를 사용하는 대신 **CLI Access Filter(CLI** 액세스 필터**)**에서 **Administrator CLI Access User List(**관리자 **CLI** 액세스 사용자 목록**)** 필드에 쉼표로 구분된 사용자 이름 목록을 입력합니다. 예를 들어, **`jchrichton, aerynsun, rygel`**을 입력합니다.

threat defense에 **CLI Access Filter(CLI** 액세스 필터**)** 방법을 사용하여 threat defense 및 다른 플랫폼 유형과 동일한 외부 인증 개체를 사용할 수 있습니다. RADIUS에서 정의한 사용자를 사용하려는 경우, **CLI Access Filter(CLI** 액세스 필터**)**를 공란으로 두어야 합니다.

이러한 사용자 이름은 RADIUS 서버의 사용자 이름과 일치해야 합니다. 이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

참고 RADIUS 서버에서만 사용자를 정의하려면 이 섹션을 비워 두어야 합니다.

k) **Save(**저장**)**를 클릭합니다.

단계 **7** **Devices(**디바이스**)** > > **Platform Settings(**플랫폼 설정**)** > **External Authentication(**외부 인증**)**

단계 **8** 새로 추가된 객체를 보려면 **Refresh(**새로 고침**)**( )를 클릭합니다.

SSL 또는 TLS 암호화를 지정할 때 LDAP의 경우 연결에 대한 인증서를 업로드해야 합니다. 그렇지 않으면 이 탭에 서버가 나열되지 않습니다.

단계 **9** 사용할 외부 인증 객체 옆에 있는 **Slider enabled(**슬라이더 활성화됨**)** ( )를 클릭합니다. 하나의 객체만 활성화 할 수 있습니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

단계 **11** 구성 변경사항을 구축합니다. 구성 변경 사항 구축의 내용을 참조하십시오.

프래그먼트 처리 설정

기본적으로 threat defense 디바이스는 IP 패킷당 최대 24개의 프래그먼트를 허용하고 재조립 작업에 대기 중인 최대 200개의 프래그먼트를 허용합니다. UDP를 통한 NFS와 같이 일상적으로 패킷을 프래그먼트하는 애플리케이션이 있는 경우 네트워크에 프래그먼트가 필요할 수도 있습니다. 그러나 트래픽을 단편화하는 애플리케이션이 없으면 **Chain(**체인**)**을 1로 설정하여 프래그먼트를 허용하지 않는 것이 좋습니다. 단편화된 패킷은 종종 서비스 거부(DoS) 공격으로 사용됩니다.

참고 이 설정은 이 정책에 할당된 디바이스의 기본값을 설정합니다. 인터페이스 구성에서 **Override Default Fragment Setting(**기본 프래그먼트 설정 재정의**)**을 선택하여 디바이스의 특정 인터페이스에 대해 이 설정을 재정의할 수 있습니다. 인터페이스를 편집할 때 **Advanced(**고급**)** > **Security Configuration(**보안 구성**)**에서 옵션을 찾을 수 있습니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스를 편집한 다음 **Interfaces(**인터페이스**)**를 선택하여 인터페이스 속성을 편집합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Fragment Settings(**프래그먼트 설정**)**를 선택합니다.

단계 **3** 다음 옵션을 구성합니다. 기본 설정을 사용하려면 **Reset to Defaults(**기본값으로 재설정**)**를 클릭합니다.

- **Size(Block)(**크기(블록)**)** - 재조립에 대해 대기할 수 있는 모든 연결에서 패킷 프래그먼트의 최대 수입니다. 기본값은 200 프래그먼트입니다.

- **Chain (Fragment)(**체인**(**프래그먼트**))** - 전체 IP 패킷을 단편화할 수 있는 최대 패킷 수입니다. 기본값은 24패킷입니다. 프래그먼트를 허용하지 않으려면 이 옵션을 1로 설정합니다.
- **Timeout (Sec)(**시간 초과**(**초**))** - 단편화된 전체 패킷이 도착할 때까지 기다리는 최대 시간(초)입니다. 기본값은 5일입니다. 이 시간 내에 모든 프래그먼트가 수신되지 않으면 모든 프래그먼트가 삭제됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

HTTP 설정

threat defense 디바이스의 하나 이상의 인터페이스에 HTTPS 연결을 허용하려면 HTTPS 설정을 구성합니다. HTTPS를 사용하여 문제 해결을 위해 패킷 캡처를 다운로드할 수 있습니다.

시작하기 전에

- Secure Firewall Management Center를 사용하여 threat defense를 관리하면 threat defense에 대한 HTTPS 액세스는 패킷 캡처 파일을 보는 용도로만 사용됩니다. threat defense에는 이 관리 모드에서 구성할 웹 인터페이스가 없습니다.
- HTTPS 로컬 사용자는 **configure user add** 명령을 사용하여 CLI에서만 구성할 수 있습니다. 기본적으로 초기 설정 중에 비밀번호를 구성한 관리자 사용자가 있습니다. AAA 외부 인증은 지원되지 않습니다.
- 이 설정은 관리 전용으로 구성한 데이터 인터페이스를 포함하여 데이터 인터페이스에만 적용됩니다. 전용 관리 인터페이스에는 적용되지 않습니다.물리적 관리 인터페이스는 논리적 진단 인터페이스와 논리적 관리 인터페이스 간에 공유됩니다. 이 구성은 논리적 진단 인터페이스(사용된 경우) 또는 다른 데이터 인터페이스에만 적용됩니다. 논리적 관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 management center에 설치하고 등록하는 데 사용됩니다. 별도의 IP 주소와 정적 라우팅을 가지고 있습니다.
- HTTPS를 사용하려면 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 HTTPS 액세스를 구성하면 됩니다.
- 연결할 수 있는 인터페이스에만 HTTPS를 사용할 수 있습니다. HTTPS 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다.
- 동일한 TCP 포트에 대한 동일한 인터페이스에서 HTTPS 액세스와 AnyConnect 원격 액세스 SSL VPN을 모두 구성할 수는 없습니다. 예를 들어, 외부 인터페이스에서 원격 액세스 SSL VPN을 구성하는 경우, 포트 443에서 HTTPS 연결에 대한 외부 인터페이스도 열 수 없습니다. 동일한 인터페이스에서 두 기능을 구성해야 하는 경우 다른 포트를 사용합니다. 예를 들어 포트 4443에서 HTTPS를 엽니다.

- 디바이스에 HTTPS 연결을 허용할 호스트 또는 네트워크를 정의하는 네트워크 개체가 필요합니다. 이 절차의 일부로 개체를 추가할 수 있지만 개체 그룹을 사용하여 IP 주소 그룹을 식별하려면 규칙에 필요한 그룹이 이미 있는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 설정합니다.

참고 시스템에서 제공하는 **any** 네트워크 개체 그룹을 사용할 수 없습니다. 대신 **any-ipv4** 또는 **any-ipv6**를 사용합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **HTTP**를 선택합니다.

단계 **3** HTTP 서버를 활성화하려면 **Enable HTTP Server(HTTP** 서버 활성화**)** 확인란을 선택합니다.

단계 **4** (선택 사항) HTTP 포트를 변경합니다. 기본값은 443입니다.

단계 **5** HTTP 연결을 허용하는 인터페이스와 IP 주소를 확인합니다.

이 테이블을 사용하여 HTTP 연결을 허용할 인터페이스와 이러한 연결을 허용할 수 있는 클라이언트의 IP 주소를 제한합니다. 개별 IP 주소가 아닌 네트워크 주소를 사용할 수 있습니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **IP Address(IP** 주소**)** - HTTP 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체 또는 그룹입니다. 드롭다운 메뉴에서 개체를 선택하거나 +를 클릭하여 새 네트워크 개체를 추가합니다.
- **Security Zones(**보안 영역**)** - HTTP 연결을 허용할 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Security Zones(**선택한 보안 영역**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

ICMP 액세스 규칙 구성

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

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

디바이스를 공격으로부터 보호하려면 ICMP 규칙을 사용하여 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 목록의 끝에 암시적 거부 ICMP 규칙이 추가되어 기본 동작이 변경됩니다. 따라서 단지 몇 가지 메시지 유형만 거부하려면 ICMP 규칙 목록의 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 인접 디바이스 검색 프로세스에서 IPv6의 ICMP 패킷이 사용됩니다.

시작하기 전에

규칙에 필요한 개체가 이미 존재하는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 설정합니다. 원하는 호스트 또는 네트워크를 정의하는 네트워크 개체 또는 그룹 및 제어하려는 ICMP 메시지 유형을 정의하는 포트 개체가 필요합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **ICMP**를 선택합니다.

단계 **3** ICMP 규칙을 구성합니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **Action(**작업**)** - 일치하는 트래픽을 허용 또는 거부할지 여부입니다.
- **ICMP Service(ICMP** 서비스**)** - ICMP 메시지를 식별하는 포트 개체 유형입니다.
- **Network(**네트워크**)** - 액세스를 제어하는 호스트 또는 네트워크를 식별하는 네트워크 개체 또는 그룹입니다.
- **Security Zones(**보안 영역**)** - 보호하려는 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Security Zones(**선택한 보안 영역**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** (선택 사항). ICMPv4 연결 불가 메시지의 속도 제한을 설정합니다.

- **Rate Limit(**속도 제한**)** - Unreachable 메시지의 속도 제한을 설정합니다(초당 메시지 1~100개). 기본값은 초당 메시지 1개입니다.
- **Burst Size(**버스트 크기**)** - 버스트 속도를 설정합니다(1~10). 시스템은 이 수의 응답을 전송하지만, 속도 제한에 도달할 때까지 후속 응답은 전송되지 않습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SSL 설정

참고 이 작업을 수행하려면 관리자 권한이 있어야 하며 리프 도메인에 있어야 합니다.

Secure Firewall Management Center의 완전한 라이선스 버전을 실행하는지 확인해야 합니다. 평가 모드에서 Secure Firewall Management Center를 실행 중인 경우 SSL 설정을 사용할 수 없습니다. 또한 라이선스가 있는 Secure Firewall Management Center 버전이 export-compliance기준을 충족하지 않으면 SSL 설정이 비활성화됩니다. SSL과 함께 원격 액세스 VPN을 사용하는 경우 스마트 계정에 강력한 암호화 기능이 활성화되어 있어야 합니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 라이선스 유형 및 제한 사항을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 수정합니다.

단계 **2** **SSL**을 선택합니다.

단계 **3** **Add SSL Configuration(SSL** 구성 추가**)** 테이블에 항목을 추가합니다.

a) **Add(**추가**)**를 클릭하여 새 항목을 만들거나 항목이 이미 있는 경우 **Edit(**편집**)**을 클릭합니다.

b) 드롭다운 목록에서 필수 보안 설정을 선택합니다.

- **Protocol Version(**프로토콜 버전**)** - Remote Access VPN 세션을 설정하는 동안 사용할 TLS 프로토콜을 지정합니다.
- **Security Level(**보안 수준**)** - SSL에 대해 설정하려는 보안 위치 지정의 종류를 나타냅니다.

단계 **4** 선택한 프로토콜 버전에 따라 **Available Algorithms(**사용 가능한 알고리즘**)**를 선택하고 **Add(**추가**)**를 클릭하여 선택한 프로토콜에 대해 포함합니다. 자세한 내용은 SSL 설정 정보, 19 페이지을 참고하십시오.

알고리즘은 선택한 프로토콜 버전에 따라 나열됩니다. 각 보안 프로토콜은 보안 수준을 설정하는 고유한 알고리즘을 식별합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

다음에 수행할 작업

Deploy(구축**)** > **Deployment(**구축**)**을 선택하고 **Deploy(**구축**)**를 클릭하여 할당된 디바이스에 정책을 구축합니다.

SSL 설정 정보

threat defense 디바이스 SSL(Secure Sockets Layer) (SSL) 프로토콜 및 전송 레이어 보안 (TLS)을 사용하 여 원격 클라이언트에서 Remote Access VPN 연결에 대 한 보안 메시지 전송을 지원 합니다. SSL 설정 창을 사용하면 SSL을 통한 원격 VPN 액세스 중 메시지 전송을 위해 협상되고 사용되는 SSL 버전 및 암호화 알고리즘을 구성할 수 있습니다.

다음 위치에 SSL 설정을 구성합니다.

Devices(디바이스**) > Platform Settings(**플랫폼 설정**) > SSL**

필드

Minimum SSL Version as Server(최소 **SSL** 버전**(**서버**))** - threat defense 디바이스가 서버 역할을 할 때 사용하는 최소 SSL/TLS 프로토콜 버전을 지정합니다. 예를 들어 Remote Access VPN 게이트웨이로 작동할 경우입니다.

TLS Version(TLS 버전**)** - 드롭다운 목록에서 다음 TLS 버전 중 하나를 선택합니다.

TLS V1	SSLv2 클라이언트 Hello를 수락하고 TLSv1 이상을 협상합니다.
TLSv1.1	SSLv2 클라이언트 Hello를 수락하고 TLSv1.1 이상을 협상합니다.
TLSV1.2	SSLv2 클라이언트 Hello를 수락하고 TLSv1.2 이상을 협상합니다.

