모범 사례: Threat Defense의 사용 사례

다음 주제에서는 device manager를 사용하여 threat defense에서 수행할 수 있는 몇 가지 일반적인 작업에 대해 설명합니다. 이러한 활용 사례에서는 디바이스 컨피그레이션 마법사를 완료했으며 이 초기 컨피그레이션을 유지했다고 가정합니다. 초기 컨피그레이션을 수정했더라도 이러한 예를 통해 제품 사용 방법을 파악할 수 있습니다.

- Device Manager에서 디바이스 구성 방법, 1 페이지
- 네트워크 트래픽을 파악하는 방법, 7 페이지
- 위협을 차단하는 방법, 15 페이지
- 악성코드를 차단하는 방법, 20 페이지
- 사용 제한 정책(URL 필터링)을 구현하는 방법, 23 페이지
- 애플리케이션 사용량을 제어하는 방법, 28 페이지
- 서브넷을 추가하는 방법, 32 페이지
- 네트워크에서 트래픽을 능동적으로 모니터링하는 방법, 37 페이지
- 추가 예시, 43 페이지

Device Manager에서 디바이스 구성 방법

설치 마법사를 완료하고 나면 작동 중인 디바이스에 몇 가지 기본 정책이 갖추어져 있어야 합니다.

- 외부 및 내부 인터페이스. 다른 데이터 인터페이스는 구성되지 않습니다.
- (Firepower 4100/9300) 데이터 인터페이스가 사전 구성되어 있지 않습니다.
- (ISA 3000) 브리지 그룹에는 2개의 내부 인터페이스와 2개의 외부 인터페이스가 있습니다. 설정을 완료하려면 BVI1의 IP 주소를 수동으로 설정해야 합니다.
- (Firepower 4100/9300 제외) 내부 및 외부 인터페이스용 보안 영역.
- (Firepower 4100/9300 제외) 내부에서 외부로 이동하는 모든 트래픽을 신뢰하는 액세스 규칙. ISA 3000에는 내부에서 외부로, 외부에서 내부로 이동하는 모든 트래픽을 허용하는 액세스 규칙이 있습니다.
- (Firepower 4100/9300 및 ISA 3000 제외) 내부에서 외부로 이동하는 모든 트래픽을 외부 인터페이스의 IP 주소에 있는 고유한 포트로 변환하는 인터페이스 NAT 규칙.

- (Firepower 4100/9300 및 ISA 3000 제외) 내부 인터페이스에서 실행 중인 DHCP 서버.

다음 단계에서는 구성하려는 추가적인 기능에 대한 개요가 제공됩니다. 각 단계에 대한 자세한 내용을 보려면 페이지에서 도움말 버튼(**?**)을 클릭하십시오.

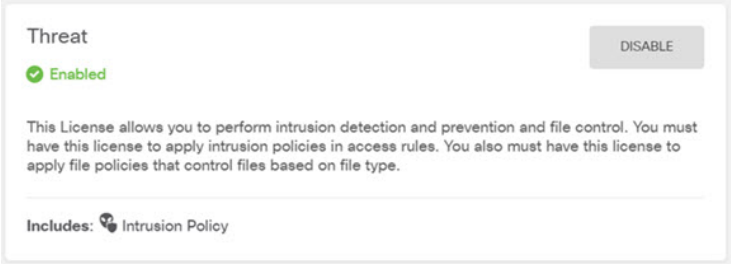
프로시저

단계 **1** 디바이스를 선택한 다음, **Smart License(**스마트 라이선스**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

사용하려는 각 선택 라이선스(위협, 악성코드, URL)에서 활성화를 클릭합니다. 설치 시 디바이스를 등록한 경우, 원하는 RA VPN 라이선스를 활성화할 수도 있습니다. 필요 여부가 확실하지 않은 경우 각 라이선스에 대한 설명을 읽어보십시오.

등록하지 않은 경우에는 이 페이지에서 등록할 수 있습니다. **Register Device(**디바이스 등록**)**를 클릭하고 지침을 따릅니다. 평가 라이선스가 만료되기 전에 등록하십시오.

예를 들어 Secure Firewall Threat Defense IPS 라이선스를 활성화하면 다음과 같습니다.



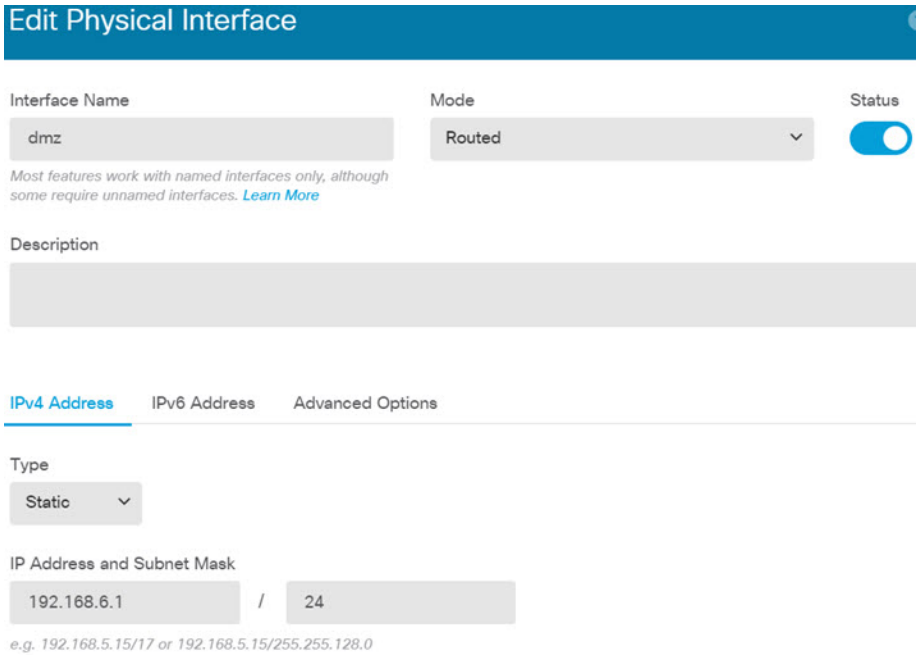
단계 **2** 다른 인터페이스에 유선으로 연결한 경우