DTLS Version(DTLS 버전**)** - 선택한 TLS 버전을 기준으로 드롭다운 목록에서 DTLS 버전을 선택합니다. 기본적으로 DTLSv1은 threat defense 디바이스에 설정됩니다. 요구 사항에 따라 DTLS 버전을 선택할 수 있습니다.

참고 TLS 프로토콜 버전이 선택한 DTLS 프로토콜 버전과 같거나 그 이상인지 확인합니다. TLS 프로토콜 버전은 다음 DTLS 버전을 지원합니다.

TLS V1	DTLSv1
TLSv1.1	DTLSv1
TLSV1.2	DTLSv1, DTLSv1.2

Diffie-Hellman Group(Diffie-Hellman그룹**)** - 드롭다운 목록에서 그룹을 선택합니다. 사용 가능한 옵션은 Group1 - 768-bit modulus(그룹 1 - 768비트 모듈러스), Group2 - 1024-bit modulus(그룹 2 - 1024비트 모듈러스), Group5 - 1536-bit modulus(그룹 5 - 1536비트 모듈러스), Group14 - 2048-bit modulus, 224-bit prime order(그룹 14 - 2048비트 모듈러스, 224비트 소수 위수) 및 Group24 - 2048-bit modulus, 256-bit prime order(그룹 24 - 2048비트 모듈러스, 256비트 소수 위수)입니다. 기본값은 Group1입니다.

Elliptical Curve Diffie-Hellman Group(Elliptical Curve Diffie-Hellman 그룹**)** - 드롭다운 목록에서 그룹을 선택합니다. 사용 가능한 옵션은 Group19 - 256-bit EC(그룹 19 - 256비트 EC), Group20 - 384-bit EC(그룹 20 - 384비트 EC) 및 Group21 - 521-bit EC(그룹 21 - 521비트 EC)입니다. 기본값은 Group19입니다.

TLSv1.2는 다음과 같은 암호화에 대한 지원을 추가합니다.

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

참고 ECDSA 및 DHE 암호가 우선 순위가 가장 높습니다.

SSL 구성 테이블을 사용하여 Secure Firewall Threat Defense 디바이스에서 지원하려는 프로토콜 버전, 보안 수준 및 비밀번호 알고리즘을 지정할 수 있습니다.

Protocol Version(프로토콜 버전**)** - Secure Firewall Threat Defense 디바이스에서 지원하고 SSL 연결에 사용하는 프로토콜 버전을 나열합니다. 사용 가능한 프로토콜 버전은 다음과 같습니다.

- 기본

- TLSV1
- TLSv1.1
- TLSV1.2
- DTLSv1
- DTLSv1.2

Security Level(보안 수준**)** - threat defense 디바이스에서 지원하고 SSL 연결에 사용하는 암호화 보안 수준을 나열합니다.

평가 라이선스가 있는 threat defense 디바이스를 사용하는 경우 기본적으로 보안 레벨은 Low(낮음)입니다. threat defense 스마트 라이선스의 경우 기본 보안 레벨은 High(높음)입니다. 다음 옵션 중 하나를 선택하여 필요한 보안 레벨을 설정할 수 있습니다.

- **All(**모두**)** - NULL-SHA를 비롯한 모든 암호화를 포함합니다.
- **Low(**낮음**)** - NULL-SHA를 제외한 모든 암호화를 포함합니다.
- **Medium(**보통**)**은 NULL-SHA, DES-CBC-SHA, RC4-SHA 및 RC4-MD5를 제외한 모든 암호화를 포함합니다(기본값).
- **Fips**는 모든 FIPS 호환 암호화(NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA 제외)를 포함합니다.
- **High(**높음**)**는 AES-256 SHA-2 암호화만 포함하며, TLS 버전 1.2 및 기본 버전에 적용됩니다.
- **Custom(**사용자 지정**)**은 Cipher algorithms/custom string(암호화 알고리즘/사용자 지정 문자열) 상자에서 지정한 하나 이상의 암호화를 포함합니다. 이 옵션은 OpenSSL 암호화 정의 문자열을 사용하는 암호 그룹에 대한 모든 권한을 제공합니다.

Cipher Algorithms/Custom String(암호화 알고리즘/사용자 지정 문자열**)** - threat defense 디바이스에서 지원하고 SSL 연결에 사용하는 암호화 알고리즘을 나열합니다. OpenSSL을 사용하는 암호화에 대한 자세한 내용은 다음 섹션을 참고하십시오. https://www.openssl.org/docs/apps/ciphers.html

threat defense 디바이스에서는 지원되는 암호화에 대한 우선순위를 다음과 같이 지정합니다.

TLSv1.2에서만 지원되는 암호화

ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256

AES256-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
AES128-SHA256

TLSv1.1 또는 TLSv1.2에서 지원되지 않는 암호화

RC4-SHA
RC4-MD5
DES-CBC-SHA
NULL-SHA

보안 셸 설정

외부와 같은 데이터 인터페이스에서 management center 액세스를 활성화한 경우 이 절차를 사용하여 해당 인터페이스에서 SSH를 활성화해야 합니다. 이 섹션에서는 threat defense에서 하나 이상의 데이터 또는 진단 인터페이스에 대한 SSH 연결을 활성화하는 방법을 설명합니다. SSH는 논리적 진단 인터페이스에서 지원되지 않습니다.

참고 SSH는 관리 인터페이스에서 기본적으로 활성화됩니다. 하지만 이 화면은 관리 SSH 액세스에 영향을 미치지 않습니다.

관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 management center에 설치하고 등록하는 데 사용됩니다. 데이터 인터페이스용 SSH는 관리 인터페이스용 SSH로 내부 및 외부 사용자 목록을 공유합니다. 다른 설정은 별도로 구성됩니다. 데이터 인터페이스의 경우 이 화면을 사용하여 SSH 및 액세스 목록을 활성화합니다. 데이터 인터페이스용 SSH 트래픽은 일반 라우팅 구성을 사용하며 설치 또는 CLI에서 구성된 정적 경로는 사용하지 않습니다.

관리 인터페이스의 경우 SSH 액세스 목록을 구성하려면 Cisco Secure Firewall Threat Defense 명령 참조의 **configure ssh-access-list** 명령을 참조하십시오. 정적 경로를 구성하려면 **configure network**

static-routes 명령을 참조하십시오. 기본적으로 초기 설정 시 관리 인터페이스를 통해 기본 경로를 구성합니다.

SSH를 사용하려면 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 SSH 액세스를 구성하면 됩니다.

연결할 수 있는 인터페이스에만 SSH를 사용할 수 있습니다. SSH 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다.

참고 3회 연속 SSH를 사용한 CLI 로그인에 실패한 경우, 디바이스가 SSH 연결을 종료합니다.

시작하기 전에

- **configure user add** 명령을 사용해 CLI에서 SSH 내부 사용자를 설정할 수 있습니다. CLI에서 내부 사용자 추가의 내용을 참조하십시오. 기본적으로 초기 설정 중에 비밀번호를 구성한 관리자 사용자가 있습니다. 플랫폼 설정에서 **External Authentication(**외부 인증**)**을 구성하여 LDAP 또는 RADIUS에서 외부 사용자를 구성할 수도 있습니다. SSH에 대한 외부 인증 설정, 9 페이지를 참조하십시오.
- 디바이스에 SSH 연결을 허용할 호스트 또는 네트워크를 정의하는 네트워크 개체가 필요합니다. 이 절차의 일부로 개체를 추가할 수 있지만 개체 그룹을 사용하여 IP 주소 그룹을 식별하려면 규칙에 필요한 그룹이 이미 있는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 설정합니다.

참고 시스템에서 제공하는 **any** 네트워크 개체를 사용할 수 없습니다. 대신 **any-ipv4** 또는 **any-ipv6**를 사용합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Secure Shell(**보안 쉘**)**를 선택합니다.

단계 **3** SSH 연결을 허용하는 인터페이스와 IP 주소를 확인합니다.

이 테이블을 사용하여 SSH 연결을 허용할 인터페이스와 이러한 연결을 허용할 수 있는 클라이언트의 IP 주소를 제한합니다. 개별 IP 주소가 아닌 네트워크 주소를 사용할 수 있습니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **IP Address(IP** 주소**)** - SSH 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체 또는 그룹입니다. 드롭다운 메뉴에서 개체를 선택하거나 +를 클릭하여 새 네트워크 개체를 추가합니다.

- **Security Zones(**보안 영역**)** - SSH 연결을 허용할 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Security Zones(**선택한 보안 영역**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SMTP 설정

Syslog 설정에서 이메일 알림을 구성하는 경우 SMTP 서버를 식별해야 합니다. Syslog에 대해 구성하는 소스 이메일 주소는 SMTP 서버의 유효한 계정이어야 합니다.

시작하기 전에

기본 및 보조 SMTP 서버의 호스트 주소를 정의하는 네트워크 개체가 존재하는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 정의합니다. 정책을 편집하면서 개체를 생성할 수도 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **SMTP Server(SMTP** 서버**)**를 클릭합니다.

단계 **3** **Primary Server IP Address(**기본 서버 **IP** 주소**)** 및 선택적으로 **Secondary Server IP Address(**보조 서버 **IP** 주소**)**를 식별하는 네트워크 개체를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SNMP 구성

단순 네트워크 관리 프로토콜(SNMP)은 PC 또는 워크스테이션에서 실행되는 네트워크 관리 스테이션을 위한 표준 방식을 정의하여 스위치, 라우터 및 보안 어플라이언스를 포함한 여러 유형의 디바이

스 상태를 모니터링합니다. SNMP 페이지를 사용하여 SNMP 관리 스테이션의 모니터링을 위해 방화벽 디바이스를 구성할 수 있습니다.

단순 네트워크 관리 프로토콜(SNMP)을 활성화하면 중앙 위치에서 네트워크 디바이스를 모니터링할 수 있습니다. Cisco 보안 어플라이언스는 SNMP 버전 1, 2c 및 3은 물론 트랩 및 SNMP 읽기 액세스를 사용하는 네트워크 모니터링을 지원합니다. SNMP 쓰기 액세스는 지원되지 않습니다.

SNMPv3는 읽기 전용 사용자 및 DES(더 이상 사용되지 않음), 3DES, AES256, AES192 및 AES128을 통한 암호화를 지원합니다.

참고 DES 옵션은 더 이상 사용되지 않습니다. 6.5 이전 버전을 사용하여 생성한 DES 암호화를 사용하는 SNMP v3 사용자가 구축에 포함된 경우, 6.6 이하 버전을 실행하는 threat defense에 대해 해당 사용자를 계속 사용할 수 있습니다. 그러나 이러한 사용자를 수정하고 DES 암호화를 유지하거나 DES 암호화를 사용하여 새 사용자를 생성할 수는 없습니다. management center에서 버전 7.0 이상을 실행하는 threat defense를 관리하는 경우 DES 암호화를 사용하는 플랫폼 설정 정책을 해당 threat defense에 구축할 수 없습니다.

참고 SNMP 구성은 라우팅 및 진단 인터페이스만 지원합니다.

참고 외부 SNMP 서버에 알림을 생성하려면 **Policies(**정책**)** > **Action(**작업**)** > **Alerts(**알림**)**에 액세스합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **SNMP**를 선택합니다.

단계 **3** SNMP를 활성화하고 기본 옵션을 구성합니다.

- **Enable SNMP Servers(SNMP** 서버 활성화**)** - SNMP 정보를 구성된 SNMP 호스트에 제공할지 여부입니다. 구성 정보를 유지하는 동안 SNMP 모니터링을 비활성화하려면 이 옵션의 선택을 취소할 수 있습니다.
- **Read Community String(**읽기 커뮤니티 문자열**)**, **Confirm(**확인**)** - threat defense 디바이스에 요청을 보낼 때 SNMP 관리 스테이션에서 사용하는 암호를 입력합니다. SNMP 커뮤니티 문자열은 SNMP 관리 스테이션과 관리 대상 네트워크 노드 사이에서 비밀로 공유됩니다. 보안 디바이스는 이 비밀번호를 사용하여 수신 SNMP 요청이 유효한지 판단합니다. 비밀번호는 대/소문자를 구분하며 최대 32자의 영숫자 문자열입니다. 공백과 특수 문자는 허용되지 않습니다.
- **System Administrator Name(**시스템 관리자 이름**)** - 디바이스 관리자 또는 다른 담당자의 이름을 입력합니다. 이 문자열은 대/소문자를 구분하며 최대 127자까지 가능합니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.

- **Location(**위치**)** - 이 보안 디바이스의 위치를 입력합니다(예: Building 42, Sector 54). 이 문자열은 대/소문자를 구분하며 최대 127자까지 가능합니다. 공백을 사용할 수는 있지만 여러 공백을 사용하는 경우에는 단일 공백으로 단축됩니다.
- **Port(**포트**)** - 수신 요청을 수락할 UDP 포트를 입력합니다. 기본값은 161입니다.

단계 **4** (SNMPv3만 해당) SNMPv3 사용자 추가, 31 페이지.

단계 **5** SNMP 호스트 추가, 33 페이지.

단계 **6** SNMP 트랩 구성, 35 페이지.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SNMP 정보

SNMP는 네트워크 디바이스 간의 관리 정보 교환을 용이하게 하는 애플리케이션 레이어 프로토콜이며 TCP/IP 프로토콜 제품군의 일부입니다. Threat Defense는 SNMP 버전 1, 2c 및 3을 사용하는 네트워크 모니터링을 지원하며, 세 가지 버전을 동시에 사용할 수 있도록 지원합니다. threat defense 인터페이스에서 실행되는 SNMP 에이전트를 사용하면 HP OpenView와 같은 NMS(네트워크 관리 시스템)을 통해 네트워크 디바이스를 모니터링할 수 있습니다. Threat Defense는 GET 요청 발행을 통해 SNMP 읽기 전용 액세스를 지원합니다. SNMP 쓰기 액세스는 허용되지 않으므로 SNMP를 사용하여 변경할 수는 없습니다. 또한 SNMP SET 요청은 지원되지 않습니다.

threat defense를 NMS로의 특정 이벤트(알림 포함)에 대해 관리 디바이스에서 관리 스테이션으로 전송되는 요청하지 않은 메시지인 트랩을 보내도록 구성하거나 NMS를 사용하여 보안 디바이스에서 MIB(관리 정보 기반)를 찾아볼 수 있습니다. MIB는 정의 모음이고 threat defense은 각 정의에 대한 값 데이터베이스를 유지합니다. MIB를 찾아보는 것은 NMS에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 발행하는 것을 의미합니다.

SNMP 에이전트는 예를 들어 네트워크 링크가 실행 또는 중단 상태로 전환될 때 알림이 필요하도록 사전 정의된 이벤트가 발생하는 경우 지정된 관리 스테이션에 알려줍니다. 이때 보내는 알림은 관리 스테이션에 스스로를 식별하는 SNMP OID를 포함합니다. 에이전트는 관리 스테이션이 정보를 요구할 때 응답하기도 합니다.

SNMP 용어

다음 표는 SNMP에서 작업할 때 일반적으로 사용되는 용어를 나열합니다.

표 *1: SNMP* 용어

용어	설명
에이전트	Secure Firewall Threat Defense에서 실행되는 SNMP 서버입니다. SNMP 에이전트는 다음과 같은 특징을 갖습니다. • 정보 요청 및 네트워크 관리 스테이션의 작업에 대해 응답합니다. • SNMP 관리자가 보거나 변경할 수 있는 객체 모음인 MIB(관리 정보 기반)에 대한 액세스를 제어합니다. • SET 작업을 허용하지 않습니다.
찾아보기	디바이스의 SNMP 에이전트에서 필요한 정보를 폴링함으로써 네트워크 관리 스테이션에서 해당 디바이스의 상태를 모니터링합니다. 이 작업은 값을 결정하기 위해 네트워크 관리 스테이션에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 생성하는 것을 포함할 수 있습니다.
MIB(관리 정보 기반)	패킷, 연결, 버퍼, 장애 조치 등에 관한 정보를 수집하기 위한 표준화된 데이터 구조입니다. MIB는 대부분의 네트워크 디바이스에서 사용되는 제품, 프로토콜 및 하드웨어 표준으로 정의됩니다. SNMP 네트워크 관리 스테이션은 MIB를 찾아보고 특정 데이터나 이벤트 전송을 실시간으로 요청할 수 있습니다.
NMS(네트워크 관리 스테이션)	SNMP 이벤트를 모니터링하고 디바이스를 관리하도록 설정된 PC나 워크스테이션입니다.
OID(객체 식별자)	NMS에서 디바이스를 식별하고 사용자에게 모니터링 및 표시되는 정보의 소스를 보여주는 시스템입니다.
트랩	SNMP 에이전트에서 NMS로 메시지를 생성하는 사전 정의된 이벤트입니다. 이벤트는 linkup, linkdown, coldstart, warmstart, authentication 또는 syslog 메시지와 같은 경보 조건을 포함합니다.

MIB 및 트랩

MIB는 표준이거나 기업별로 구분됩니다. 표준 MIB는 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. 트랩은 네트워크 디바이스에서 발생하는 중요 이벤트(대부분 오류나 장애)를 보고합니다. SNMP 트랩은 표준 또는 기업별 MIB로 정의됩니다. 표준 트랩은 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. SNMP 트랩은 ASA 소프트웨어로 컴파일됩니다.

필요한 경우 다음 위치에서 RFC, 표준 MIB 및 표준 트랩을 다운로드할 수 있습니다.

http://www.ietf.org/

SNMP 개체 탐색기를 찾아 다음 위치에서 Cisco MIB, 트랩 및 OID를 찾습니다.

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

또한 다음 위치에서 FTP를 통해 Cisco OID를 다운로드할 수 있습니다.

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

MIB에서 지원되는 테이블 및 객체

다음 섹션에서는 지정된 MIB에 대해 지원되는 테이블 및 를 소개합니다.

원격 액세스 **VPN** 폴링

표 ***2: CISCO-REMOTE-ACCESS-MONITOR-MIB***

카운터	**OID**	설명
활성 세션	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	현재 활성 세션 수입니다.
사용자	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	활성 세션이 있는 사용자 수입니다.
최대 세션	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	시스템 가동 이후 최대 RA 세션 수입니다.

사이트 간 **VPN** 터널 폴링

표 ***3: CISCO-REMOTE-ACCESS-MONITOR-MIB***

카운터	**OID**	설명
LAN-LAN 세션	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	현재 활성 LAN-LAN 세션의 수입니다.
피크 LAN-LAN 세션	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	시스템 가동 이후 최대 동시 LAN-LAN 세션 수입니다.

연결 폴링

표 ***4: CISCO-FIREWALL-MIB***

카운터	**OID**	설명
활성 연결	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	전체 방화벽에서 현재 사용 중인 연결 수입니다.
최대 연결 수	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	시스템 가동 이후 한 번에 사용 중인 최대 연결 수입니다.

카운터	**OID**	설명
초당 연결 수	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	방화벽의 현재 초당 연결 수입니다.
초당 최대 연결 수	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	시스템 가동 이후 방화벽에서 초당 최대 연결 수입니다.

NAT 변환 폴링

표 ***5: CISCO-NAT-EXT-MIB***

카운터	**OID**	설명
활성 변환	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	NAT 디바이스에서 현재 사용 가능한 총 주소 변환 항목 수입니다. 정적 및 동적 주소 변환 메커니즘에서 생성된 변환 항목의 집계를 나타냅니다.
피크 활성 변환	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	시스템 가동 이후 한 번에 활성화된 주소 변환 항목의 최대 수입니다. 이는 시스템 가동 이후 한 번에 활성화된 주소 변환 항목의 상위 워터마크를 나타냅니다. 이 개체는 정적 및 동적 주소 변환 메커니즘에서 생성된 변환 항목을 포함합니다.

라우팅 테이블 항목 폴링

표 ***6: IP-FORWARD-MIB***

카운터	**OID**	설명
활성 변환	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	유효한 현재 inetCidrRouteTable 항목의 총계입니다.

인터페이스 듀플렉스 상태 폴링

표 *7: CISCO-IF-EXTENSION-MIB*

카운터	**OID**	설명
듀플렉스 상태	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	이 개체는 지정된 인터페이스에서 구성된 양방향 상태를 지정합니다.
탐지된 듀플렉스 상태	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	이 개체는 지정된 인터페이스에서 탐지된 양방향 상태를 지정합니다.

Snort 3 침입 이벤트 속도 폴링

표 *8: CISCO-UNIFIED-FIREWALL-MIB*

카운터	**OID**	설명
Snort 3 침입 이벤트 속도	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	지난 300초 동안 Snort가 이 방화벽에서 기록한 침입 이벤트의 평균 속도입니다.

BGP 피어 플랩 트랩 알림

표 *9: BGP4-MIB*

카운터	**OID**	설명
BGP 피어 플랩	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	BGP FSM이 번호가 높은 상태에서 번호가 낮은 상태로 이동할 때 BGPBackwardTransition 이벤트가 생성됩니다.

참고 CPU 모니터링(hrProcessorTable 및 hrNetworkTable)과 관련된 SNMP OID 1.3.6.1.2.1.25.3.3 및 1.3.6.1.2.1.25.3.4가 ASA FirePOWER에서 제거되었습니다. 디바이스 관리자를 통해서만 디바이스의 CPU 상태 세부 정보를 보고 모니터링할 수 있습니다.

SNMPv3 사용자 추가

참고 SNMPv3에 대해서만 사용자를 생성합니다. 이러한 단계는 SNMPv1 또는 SNMPv2c에 적용할 수 없습니다.

SNMPv3는 읽기 전용 사용자만 지원합니다.

SNMP 사용자는 지정된 사용자 이름, 인증 비밀번호, 암호화 비밀번호 및 승인, 그리고 사용할 암호화 알고리즘을 가져야 합니다.

참고 클러스터링 또는 고가용성과 함께 SNMPv3를 사용할 때 초기 클러스터 형성 후 또는 고가용성 유닛을 교체한 후 새 클러스터 유닛을 추가하면 SNMPv3 사용자가 새 유닛에 복제되지 않습니다. 사용자를 제거하고 다시 추가한 다음 사용자가 새 유닛에 복제하도록 강제로 구성을 재구축해야 합니다.

인증 알고리즘 옵션은 MD5(사용되지 않음. 6.5 이전만 해당), SHA, SHA224, SHA256 및 SHA384입니다.

참고 MD5 옵션은 더 이상 사용되지 않습니다. 6.5 이전 버전을 사용하여 생성된 MD5 인증 알고리즘을 사용하는 SNMP v3 사용자가 구축에 포함된 경우, 6.7 이하 버전을 실행하는 FTD에 해당 사용자를 계속 사용할 수 있습니다. 그러나 이러한 사용자를 편집하고 MD5 인증 알고리즘을 유지할 수 없으며, MD5 인증 알고리즘을 사용하여 새 사용자를 생성할 수는 없습니다. management center에서 버전 7.0 이상을 실행하는 threat defense를 관리하는 경우 MD5 인증 알고리즘을 사용하는 플랫폼 설정 정책을 해당 threat defense에 구축할 수 없습니다.

암호화 알고리즘 옵션은 DES(더 이상 사용되지 않음, 6.5 이전만 해당), 3DES, AES256, AES192 및 AES128입니다.

참고 DES 옵션은 더 이상 사용되지 않습니다. 6.5 이전 버전을 사용하여 생성한 DES 암호화를 사용하는 SNMP v3 사용자가 구축에 포함된 경우, 6.7 이하 버전을 실행하는 threat defense에 대해 해당 사용자를 계속 사용할 수 있습니다. 그러나 이러한 사용자를 수정하고 DES 암호화를 유지하거나 DES 암호화를 사용하여 새 사용자를 생성할 수는 없습니다. management center에서 버전 7.0 이상을 실행하는 threat defense를 관리하는 경우 DES 암호화를 사용하는 플랫폼 설정 정책을 해당 threat defense에 구축할 수 없습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **SNMP** > **Users(**사용자**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** **Security Level(**보안 수준**)** 드롭다운 목록에서 사용자의 보안 수준을 선택합니다.

- **Auth** - Authentication but No Privacy(인증 있음 및 개인정보 보호 없음)로 메시지가 인증을 받음을 의미합니다.
- **No Auth** - No Authentication and No Privacy(인증 없음 및 개인정보 보호 없음)로 메시지에 보안이 적용되지 않음을 의미합니다.
- **Priv** - Authentication and Privacy(인증 있음 및 개인정보 보호 있음)로 메시지가 인증을 받고 암호화됨을 의미합니다.

단계 **5** **Username(**사용자 이름**)** 필드에 SNMP 사용자 이름을 입력합니다. 사용자 이름은 32자 이하여야 합니다.

단계 **6** **Encryption Password Type(**비밀번호 유형 암호화**)** 드롭다운 목록에서 사용할 비밀번호 유형을 선택합니다.

- **Clear text(**일반 텍스트**)** - threat defense 디바이스는 구축할 때 비밀번호를 계속 암호화합니다.
- **Encrypted(**암호화됨**)** - threat defense 디바이스는 암호화된 비밀번호를 직접 구축합니다.

단계 **7** **Auth Algorithm Type(**인증 알고리즘 유형**)** 드롭다운 목록에서 사용할 인증 유형 (SHA, SHA224, SHA256 또는 SHA384)을 선택합니다.

참고 MD5 옵션은 더 이상 사용되지 않습니다. 6.5 이전 버전을 사용하여 생성된 MD5 인증 알고리즘을 사용하는 SNMP v3 사용자가 구축에 포함된 경우, 6.7 이하 버전을 실행하는 FTD에 해당 사용자를 계속 사용할 수 있습니다. 그러나 이러한 사용자를 편집하고 MD5 인증 알고리즘을 유지할 수 없으며, MD5 인증 알고리즘을 사용하여 새 사용자를 생성할 수는 없습니다. management center에서 버전 7.0 이상을 실행하는 threat defense를 관리하는 경우 MD5 인증 알고리즘을 사용하는 플랫폼 설정 정책을 해당 threat defense에 구축할 수 없습니다.

단계 **8** **Authentication Password(**인증 비밀번호**)** 필드에 인증에 사용할 비밀번호를 입력합니다. Encryption Password Type(비밀번호 유형 암호화)으로 Encrypted(암호화됨)를 선택하면 비밀번호는 xx:xx:xx... 형식이어야 합니다. 여기서 xx는 16진수 값입니다.

참고 비밀번호의 길이는 선택한 인증 알고리즘에 따라 다릅니다. 모든 비밀번호의 길이는 256자 이하여야 합니다.

Encrypt Password Type(비밀번호 유형 암호화)로 Clear Text(일반 텍스트)를 선택한 경우, **Confirm(**확인**)** 필드에 암호를 반복합니다.

단계 **9** **Encryption Type(**암호화 유형**)**드롭다운 목록에서 사용할 암호화 유형을 선택합니다(AES128, AES192, AES256, 3DES 또는).

참고 AES 또는 3DES 암호화를 사용하려면 디바이스에 적절한 라이선스가 설치되어 있어야 합니다.

참고 DES 옵션은 더 이상 사용되지 않습니다. 6.5 이전 버전을 사용하여 생성한 DES 암호화를 사용하는 SNMP v3 사용자가 구축에 포함된 경우, 6.7 이하 버전을 실행하는 threat defense에 대해 해당 사용자를 계속 사용할 수 있습니다. 그러나 이러한 사용자를 수정하고 DES 암호화를 유지하거나 DES 암호화를 사용하여 새 사용자를 생성할 수는 없습니다. management center에서 버전 7.0 이상을 실행하는 threat defense를 관리하는 경우 DES 암호화를 사용하는 플랫폼 설정 정책을 해당 threat defense에 구축할 수 없습니다.

단계 **10** **Encryption Password(**암호화 비밀번호**)** 필드에 암호화에 사용할 비밀번호를 입력합니다. Encryption Password Type(암호화 비밀번호 유형)으로 Encrypted(암호화됨)를 선택하면 비밀번호는 xx:xx:xx... 형식이어야 합니다. 여기서 xx는 16진수 값입니다. 암호화된 비밀번호의 경우 길이는 선택한 암호화 유형에 따라 다릅니다. 비밀번호 크기는 다음과 같습니다(각 xx는 8진법).

- AES 128에는 16 8진수 필요
- AES 192에는 24 8진수 필요
- AES 25에는 32 8진수 필요
- 3DES에는 32 8진수 필요
- DES는 모든 크기일 수 있음

참고 모든 비밀번호의 길이는 256자 이하여야 합니다.

Encrypt Password Type(비밀번호 유형 암호화)로 Clear Text(일반 텍스트)를 선택한 경우, **Confirm(**확인**)** 필드에 암호를 반복합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SNMP 호스트 추가

Host(호스트)를 사용하여 SNMP 페이지의 SNMP 호스트 테이블에 항목을 추가하거나 편집합니다. 이 항목은 threat defense 디바이스에 액세스할 수 있는 SNMP 관리 스테이션을 나타냅니다.

최대 8192개의 호스트를 추가할 수 있습니다. 하지만 이 중 128개만 트랩에 사용할 수 있습니다.

시작하기 전에

SNMP 관리 스테이션을 정의하는 네트워크 개체가 존재하는지 확인합니다. **Device(**디바이스**)** > **Object Management(**개체 관리**)**를 선택하여 네트워크 개체를 구성합니다.

참고 지원되는 네트워크 개체에는 IPv6 호스트, IPv4 호스트, IPv4 범위 및 IPv4 서브넷 주소가 포함됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **SNMP** > **Hosts(**호스트**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** **IP Address(IP** 주소**)**필드에 유효한 IPv6 또는 IPv4 호스트를 입력하거나 SNMP 관리 스테이션의 호스트 주소를 정의하는 네트워크 개체를 선택합니다.

IP 주소는 IPv6 호스트, IPv4 호스트, IPv4 범위 또는 IPv4 서브넷일 수 있습니다.

단계 **5** **SNMP version(SNMP** 버전**)** 드롭다운 목록에서 적절한 SNMP 버전을 선택합니다.

단계 **6** (SNMPv3만 해당) **User Name(**사용자 이름**)** 드롭다운 목록에서 구성한 SNMP 사용자의 사용자 이름을 선택합니다.

참고 SNMP 호스트당 최대 23명의 SNMP 사용자를 연결할 수 있습니다.

단계 **7** (SNMPv1, 2c만 해당) **Read Community String(**읽기 커뮤니티 문자열**)** 필드에 디바이스에 대한 읽기 액세스용으로 이미 구성한 커뮤니티 문자열을 입력합니다. 문자열을 다시 입력하여 확인합니다.

참고 이 문자열은 이 SNMP 스테이션에서 사용된 문자열이 **Enable SNMP Server(SNMP** 서버 활성화**)** 섹션에서 사전 정의된 문자열과 다른 경우에만 필요합니다.

단계 **8** 디바이스 및 SNMP 관리 스테이션 간의 통신 유형을 선택합니다. 두 유형을 선택할 수 있습니다.

- **Poll** - 관리 스테이션이 주기적으로 디바이스의 정보를 요청합니다.
- **Trap** - 디바이스가 트랩 이벤트를 발생하면 관리 스테이션으로 전송합니다.

참고 SNMP 호스트 IP 주소가 IPv4 범위 또는 IPv4 서브넷일 때 **Poll** 또는 **Trap** 중 하나만 구성할 수 있으며 둘 다를 구성할 수는 없습니다.

단계 **9** **Port(**포트**)** 필드에 SNMP 호스트에 대한 포트 번호를 입력합니다. 기본값은 162입니다. 유효한 범위는 1 ~65535입니다.

단계 **10** **Reachable By(**연결 방법**)** 옵션 아래에서 디바이스 및 SNMP 관리 스테이션 간의 통신을 위한 인터페이스 유형을 선택합니다. 디바이스의 관리 인터페이스 또는 사용 가능한 보안 영역/명명된 인터페이스를 선택할 수 있습니다.

- 디바이스 관리 인터페이스 - 디바이스와 SNMP 관리 스테이션 간의 통신은 관리 인터페이스를 통해 수행됩니다.
  - SNMPv3 폴링에 대해 이 인터페이스를 선택하면 구성된 모든 SNMPv3 사용자가 폴링할 수 있으며 단계 6, 34 페이지 단계에서 선택한 사용자로 제한되지 않습니다. 여기서 SNMPv1 및 SNMPv2c는 SNMPv3 호스트에서 허용되지 않습니다.

- SNMPv1 및 SNMPv2c 폴링에 대해 이 인터페이스를 선택하면 폴링이 단계 5, 34 페이지 단계에서 선택한 버전으로 제한되지 않습니다.

- 보안 영역 또는 명명된 인터페이스 - 디바이스와 SNMP 관리 스테이션 간의 통신은 보안 영역 또는 인터페이스를 통해 수행됩니다.
  - **Available Zones(**사용 가능한 영역**)** 필드에서 영역을 검색합니다.
  - **Selected Zones/Interfaces(**선택된 영역/인터페이스**)** 필드에서 디바이스가 관리 스테이션과 통신하는 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Zone/Interface(**선택한 영역/ 인터페이스**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 선택한 인터페이스 또는 영역이 디바이스에 포함되어 있는 경우에만 디바이스에서 호스트가 구성됩니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

SNMP 트랩 구성

SNMP Traps(SNMP 트랩)을 사용하여 threat defense 디바이스에 대한 SNMP 트랩(이벤트 알림)을 구성합니다. 트랩은 찾아보기와 다릅니다. 이는 linkup, linkdown 및 syslog 이벤트 생성과 같은 특정 이벤트에 대해 threat defense 디바이스에서 관리 스테이션으로의 요청되지 않은 "코멘트"입니다. 디바이스 SNMP 개체 ID(OID)가 디바이스에서 보낸 SNMP 이벤트 트랩에 나타납니다.

일부 트랩은 특정 하드웨어 모델에 적용됩니다. 이러한 모델 중 하나에 정책을 적용하면 이러한 트랩은 무시됩니다. 예를 들어 모든 모델에 현장 교체 가능한 디바이스가 있는 것은 아니므로 해당 모델에 **Field Replaceable Unit Insert/Delete** 트랩이 구성되지 않습니다.

SNMP 트랩은 표준 또는 기업별 MIB로 정의됩니다. 표준 트랩은 IETF에 의해 생성되며 다양한 RFC에 문서화되어 있습니다. SNMP 트랩은 threat defense 소프트웨어로 컴파일됩니다.

필요한 경우 다음 위치에서 RFC, 표준 MIB 및 표준 트랩을 다운로드할 수 있습니다.

http://www.ietf.org/

다음 위치에서 Cisco MIB, 트랩 및 OID의 전체 목록을 검색하십시오.

SNMP Object Navigator

또한 다음 위치에서 FTP를 통해 Cisco OID를 다운로드할 수 있습니다.

ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **SNMP** > **SNMP Traps(SNMP** 트랩**)**을 클릭하여 threat defense 디바이스에 대한 SNMP 트랩(이벤트 알림)을 구성합니다.

단계 **3** 적절한 Enable Traps(트랩 활성화) 옵션을 선택합니다. 옵션 중 하나 또는 두 가지를 선택할 수 있습니다.

a) 이후의 네 섹션에서 모든 트랩을 빠르게 선택하려면 **Enable All SNMP Traps(**모든 **SNMP** 트랩 활성화**)**를 선택합니다.

b) 트랩 관련 syslog 메시지 전송을 활성화하려면 **Enable All Syslog Traps(**모든 **Syslog** 트랩 활성화**)**를 선택합니다.

참고 SNMP 트랩은 실시간에 가까울 것으로 예상되는 threat defense의 다른 알림 메시지보다 우선 순위가 높습니다. 모든 SNMP 또는 syslog 트랩을 활성화하면 SNMP 프로세스가 에이전트 및 네트워크에서 초과 리소스를 소비하여 시스템이 중단될 수 있습니다. 시스템 지연, 완료되지 않은 요청 또는 시간 초과가 있는 경우 SNMP 및 syslog 트랩을 선택적으로 활성화할 수 있습니다. 심각도 수준 또는 메시지 ID별로 syslog 메시지가 생성되는 속도를 제한할 수도 있습니다. 예를 들어 212로 시작하는 모든 syslog 메시지 ID는 SNMP 클래스와 연결되어 있습니다. Syslog 메시지 생성 속도 제한, 50 페이지 섹션을 참조하십시오.

단계 **4** **Standard(**표준**)** 섹션의 이벤트 알림 트랩은 기본적으로 기존 정책에 대해 활성화됩니다.

- **Authentication(**인증**)** - 무단 SNMP 액세스입니다. 이 인증 실패는 잘못된 커뮤니티 문자열이 있는 패킷에 대해 발생합니다.
- **Link Up(**링크업**)** - 알림에 표시된 대로 디바이스의 통신 링크 중 하나를 사용할 수 있습니다.
- **Link Down(**링크다운**)** - 알림에 표시된 대로 디바이스의 통신 링크 중 하나가 실패했습니다.
- **Cold Start(**콜드 스타트**)** - 디바이스가 다시 초기화하고 있거나, 프로토콜 엔티티 구현이 변경될 수 있습니다.
- **Warm Start(**웜 스타트**)** - 디바이스 자체 구성 또는 프로토콜 엔티티 구현이 변경될 수 있도록 다시 초기화하고 있습니다.

단계 **5** **Entity MIB** 섹션에서 원하는 이벤트 알림 트랩을 선택합니다.

- **Field Replaceable Unit Insert(**현장 교체 가능 디바이스 삽입**)** - 현장 교체 가능 디바이스(FRU)가 표시된 대로 삽입되었습니다. (FRU에는 전원 공급 장치, 팬, 프로세서 모듈, 인터페이스 모듈 등과 같은 어셈블리가 포함됩니다.)
- **Field Replaceable Unit Delete(**현장 교체 가능 디바이스 삭제**)** - 현장 교체 가능 디바이스(FRU)가 알림에 표시된 대로 제거되었습니다.
- **Configuration Change(**구성 변경**)** - 알림에 표시된 대로 하드웨어가 변경되었습니다.

단계 **6** **Resource(**리소스**)** 섹션에서 원하는 이벤트 알림 트랩을 선택합니다.

- **Connection Limit Reached(**연결 제한 도달**)** - 이 트랩은 구성된 연결 제한에 도달했기 때문에 연결 시도가 거부되었음을 나타냅니다.

단계 **7** **Other(**기타**)** 섹션에서 원하는 이벤트 알림 트랩을 선택합니다.

- **NAT Packet Discard(NAT** 패킷 폐기**)** - 이 알림은 IP 패킷이 NAT 기능에 의해 폐기될 때 생성됩니다. 사용 가능한 네트워크 주소 변환 주소 또는 포트가 구성된 임계값 아래로 하락함
- **CPU Rising Threshold(CPU** 상승 임계값**)**-이 알림은 CPU 사용률 상승이 구성된 기간 동안 사전 정의된 임계값을 초과할 때 생성됩니다. CPU 상승 임계값 알림을 활성화하려면 이 옵션을 선택합니다.
  - **Percentage(**백분율**)**-높은 임계값 알림의 기본값은 70%입니다. 범위는 10% ~ 94%입니다. 중요 임계값은 95%로 하드 코딩됩니다.
  - **(Period)**기간-기본 모니터링 기간은 1분입니다. 범위는 1 ~ 60분입니다.
- **Memory Rising Threshold(**메모리 상승 임계값**)**-이 알림은 메모리 사용률이 미리 정의된 임계값을 초과하여 사용 가능한 메모리가 감소하면 생성됩니다. 메모리 상승 임계값 알림을 활성화하려면 이 옵션을 선택합니다.
  - **Percentage(**백분율**)**-높은 임계값 알림의 기본값은 70%입니다. 범위는 50% ~ 95%입니다.
- **Failover(**페일 오버**)** –이 알림은 CISCO-UNIFIED-FIREWALL-MIB에서 보고한 페일오버 상태가 변경되면 생성됩니다.
- **Cluster(**클러스터**)**-이 알림은 CISCO-UNIFIED-FIREWALL-MIB에서 보고한 대로 클러스터 상태가 변경되면 생성됩니다.
- **Peer Flap(**피어 플랩**)** – 이 알림은 BGP 경로 플랩이 있을 때 생성되며, BGP 시스템이 네트워크 연결성 정보를 알리기 위해 과도한 수의 업데이트 메시지를 전송하는 상황입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Syslog 설정

threat defense 디바이스에 대한 시스템 로그를 활성화할 수 있습니다. 기록 정보는 네트워크 또는 디바이스 구성 관련 문제를 식별하고 격리하는 데 도움이 됩니다. 일부 보안 이벤트를 시스템 로그 서버에 전송할 수도 있습니다. 다음 주제에서는 기록 및 기록을 구성하는 방법에 대해 설명합니다.

Syslog 정보

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다. Cisco 디바이스는 로그 메시지를 UNIX 스타일 syslog 서비스로 전송할 수 있습니다. syslog 서비스는 메시지를 수신하고 파일로 저장하거나 간단한 구성 파일에 따라 인쇄합니다. 이 로깅 양식을 통해 로그를 안전하게 장기 보관할 수 있습니다. 로그는 일상적인 문제 해결과 인시던트 처리에 모두 유용합니다.

표 ***10:*** 시스템 로그 ***Secure Firewall Threat Defense***

관련 로그	세부 사항	구성
디바이스 및 시스템 상태, 네트워크 구성	이 syslog 구성에서는 데이터 플레인에서 실행되는 기능, 즉 **show running-config** 명령으로 볼 수 있는 CLI 구성에 정의된 기능에 대해 메시지를 생성합니다. 여기에는 라우팅, VPN, 데이터 인터페이스, DHCP 서버, NAT 등과 같은 기능이 포함됩니다. 데이터 플레인 syslog 메시지는 번호가 매겨지며 ASA 소프트웨어를 실행하는 디바이스에서 생성된 메시지와 동일합니다. 하지만 Secure Firewall Threat Defense는 ASA 소프트웨어에 사용할 수 있는 모든 메시지 유형을 생성하지는 않습니다. 이 메시지에 대한 정보는 https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html의 *Cisco Secure Firewall Threat Defense Syslog* 메시지를 참조하십시오. 이 구성은 다음 주제에서 설명됩니다.	플랫폼 설정
보안 이벤트	이 syslog 구성은 파일 및 악성코드, 연결, 보안 인텔리전스 및 침입 이벤트에 대한 알림을 생성합니다.	액세스 제어 정책의 **Platform Settings(**플랫폼 설정**)** 및 **Logging(**로깅**)**
(모든 디바이스) 정책, 규칙 및 이벤트	이 시스템 로그 구성은 Cisco Secure Firewall Management Center 관리 가이드의 알림 응답 지원 구성에서 설명한 대로 액세스 제어 규칙, 침입 규칙 및 기타 고급 서비스에 대한 알림을 생성합니다. 이러한 메시지에 번호가 매겨지지는 않습니다. 이 유형의 시스템 로그 구성에 대한 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 시스템 로그 알림 응답 생성의 내용을 참조하십시오.	액세스 제어 정책의 **Alert Responses(**알림 응답**)** 및 **Logging(**로깅**)**

두 개 이상의 syslog 서버를 구성하고 각 서버로 전송되는 메시지 및 이벤트를 제어할 수 있습니다. 콘솔, 이메일, 내부 버퍼 등과 같은 다른 대상을 구성할 수도 있습니다.

심각도 레벨

다음 표는 syslog 메시지 심각도 수준을 나열합니다.

표 ***11: Syslog*** 메시지 심각도 레벨

레벨 번호	심각도 레벨	설명
0	**emergencies(**비상**)**	시스템을 사용할 수 없습니다.
1	**Alert(**긴급 경고**)**	즉각적인 행동이 필요합니다.
2	**critical(**심각**)**	심각한 상태입니다.
3	**error(**오류**)**	오류 상태입니다.
4	**warning(**경고**)**	경고 상태입니다.
5	**notification(**알림**)**	일반적이지만 중요한 상태입니다.
6	**informational(**정보**)**	정보 메시지만 해당됩니다.
7	**debugging(**디버깅**)**	디버깅 메시지만 해당됩니다. 문제를 디버깅할 때 이 레벨에서 일시적으로만 기록합니다. 이 로그 레벨은 시스템 성능에 영향을 미칠 수 있는 메시지를 너무 많이 생성할 수 있습니다.

참고 ASA 및 Threat Defense은 심각도 레벨 0(응급)으로 시스템 로그 메시지를 생성하지 않습니다.

Syslog 메시지 필터링

특정 syslog 메시지만 특정 출력 대상에 전송되도록 생성된 syslog 메시지를 필터링할 수 있습니다. 예를 들어 모든 syslog 메시지를 하나의 출력 대상으로 전송하고 이 syslog 메시지의 하위 집합을 다른 출력 대상으로 보내도록 위협 방지 디바이스를 구성할 수 있습니다.

구체적으로 syslog 메시지가 다음 기준에 따라 출력 대상으로 전송되도록 지시할 수 있습니다.

- Syslog 메시지 ID 번호

  (이 번호는 연결 및 침입 이벤트 같은 보안 이벤트에 대한 syslog 메시지에 적용되지 않습니다.)

- Syslog 메시지 심각도 레벨
- Syslog 메시지 클래스(기능 영역에 해당)

  (이 번호는 연결 및 침입 이벤트 같은 보안 이벤트에 대한 syslog 메시지에 적용되지 않습니다.)

출력 대상을 설정할 때 지정할 수 있는 메시지 목록을 생성함으로써 이 기준을 사용자 정의할 수 있습니다. 또는 특정 메시지 클래스를 메시지 목록과는 별개로 각 출력 대상 유형으로 전송하도록 위협 방지 디바이스를 구성할 수도 있습니다.

(메시지 목록은 연결 및 침입 이벤트 같은 보안 이벤트에 대한 syslog 메시지에 적용되지 않습니다.)

Syslog 메시지 클래스

참고 이 주제는 보안 이벤트(예: 연결, 침입 등)에 대한 메시지에 적용되지 않습니다.

syslog 메시지 클래스를 2가지 방법으로 사용할 수 있습니다.

- 전체 syslog 메시지 카테고리에 대한 출력 위치를 지정합니다. **logging class** 명령을 사용합니다.
- 메시지 클래스를 지정하는 메시지 목록을 생성합니다. **logging list** 명령을 사용합니다.

syslog 메시지 클래스는 디바이스의 기능에 해당하는 유형에 따라 syslog 메시지를 분류하는 방식을 제공합니다. 예를 들어 rip 클래스는 RIP 라우팅을 나타냅니다.

특정 클래스의 모든 syslog 메시지는 syslog 메시지 ID 번호의 첫 3자리가 같습니다. 예를 들어 611로 시작하는 모든 syslog 메시지 ID는 vpnc(VPN 클라이언트)와 연결되어 있습니다. VPN 클라이언트 기능에 연결된 syslog 메시지는 611101부터 611323까지입니다.

또한 대부분의 ISAKMP syslog 메시지는 터널 식별을 돕는 공통의 접두사가 있는 객체 세트를 갖습니다. 이러한 객체가 있는 경우 syslog 메시지의 설명 텍스트 앞에 위치합니다. syslog 메시지가 생성되는 시점에 객체를 알 수 없는 경우 구체적인 heading = value 조합은 표시되지 않습니다.

객체는 다음과 같이 접두사가 붙습니다.

그룹 = *groupname*, 사용자 이름 = *user*, IP = *IP_address*

그룹이 터널-그룹인 경우 사용자 이름은 로컬 데이터베이스 또는 AAA 서버의 사용자 이름이고 IP 주소는 원격 액세스 클라이언트 또는 레이어 2 피어의 공용 IP 주소입니다.

다음 표에는 메시지 클래스와 각 클래스의 메시지 ID 범위가 나와 있습니다.

표 ***12: Syslog*** 메시지 클래스와 연결된 메시지 ***ID*** 번호

클래스	정의	**Syslog** 메시지 **ID** 번호
auth	사용자 인증	109, 113
—	액세스 목록	106
—	애플리케이션 방화벽	415
bridge	투명한 방화벽	110, 220
ca	PKI 인증 기관	717
citrix	Citrix 클라이언트	723
—	클러스터링	747

클래스	정의	**Syslog** 메시지 **ID** 번호
—	카드 관리	323
config	CLI(Command Line Interface)	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policy	734
eap, eapoudp	Network Admission Control용 EAPoUDP 또는 EAP	333, 334
eigrp	EIGRP 라우팅	336
email	이메일 프록시	719
—	환경 모니터링	735
HA	페일오버	101, 102, 103, 104, 105, 210, 311, 709
—	ID 기반 방화벽	746
ids	Intrusion Detection System(침입 탐지 시스템)	400, 733
—	IKEv2 툴킷	750, 751, 752
ip	IP 스택	209, 215, 313, 317, 408
ipaa	IP 주소 할당	735
ips	Intrusion Protection System(침입 방지 시스템)	400, 401, 420
—	IPv6	325
—	봇넷 트래픽 필터링	338
—	라이선싱	444
mdm-proxy	MDM 프록시	802
nac	NAC(Network Admission Control)	731, 732
nacpolicy	NAC 정책	731
nacsettings	NAC 정책을 적용할 NAC 설정	732
—	네트워크 액세스 포인트	713
np	네트워크 프로세서	319
—	NP SSL	725

클래스	정의	**Syslog** 메시지 **ID** 번호
ospf	OSPF 라우팅	318, 409, 503, 613
—	비밀번호 암호화	742
—	전화 프록시	337
rip	RIP 라우팅	107, 312
rm	리소스 관리자	321
—	Smart Call Home	120
session	사용자 세션	204, 302, 303, 304, 202 305, 314 및 405, 108, 201, 406 및/또는/또는//407/106
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL 스택	725
svc	SSL VPN 클라이언트	722
sys	시스템	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	위협 탐지	733
tre	트랜잭션 규칙 엔진	780
—	UC-IME	339
tag-switching	서비스 태그 스위칭	779
VM	VLAN 매핑	730
vpdn	PPTP 및 L2TP 세션	213, 403, 603
vpn	IKE 및 IPSEC	316, 320, 404, 501, 602, 402
vpnc	VPN 클라이언트	611
vpnfo	VPN 페일오버	720
vpnlb	VPN 로드 밸런싱	718
—	VXLAN	778
webfo	WebVPN 페일오버	721

클래스	정의	**Syslog** 메시지 **ID** 번호
webvpn	WebVPN 및 AnyConnect Client	716
—	NAT 및 PAT	305

로깅 지침

이 섹션에는 로깅을 구성하기 전에 검토해야 할 지침 및 제한사항이 포함되어 있습니다.

IPv6 지침

- IPv6가 지원됩니다. TCP 또는 UDP를 사용하여 Syslog를 전송할 수 있습니다.
- Syslogs 전송에 대해 구성된 인터페이스가 활성화되어 있으며 IPv6를 지원 가능하며 syslog 서버에 지정된 인터페이스를 통해 연결할 수 있는지 확인합니다.
- IPv6를 통한 보안 로깅은 지원되지 않습니다.

추가 지침

- management center를 기본 시스템 로그 서버로 구성하지 마십시오. management center는 일부 시스템 로그를 로깅할 수 있습니다. 그러나 모든 센서에 대한 연결 이벤트의 방대한 정보를 수용할 수 있는 적절한 스토리지 프로비저닝이 없습니다. 특히 여러 센서를 사용하고 모두 시스템 로그를 전송하는 경우에는 더욱 그렇습니다.
- syslog 서버는 syslogd라는 서버 프로그램을 실행해야 합니다. Windows 운영 체제에는 syslog 서버가 포함되어 있습니다.
- 위협 방지 디바이스에서 생성된 로그를 보려면 로깅 출력 대상을 지정해야 합니다. 로깅 출력 대상을 지정하지 않고 로깅을 활성화하면 위협 방지 디바이스는 메시지를 생성하지만 메시지를 볼 수 있는 위치에 저장하지 않습니다. 각 다른 로깅 출력 대상을 별도로 지정해야 합니다.
- TCP를 전송 프로토콜로 사용하는 경우 시스템은 메시지가 손실되지 않도록 syslog 서버에 대한 4개의 연결을 엽니다. syslog 서버를 사용하여 매우 많은 수의 디바이스에서 메시지를 수집하는 경우 결합된 연결 오버헤드가 서버에 비해 너무 많은 경우 UDP를 대신 사용합니다.
- 두 개의 서로 다른 목록 또는 다른 syslog 서버 또는 동일한 위치에 할당 중인 클래스를 갖는 것은 불가능합니다.
- 최대 16개의 syslog 서버를 구성할 수 있습니다.
- syslog 서버는 위협 방지 디바이스를 통해 연결할 수 있습니다. syslog 서버가 연결할 수 없는 인터페이스의 ICMP 연결 불가 메시지를 거부하고 syslog를 동일한 서버로 전송하도록 디바이스를 구성할 수 있습니다. 모든 심각도 레벨에 대해 로깅을 활성화했는지 확인합니다. syslog 서버가 충돌하지 않게 하려면 syslogs 313001, 313004 및 313005의 생성을 억제합니다.
- syslog에 대한 UDP 연결 수는 하드웨어 플랫폼의 CPU 수 및 구성한 syslog 서버 수와 직접 관련이 있습니다. 어느 시점이든 CPU에는 구성된 syslog 서버의 수와 동일한 수의 UDP syslog 연결이

있을 수 있습니다. 이는 정상적인 동작입니다. 전역 UDP 연결 유휴 시간 초과가 이 세션에 적용되며 기본값은 2분입니다. 이러한 세션을 더욱 신속하게 종료하려면 설정을 조정할 수 있지만 시간 초과는 syslog 뿐만 아니라 모든 UDP 연결에 적용됩니다.

- TCP를 통해 위협 방지 디바이스가 syslogs를 전송할 때 syslogd 서비스가 재시작된 후에 연결을 초기화하는 데 약 1분 이상이 걸릴 수 있습니다.

FTD 디바이스에 대한 Syslog 로깅 구성

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 시스템 로그 메시지에 적용되는 Threat Defense 플랫폼 설정, 45 페이지의 내용을 참조하십시오.

syslog 설정을 구성하려면 다음 단계를 수행합니다.

시작하기 전에

로깅 지침, 43 페이지의 요구 사항을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** 목차에서 **Syslog**를 클릭합니다.

단계 **3** 로깅을 활성화하고 FTP 서버 설정을 지정하고 플래시 사용을 지정하려면 **Logging Setup(**로깅 설정**)**을 클릭합니다. 자세한 내용은 로깅 활성화 및 기본 설정, 45 페이지을 참조해 주십시오.

단계 **4** 특정 대상에 대한 로깅을 활성화하고 메시지 심각도 레벨, 이벤트 클래스 또는 사용자 지정 이벤트 목록에 대한 필터링을 지정하려면 **Logging Destinations(**로깅 대상**)**를 클릭합니다. 자세한 내용은 로깅 대상 활성화, 47 페이지을 참조해 주십시오.

로깅 대상을 활성화하여 해당 대상에서 메시지를 볼 수 있도록 해야 합니다.

단계 **5** 이메일 메시지로 전송되는 시스템 로그 메시지의 소스 주소로 사용할 이메일 주소를 지정하려면 **E-mail Setup(**이메일 설정**)**을 클릭합니다. 자세한 내용은 이메일 주소로 Syslog 메시지 전송, 48 페이지을 참조해 주십시오.

단계 **6** **Events List(**이벤트 목록**)**를 클릭하여 이벤트 클래스, 심각도 레벨 및 이벤트 ID를 포함하는 사용자 지정 이벤트 목록을 정의합니다. 자세한 내용은 사용자 지정 이벤트 목록 생성, 49 페이지을 참조해 주십시오.

단계 **7** **Rate Limit(**속도 제한**)**을 클릭하여 구성된 모든 대상에 전송되는 메시지의 양을 지정하고 속도 제한을 할당할 메시지 심각도 레벨을 정의합니다. 자세한 내용은 Syslog 메시지 생성 속도 제한, 50 페이지을 참조해 주십시오.

단계 **8** **Syslog Settings(**시스템 로그 설정**)**를 클릭하여 로깅 기능을 지정하고 타임스탬프 추가를 활성화하며, 다른 설정을 활성화하여 서버를 시스템 로그 대상으로 설정합니다. 자세한 내용은 Syslog 설정, 51 페이지을 참조해 주십시오.

단계 **9** **Syslog Servers(**시스템 로그 서버**)**를 클릭하여 로깅 대상으로 지정된 시스템 로그 서버의 IP 주소, 사용된 프로토콜, 형식 및 보안 영역을 지정합니다. 자세한 내용은 Syslog 서버 설정, 53 페이지을 참조해 주십시오.

보안 이벤트 시스템 로그 메시지에 적용되는 **Threat Defense** 플랫폼 설정

'보안 이벤트'에는 연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트가 포함됩니다.

Devices(디바이스**) > Platform Settings(**플랫폼 설정**) > Threat Defense Settings(Threat Defense** 설정**) > Syslog(**시스템 로그**)** 페이지 및 해당 탭의 일부 시스템 로그 설정은 보안 이벤트에 대한 시스템 로그 메시지에 적용되지만, 대부분은 시스템 상태 및 네트워킹 관련 이벤트용 메시지에만 적용됩니다.

보안 이벤트에 대한 시스템 로그 메시지에는 다음 설정이 적용됩니다.

- **Logging Setup(**로깅 설정**)** 탭:
  - **EMBLEM** 형식으로 **syslog** 전송
- **Syslog Settings(Syslog** 설정**)** 탭:
  - **Syslog** 메시지에서 타임스탬프 활성화
  - 타임스탬프 형식
  - **Syslog** 디바이스 **ID** 활성화
- **Syslog Servers(Syslog** 서버**)** 탭:
  - **Add Syslog Server(Syslog** 서버 추가**)** 양식(및 구성된 서버 목록)의 모든 옵션

로깅 활성화 및 기본 설정

시스템에서 데이터 플레인 이벤트에 대한 syslog 메시지를 생성하려면 로깅을 활성화해야 합니다.

또한 로컬 버퍼가 가득 차면 플래시 또는 FTP 서버를 스토리지 위치로 설정할 수 있습니다. 로깅 데이터를 저장한 후에 조작할 수 있습니다. 예를 들어 특정 유형의 syslog 메시지가 기록될 때 실행할 작업을 지정하고, 로그에서 데이터를 추출하고 보고를 위해 기록을 다른 파일에 저장하거나, 사이트별 스크립트를 사용하여 통계를 추적할 수 있습니다.

다음 절차에서는 몇 가지 기본 syslog 설정에 관해 설명합니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 threat defense 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 시스템 로그 메시지에 적용되는 Threat Defense 플랫폼 설정, 45 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Syslog** > **Logging Setup(**로깅 설정**)**을 선택합니다.

단계 **3** 로깅을 활성화하고 기본 로깅 설정을 구성합니다.

- **Enable Logging(**로깅 활성화**)** - threat defense 디바이스의 데이터 플레인 시스템 로깅을 켭니다.
- **Enable Logging on the Failover Standby Unit(**장애 조치 대기 유닛에서 로깅 활성화**)** - 가능한 경우 threat defense 디바이스에 대한 대기 로깅을 켭니다.
- **Send syslogs in EMBLEM format(EMBLEM** 형식으로 **syslog** 전송**)** - 모든 로깅 대상에 대해 EMBLEM 형식 로깅을 활성화합니다. EMBLEM을 활성화하면 UDP 프로토콜을 사용하여 syslog 메시지를 게시해야 합니다. EMBLEM은 TCP와 호환되지 않습니다.

  참고 RFC5424 형식의 시스템 로그 메시지는 일반적으로 우선순위 값(PRI)을 표시합니다. 그러나 management center에서 관리되는 threat defense의 syslog 메시지에 PRI 값을 표시하려면 EMBLEM 형식을 활성화해야 합니다. PRI에 대한 자세한 내용은 RFC5424를 참조하십시오.

- **Send debug messages as syslogs(**디버그 메시지를 **syslog**로 전송**)** - 모든 디버그 추적 출력을 syslog로 리디렉션합니다. 이 옵션이 활성화되어 있으면 syslog 메시지가 콘솔에 표시되지 않습니다. 따라서 디버그 메시지를 보려면 콘솔에서 로깅을 활성화하고 디버그 syslog 메시지 번호 및 로깅 레벨에 대한 대상으로 구성해야 합니다. 사용할 syslog 메시지 번호는 711001입니다. 이 syslog의 기본 로깅 레벨은 디버그입니다.
- **Memory Size of Internal Buffer(**내부 버퍼의 메모리 크기**)** - 버퍼를 활성화한 경우 syslog 메시지가 저장되는 내부 로그 버퍼의 크기를 지정합니다. 버퍼는 가득 차면 덮어쓰기됩니다. 기본값은 4096바이트입니다. 범위는 4096~52428800입니다.

단계 **4** (선택 사항) **Enable Logging to Secure Firewall Management Center(Secure Firewall Management Center**에 로깅 활성화**)** 확인란을 선택하여 VPN 로깅을 활성화합니다. **Logging level(**로깅 레벨**)** 드롭다운 목록에서 VPN 메시지의 syslog 심각도 레벨을 선택합니다.

VPN 문제 해결 시스템 로그는 management center에 과도한 로드를 추가할 수 있습니다. 따라서 이 옵션은 주의해서 활성화하십시오. 또한 사이트 간 또는 원격 액세스 VPN을 사용하여 디바이스를 구성하면 기본적으로 VPN 시스템 로그를 관리 센터로 전송할 수 있습니다. 기본 로깅 레벨은 Error(오류)입니다. 시스템 로그의 과도한 흐름을 management center로 제한하려면 로깅 레벨을 Error(오류) 이상으로 제한하는 것이 좋습니다(특히 여러 디바이스가 관련된 RAVPN의 경우).

레벨에 대한 자세한 내용은 심각도 레벨, 38 페이지 섹션을 참조하십시오.

단계 **5** (선택 사항) 버퍼를 덮어쓰기 전에 로그 버퍼 내용을 서버에 저장하려면 FTP 서버를 구성합니다. FTP 서버 정보를 지정합니다.

- **FTP Server Buffer Wrap(FTP** 서버 버퍼 랩**)** - 덮어쓰기 전에 버퍼 내용을 FTP 서버에 저장하려면 이 확인란을 선택하고 다음 필드에 필요한 대상 정보를 입력합니다. FTP 구성을 제거하려면 이 옵션의 선택을 취소합니다.
- **IP Address(IP** 주소**)** - FTP 서버의 IP 주소를 포함하는 호스트 네트워크 개체를 선택합니다.

- **User Name(**사용자 이름**)** - FTP 서버에 연결할 때 사용할 사용자 이름을 입력합니다.
- **Path(**경로**)** - 버퍼 내용을 저장해야 하는 FTP 루트에 상대적인 경로를 입력합니다.
- **Password/ Confirm(**비밀번호/확인**)** - FTP 서버에 대한 사용자 이름을 인증하는 데 사용되는 비밀번호를 입력하고 확인합니다.

단계 **6** (선택 사항) 버퍼를 덮어쓰기 전에 로그 버퍼 내용을 플래시에 저장하려면 플래시 크기를 지정합니다.

- **Flash(**플래시**)** - 덮어쓰기 전에 버퍼 내용을 플래시 메모리에 저장하려면 이 확인란을 선택합니다.
- **Maximum flash to be used by logging (KB)(**로깅에 사용할 최대 플래시**(KB))** - 로깅에 사용할 플래시 메모리의 최대 공간을 KB 단위로 지정합니다. 범위는 4-8044176 킬로바이트입니다.
- **Minimum free space to be preserved(KB)(**유지할 최소 여유 공간**(KB))** - 플래시 메모리에 유지할 최소 여유 공간을 KB 단위로 지정합니다. 범위는 0-8044176 킬로바이트입니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

로깅 대상 활성화

로깅 대상을 활성화하여 해당 대상에서 메시지를 볼 수 있도록 해야 합니다. 대상을 활성화할 때 대상에 대한 메시지 필터도 지정해야 합니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 시스템 로그 메시지에 적용되는 Threat Defense 플랫폼 설정, 45 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Syslog** > **Logging Destinations(**로깅 대상**)**을 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하여 대상을 활성화하고 로깅 필터를 적용하거나 기존 대상을 편집합니다.

단계 **4** **Logging Destinations(**로깅 대상**)** 대화 상자에서 대상을 선택하고 대상에 사용할 필터를 구성합니다.

a) **Logging Destination(**로깅 대상**)** 드롭다운 목록에서 활성화하려는 대상을 선택합니다. 대상 당 하나의 필터(콘솔, 이메일, 내부 버퍼, SNMP 트랩, SSH 세션 및 Syslog 서버)를 만들 수 있습니다.

참고 콘솔 및 SSH 세션 로깅은 진단 CLI에서만 작동합니다. **system support diagnostic-cli**을 입력합니다.

b) **Event Class(**이벤트 클래스**)**에서 테이블에 없는 모든 클래스에 적용할 필터를 선택합니다.

이러한 필터를 구성할 수 있습니다.

- **Filter on severity(**심각도 필터**)** - 심각도 레벨을 선택합니다. 이 레벨 이상의 메시지가 대상으로 전송됩니다.
- **Use Event List(**이벤트 목록 사용**)** - 필터를 정의하는 이벤트 목록에서 선택합니다. **Event Lists(**이벤트 목록**)** 페이지에서 이러한 목록을 생성합니다.
- **Disable Logging(**로깅 비활성화**)** - 이 대상으로 메시지가 전송되지 않도록 합니다.

c) 이벤트 클래스당 필터를 작성하려면 **Add(**추가**)**를 클릭하여 새 필터를 생성하거나 기존 필터를 편집하고 이벤트 클래스 및 심각도 레벨을 선택하여 해당 클래스의 메시지를 제한합니다. 필터를 저장하려면 **OK(**확인**)**를 클릭합니다.

이벤트 클래스에 대한 설명은 Syslog 메시지 클래스, 40 페이지의 내용을 참조하십시오.

d) **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

이메일 주소로 **Syslog** 메시지 전송

Syslog 메시지가 이메일로 전송되도록 수신자 목록을 설정할 수 있습니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 시스템 로그 메시지에 적용되는 Threat Defense 플랫폼 설정, 45 페이지의 내용을 참조하십시오.

시작하기 전에

- SMTP 서버 플랫폼 설정 페이지에서 SMTP 서버 구성
- 로깅 활성화 및 기본 설정, 45 페이지
- 로깅 대상 활성화

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Syslog** > **Email Setup(**이메일 설정**)**을 선택합니다.

단계 **3** 이메일 메시지로 전송되는 syslog 메시지의 소스 주소로 사용할 이메일 주소를 지정합니다.

단계 **4** 지정된 syslog 메시지의 새로운 이메일 주소 수신자를 입력하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** 드롭다운 목록에서 수신자에게 전송되는 syslog 메시지의 심각도 레벨을 선택합니다.

대상 이메일 주소에 사용되는 syslog 메시지 심각도 필터는 지정된 심각도 레벨 이상의 메시지가 전송되도록 만듭니다. 레벨에 대한 자세한 내용은 심각도 레벨, 38 페이지 섹션을 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

사용자 지정 이벤트 목록 생성

이벤트 목록은 어떤 메시지를 대상으로 전송할지 제어하기 위해 기록 대상에 적용할 수 있는 맞춤형 필터입니다. 일반적으로 심각도만을 기준으로 대상에 대한 메시지를 필터링하지만, 이벤트 목록을 사용하여 이벤트 클래스, 심각도 및 메시지 식별자(ID)의 조합을 기준으로 어떤 메시지를 전송할지 세부 조정할 수 있습니다.

사용자 정의 이벤트 목록을 만드는 과정은 두 단계로 이루어집니다. **Event Lists(**이벤트 목록**)**에서 사용자 정의 목록을 만든 다음 이벤트 목록을 사용하여 다양한 대상 유형에 대한 로깅 필터를 **Logging Destinations(**로깅 대상**)**에서 정의할 수 있습니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 시스템 로그 메시지에 적용되는 Threat Defense 플랫폼 설정, 45 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Syslog** > **Events List(**이벤트 목록**)**를 선택합니다.

단계 **3** 이벤트 목록을 구성합니다.

a) **Add(**추가**)**를 클릭하여 새 목록을 추가하거나 기존 목록을 편집합니다.

b) **Name(**이름**)**필드에 이벤트 이름을 입력합니다. 공백은 허용되지 않습니다.

c) 심각도 또는 이벤트 클래스를 기반으로 메시지를 식별하려면 **Severity/Event Class(**심각도/이벤트 클래스**)** 탭을 선택하고 항목을 추가하거나 편집합니다.

사용 가능한 클래스에 대한 내용은 Syslog 메시지 클래스, 40 페이지 섹션을 참조하십시오.

레벨에 대한 자세한 내용은 심각도 레벨, 38 페이지 섹션을 참조하십시오.

특정 이벤트 클래스는 투명 모드에서 해당 디바이스에 적용할 수 없습니다. 이러한 옵션이 구성되면 무시되며 구축되지 않습니다.

d) 메시지 ID별로 메시지를 식별하려면 **Message ID(**메시지 **ID)**를 선택하고 ID를 추가하거나 편집합니다.

하이픈을 사용하여 ID 범위를 입력할 수 있습니다(예: 100000-200000). ID는 6자리입니다. 처음 세 자리를 기능에 매핑하는 방법에 대한 내용은 Syslog 메시지 클래스, 40 페이지 섹션을 참조하십시오.

특정 메시지 번호는 Cisco ASA Series Syslog Messages(Cisco ASA Series Syslog 메시지)를 참조하십시오.

e) 이벤트 목록을 저장하려면 **OK(**확인**)**를 클릭합니다.

단계 **4** **Logging Destinations(**로깅 대상**)**를 클릭하고 필터를 사용해야 하는 대상을 추가하거나 편집합니다.

로깅 대상 활성화, 47 페이지의 내용을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Syslog 메시지 생성 속도 제한

심각도 수준 또는 메시지 ID별로 syslog 메시지가 생성되는 속도를 제한할 수 있습니다. 각 로깅 수준 및 각 Syslog 메시지 ID에 대해 개별적인 제한을 지정할 수 있습니다. 설정이 충돌하면 Syslog 메시지 ID 제한이 우선 적용됩니다.

팁 보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 대부분의 FTD 플랫폼 설정이 이러한 메시지에 적용되지 않습니다. 보안 이벤트 시스템 로그 메시지에 적용되는 Threat Defense 플랫폼 설정, 45 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Syslog** > **Rate Limit(**속도 제한**)**을 선택합니다.

단계 **3** 심각도 레벨별로 메시지 생성을 제한하려면 **Logging Level(**로깅 레벨**)** > **Add(**추가**)**를 클릭하고 다음 옵션을 구성합니다.

- **Logging Level** - 속도를 제한하는 심각도 레벨입니다. 레벨에 대한 자세한 내용은 심각도 레벨, 38 페이지 섹션을 참조하십시오.
- **Number of messages** - 지정된 기간에 허용된 지정된 유형의 최대 메시지 수입니다.

- **Interval** - 속도 제한 카운터가 재설정되기 전의 시간(초)입니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** syslog 메시지 ID별로 메시지 생성을 제한하려면 **Syslog Level(Syslog** 레벨**)** > **Add(**추가**)**를 클릭하고 다음 옵션을 구성합니다.

- **Syslog ID** - 속도를 제한하는 syslog 메시지 ID입니다. 특정 메시지 번호는 Cisco ASA Series Syslog Messages(Cisco ASA Series Syslog 메시지)를 참조하십시오.
- **Number of messages** - 지정된 기간에 허용된 지정된 유형의 최대 메시지 수입니다.
- **Interval** - 속도 제한 카운터가 재설정되기 전의 시간(초)입니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Syslog 설정

syslog 서버로 전송되는 syslog 메시지에 포함될 기능 코드를 설정하고, 각 메시지에 타임스탬프가 포함되는지 여부를 지정하고, 메시지에 포함할 디바이스 ID를 지정하고, 메시지의 심각도 레벨을 보고 수정하도록 일반 syslog 설정을 구성하고, 특정 메시지의 생성을 비활성화할 수 있습니다.

보안 이벤트(예: 연결 및 침입 이벤트)에 대한 syslog 메시지를 보내도록 디바이스를 구성하는 경우 이 페이지의 일부 설정은 이러한 메시지에 적용되지 않습니다. Cisco Secure Firewall Management Center 관리 가이드의 보안 이벤트 시스템 로그 메시지에 적용되는 위협 방어 플랫폼 설정을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Syslog** > **Syslog Settings(Syslog** 설정**)**를 선택합니다.

단계 **3** **Facility(**시설**)** 드롭다운 목록에서 파일 메시지의 기반으로 사용할 syslog 서버에 대한 시스템 로그를 선택합니다.

기본값은 대부분의 UNIX 시스템이 기대하는 LOCAL4(20)입니다. 하지만 네트워크 디바이스가 이용 가능한 시설을 공유하기 때문에 시스템 로그에 대한 이 값을 변경해야 할 수 있습니다.

일반적으로 시설 값은 보안 이벤트의 메시지와는 무관합니다.

단계 **4** syslog 메시지에 메시지가 생성된 날짜와 시간을 포함하려면 **Enable timestamp on each syslog message(**각 **Syslog** 메시지에서 타임스탬프 활성화**)** 확인란을 선택합니다.

단계 **5** syslog 메시지에 대한 **Timestamp Format(**타임스탬프 형식**)**을 선택합니다.

- 레거시(MMM dd yyyy HH:mm:ss) 형식은 syslog 메시지의 기본 형식입니다.

이 타임스탬프 형식을 선택하면 메시지에 시간대가 표시되지 않으며 항상 UTC입니다.

- RFC 5424(yyyy-MM-ddTHH:mm:ssZ)는 RFC 5424 syslog 형식에 지정된 대로 ISO 8601 타임스탬프 형식을 사용합니다.

  RFC 5424 형식을 선택하는 경우 각 타임스탬프 끝에 "Z"가 추가되어 타임스탬프가 UTC 시간대를 사용함을 나타냅니다.

단계 **6** 메시지의 시작 부분에 있는 syslog 메시지에 디바이스 식별자를 추가하려면 **Enable Syslog Device ID(Syslog** 디바이스 **ID** 활성화**)** 확인란을 선택한 다음 ID 유형을 선택합니다.

- **Interface(**인터페이스**)** - 어플라이언스가 메시지를 보내는 인터페이스와 상관없이 선택한 인터페이스의 IP 주소를 사용합니다. 인터페이스를 식별하는 보안 영역을 선택합니다. 영역은 단일 인터페이스로 매핑되어야 합니다.
- **User Defined ID(**사용자 정의 **ID)** - 선택한 텍스트 문자열(최대 16자)을 사용합니다.
- **Host Name(**호스트 이름**)** - 디바이스의 호스트 이름을 사용합니다.

단계 **7** Syslog Message 테이블을 사용하여 특정 syslog 메시지의 기본 설정을 변경합니다. 기본 설정을 변경하려는 경우에만 이 테이블에서 규칙을 구성해야 합니다. 메시지에 할당된 심각도를 변경하거나 메시지 생성을 비활성화할 수 있습니다.

기본적으로 Netflow가 활성화되고 항목이 테이블에 표시됩니다.

a) Netflow로 인해 중복되는 syslog 메시지를 표시하지 않으려면 **Netflow Equivalent Syslogs**를 선택합니다.

이렇게 하면 메시지가 억제된 메시지로 테이블에 추가됩니다.

참고 이러한 syslog 항목 중 하나라도 이미 테이블에 있으면 기존 규칙을 덮어쓰지 않습니다.

b) 새 규칙을 추가하려면 **Add(**추가**)**를 클릭합니다.

c) **Syslog ID** 드롭다운 목록에서 구성을 변경하려는 메시지 번호를 선택한 다음 **Logging Level(**로깅 레벨**)** 드롭다운 목록에서 새 심각도 레벨을 선택하거나 **Suppressed(**억제**)**를 선택하여 메시지 생성을 비활성화합니다. 일반적으로 심각도 레벨을 변경하지 않고 메시지를 비활성화하지 않지만 원하는 경우 두 필드를 모두 변경할 수 있습니다.

d) 테이블에 규칙을 추가하려면 **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

Syslog 서버 설정

시스템에서 생성한 메시지를 처리하는 시스템 로그 서버를 구성하려면 다음 단계를 수행합니다.

이 시스템 로그 서버가 연결 및 침입 이벤트와 같은 보안 이벤트를 수신하도록 하려는 경우 보안 이벤트 시스템 로그 메시지에 적용되는 Threat Defense 플랫폼 설정, 45 페이지의 내용도 참조하십시오.

시작하기 전에

- 로깅 지침, 43 페이지의 요구 사항을 참조하십시오.
- 디바이스가 네트워크의 시스템 로그 수집기에 연결할 수 있는지 확인합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Syslog** > **Syslog Server(Syslog** 서버**)**를 선택합니다.

단계 **3** TCP 프로토콜을 사용하는 syslog 서버가 다운된 경우 트래픽을 허용하려면 **Allow user traffic to pass when TCP syslog server is down(TCP syslog** 서버가 중단되었을 때 사용자 트래픽이 전달되도록 허용**)** 확인란을 선택합니다.

단계 **4** **Message queue size (messages)(**메시지 대기열 크기**(**메시지**))** 필드에서 시스템 로그 서버가 사용 중일 때 보안 어플라이언스에 시스템 로그 메시지를 저장하기 위한 대기열의 크기를 입력합니다. 최소값은 메시지 1개입니다. 기본값은 512입니다. 무제한 메시지 수가 대기열에 포함되도록 허용하려면 0을 지정합니다(사용 가능한 블록 메모리가 있는 경우).

메시지가 구성된 대기열 크기를 초과하면 삭제되고 시스템 로그가 누락됩니다. 이상적인 대기열 크기를 결정하려면 사용 가능한 블록 메모리를 식별해야 합니다. **show blocks** 명령을 사용하여 현재 메모리 블록 사용을 파악합니다. 명령 및 해당 속성에 대한 자세한 내용은 *Cisco Secure Firewall ASA Series* 명령 참조 가이드를 참조하십시오. 추가 지원은 Cisco TAC에 요청하십시오.

단계 **5** **Add(**추가**)**를 클릭하여 새 syslog 서버를 추가합니다.

a) **IP Address(IP** 주소**)** 드롭다운 목록에서 syslog 서버의 IP 주소를 포함하는 호스트 네트워크 개체를 선택합니다.

b) 프로토콜(TCP 또는 UDP)을 선택하고 threat defense 디바이스와 syslog 서버 간의 통신 포트 번호를 입력합니다.

UDP는 TCP에 비해 속도가 빠르고 디바이스의 리소스를 적게 사용합니다.

기본 UDP 포트는 514입니다. TCP에 대해 포트 1470을 수동으로 구성해야 합니다. 각 프로토콜에 대한 유효한 비 기본 포트 값은 1025부터 65535입니다.

c) **Log messages in Cisco EMBLEM format (UDP only)(Cisco EMBLEM** 형식 로그 메시지**(UDP** 전용**))** 확인란을 선택하여 Cisco EMBLEM 형식의 메시지 로깅 여부를 지정합니다(프로토콜로 UDP가 선택된 경우만 사용 가능).

참고 RFC5424 형식의 시스템 로그 메시지는 일반적으로 우선순위 값(PRI)을 표시합니다. 그러나 management center에서는 Cisco EMBLEM 형식으로 로깅을 활성화하는 경우에만 관리되는 threat defense의 시스템 로그 메시지에 있는 PRI 값이 표시됩니다. PRI에 대한 자세한 내용은 RFC5424를 참조하십시오.

d) TCP를 통한 SSL/TLS를 사용하여 디바이스와 서버 간의 연결을 암호화하려면 Enable Secure Syslog(보안 Syslog 활성화) 확인란을 선택합니다.

참고 이 옵션을 사용하려면 TCP를 프로토콜로 선택해야 합니다. 또한 **Devices(**디바이스**)** > **Certificates(**인증서**)** 페이지에서 시스템 로그 서버와 통신하는 데 필요한 인증서를 업로드해야 합니다. 마지막으로, threat defense 디바이스에서 syslog 서버로 인증서를 업로드하여 보안 관계를 완료하고 트래픽의 비밀번호를 해독하도록 허용합니다. **Enable Secure Syslog(**보안 시스템 로그 활성화**)** 옵션은 디바이스 관리 인터페이스에서 지원되지 않습니다.

e) syslog 서버와 통신하려면 **Device Management Interface(**디바이스 관리 인터페이스**)** 또는 **Security Zones or Named Interfaces(**보안 영역 또는 이름이 지정된 인터페이스**)**를 선택합니다.

- **Device Management Interface(**디바이스 관리 인터페이스**)**: 관리 인터페이스에서 시스템 로그를 전송합니다. Snort 이벤트에서 시스템 로그를 설정할 때 이 옵션을 사용하는 것이 좋습니다.

  참고 디바이스 관리 인터페이스 옵션은 **Enable Secure Syslog(**보안 시스템 로그 활성화**)** 옵션을 지원하지 않습니다.

- **Security Zones or Named Interfaces(**보안 영역 또는 이름이 지정된 인터페이스**)**: **Available Zones(**사용 가능한 영역**)** 목록에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭합니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

전역 시간 제한 구성

다양한 프로토콜의 연결 및 변환 슬롯에 대해 전역 유휴 타임아웃 시간을 설정할 수 있습니다. 지정한 유휴 시간 동안 슬롯이 사용되지 않은 경우 리소스가 해제 풀로 반환됩니다.

디바이스와 콘솔 세션에 대한 시간 제한을 설정할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Timeouts(**시간 제한**)**를 선택합니다.

단계 **3** 변경하려는 시간 제한을 구성합니다.

지정된 설정에 대해 **Custom(**사용자 정의**)**을 선택하여 고유 값을 정의하고, **Default(**기본값**)**를 선택하여 시스템 기본값으로 되돌립니다. 대부분의 경우 최대 시간 제한은 1193시간입니다.

Disable(비활성화**)**을 선택하여 일부 시간 제한을 비활성화할 수 있습니다.

- **Console Timeout(**콘솔 시간 초과**)** - 콘솔 연결이 끊어질 때까지의 유휴 시간이며, 범위는 0 또는 5~1440분입니다. 기본값은 0입니다. 즉 세션에 시간 제한이 없습니다. 값을 변경하면 기존 콘솔 세션에서 이전 시간 제한 값을 사용합니다. 새 값은 새 연결에만 적용됩니다.
- **Translation Slot (xlate)**—변환 슬롯이 해제될 때까지의 유휴 시간입니다. 이 기간은 1분 이상이어야 합니다. 기본값은 3시간입니다.
- **Connection (Conn)**—연결 슬롯이 해제되기 전에 경과해야 하는 유휴 시간입니다. 이 시간은 5분 이상이어야 합니다. 기본값은 1시간입니다.
- **Half-Closed**—절반이 닫힌 TCP 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. FIN 및 FIN-ACK가 모두 확인된 경우 연결은 절반이 닫힌 것으로 간주됩니다. FIN만 확인된 경우 일반 연결 시간 초과가 적용됩니다. 최소값은 30초입니다. 기본값은 10분입니다.
- **UDP**—UDP 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 이 시간은 1분 이상이어야 합니다. 기본값은 2분입니다.
- **ICMP**—UDP 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 기본값 및 최소값은 2초입니다.
- **RPC/Sun RPC**—SunRPC 슬롯이 해제될 때까지의 유휴 시간입니다. 이 시간은 1분 이상이어야 합니다. 기본값은 10분입니다.

  Sun RPC 기반 연결에서 상위 연결이 삭제되거나 시간 초과되면, 새로운 하위 연결은 상위-하위 연결의 일부로 간주되지 않을 수도 있으며 시스템의 정책 또는 규칙 모음에 따라 평가될 수 있습니다. 상위 연결의 시간이 초과되면 기존 하위 연결은 설정한 시간 제한 값에 도달할 때까지만 사용할 수 있습니다.
- **H. 225**—H.225 신호 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 기본값은 1시간입니다. 모든 호출이 지원진 직후 연결을 닫으려면 타임아웃은 1초(0:0:1)가 좋습니다.
- **H. 323**—H.245(TCP) 및 H.323(UDP) 미디어 연결이 닫히기 전에 경과해야 하는 유휴 시간입니다. 기본값 및 최소값은 5분입니다. H.245 및 H.323 미디어 연결 모두에 동일한 연결 플래그가 설정되어 있으므로 H.245(TCP) 연결에서 H.323(RTP 및 RTCP) 미디어 연결과 유휴 타임아웃을 공유합니다.
- **SIP**—SIP 신호 포트 연결이 닫힐 때까지의 유휴 시간입니다. 이 시간은 5분 이상이어야 합니다. 기본값은 30분입니다.

- **SIP Media**—SIP 미디어 포트 연결이 닫힐 때까지의 유휴 시간입니다. 이 시간은 1분 이상이어야 합니다. 기본값은 2분입니다. SIP 미디어 타이머는 UDP 비활성 타임아웃 대신 SIP UDP 미디어 패킷이 있는 SIP RTP/RTCP에 사용됩니다.
- **SIP Disconnect**—CANCEL 또는 BYE 메시지에 대해 200 OK를 수신하지 못한 경우 SIP 세션이 삭제되기까지의 유휴 시간(0:0:1~0:10:0)입니다. 기본값은 2분(0:2:0)입니다.
- **SIP Invite**—PROVISIONAL 응답 및 미디어 xlate에 대한 핀홀이 닫히기 전까지 경과해야 하는 유휴 시간(0:1:0~00:30:0)입니다. 기본값은 3분(0:3:0)입니다.
- **SIP Provisional Media**—SIP 프로비전 미디어 연결에 대한 타임아웃 값(1~30분)입니다. 기본은 2분입니다.
- **Floating Connection**—여러 경로가 서로 다른 메트릭으로 네트워크에 존재하는 경우 시스템은 연결 생성 시 최상의 메트릭이 있는 경로를 사용합니다. 더 나은 경로를 사용할 수 있게 되면 연결을 다시 설정하여 해당 경로를 사용할 수 있도록 이 시간 제한을 통해 연결을 닫을 수 있습니다. 기본값은 0(연결이 시간 초과되지 않음)입니다. 더 나은 경로를 사용하려면 타임아웃 값을 0:0:30~1193:0:0로 설정합니다.
- **PAT Xlate**—PAT 변환 슬롯이 해제될 때까지의 유휴 시간(0:0:30~0:5:0)입니다. 기본값은 30초입니다. 이전 연결이 업스트림 디바이스에서 여전히 열려 있을 수 있기 때문에 업스트림 라우터가 확보된 PAT 포트를 사용하는 새 연결을 거부하는 경우 시간 제한을 늘릴 수 있습니다.
- **TCP Proxy Reassembly**—리어셈블리를 기다리는 버퍼링된 패킷이 삭제되기 전에 경과해야 하는 유휴 타임아웃(0:0:10~1193:0:0)입니다. 기본값은 1분(0:1:0)입니다.
- **ARP Timeout(ARP** 시간 초과**)**—ARP 테이블 재작성 간격(초)이며 범위는 60초~4294967초입니다. 기본값은 14,400초(4시간)입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Threat Defense를 위한 NTP 시간 동기화 구성

디바이스에서 클럭 설정을 동기화하려면 NTP(Network Time Protocol) 서버를 사용합니다. management center에서 관리하는 모든 threat defense을(를) management center과(와) 동일한 NTP 서버를 사용하도록 설정하는 것이 좋습니다. threat defense은(는) 설정된 NTP 서버에서 직접 시간을 가져옵니다. threat defense의 설정된 NTP 서버에 연결할 수 없는 경우와 시간을 management center과(와) 동기화합니다.

디바이스는 NTPv4를 지원합니다.

참고 Firepower 4100/9300 섀시에 threat defense를 구축 중인 경우, Smart Licensing의 올바른 작동 및 디바이스 등록 시 올바른 타임스탬프를 보장하려면 Firepower 4100/9300 섀시에서 NTP를 구성해야 합니다. Firepower 4100/9300 섀시 및 management center에 대해 동일한 NTP 서버를 사용해야 합니다.

시작하기 전에

- 조직에 threat defense가 연결할 수 있는 하나 이상의 NTP 서버가 있는 경우, management center의 **System(**시스템**) > Configuration(**구성**)** 페이지에서 시간 동기화를 위해 구성한 디바이스용으로 동일한 하나 이상의 NTP 서버를 사용합니다.
- management center에 대한 NTP 서버 또는 서버 모음을 구성할 때 **Use the authenticated NTP server only(**인증된 **NTP** 서버만 사용**)**를 선택했다면, 디바이스는 management center(으)로 인증하도록 구성된 NTP 서버 또는 서버 모음만 사용합니다. (매니지드 디바이스는 management center와 동일한 NTP 서버를 사용하지만, NTP 연결에서는 인증을 사용하지 않습니다.)
- 디바이스가 NTP 서버에 연결할 수 없거나 조직에 NTP 서버가 없는 경우에는 다음 절차에 설명된 대로 **Via NTP from Defense Center(**방어 센터에서 **NTP**를 통해**)** 옵션을 사용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **Time Synchronization(**시간 동기화**)**을 선택합니다.

단계 **3** 다음 클럭 옵션 중 하나를 구성합니다.

- **Via NTP from Defense Center(**방어 센터에서 **NTP**를 통해**)**—(기본값). 매니지드 디바이스는 management center에 대해 설정한 NTP 서버에서 시간을 가져오고 (인증된 NTP 서버 제외) 시간을 해당 서버와 직접 동기화합니다. 그러나 다음 중 하나라도 해당하는 경우 매니지드 디바이스는 management center에서 시간을 동기화합니다.
  - management center의 NTP 서버는 디바이스에서 연결할 수 없습니다.
  - management center에 인증되지 않은 서버가 없습니다.
- **Via NTP from(NTP**를 통해**)** - management center가 네트워크에서 NTP 서버를 사용 중인 경우, 이 옵션을 선택하고 정규화된 DNS 이름(예: ntp.example.com) 또는 FMC의 **System(**시스템**) > Configuration(**구성**) > Time Synchronization(**시간 동기화**)**에서 지정한 동일한 NTP 서버의 IPv4 또는 IPv6 주소를 입력합니다. NTP 서버에 연결할 수없는 경우 management center는 NTP 서버로 작동합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

정책 애플리케이션에 대한 디바이스 표준 시간대 구성

기본적으로 시스템은 UTC 표준 시간대를 사용합니다. 디바이스에 대해 다른 표준 시간대를 지정하려면 이 절차를 사용합니다.

지정하는 표준 시간대는 이 기능을 지원하는 정책의 시간 기반 정책 애플리케이션에만 사용됩니다.

참고 시간 기반 ACL은 FMC 7.0부터 Snort 3에서도 지원됩니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 수정합니다.

Objects(개체**)** > **Object Management(**개체 관리**)** > **Time Zone(**표준 시간대**)** 페이지에서 표준 시간대 개체를 생성 할 수도 있습니다.

단계 **2** +를 클릭하여 새 표준 시간대 개체를 생성합니다.

단계 **3** 표준 시간대를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 시간 범위 개체를 생성하고, 액세스 제어 및 사전 필터 규칙에서 적용 가능한 시간 범위를 선택하고, 올바른 시간대와 연결된 디바이스에 상위 정책을 할당합니다.
- Deploy configuration changes(구성 변경 사항 구축)참조.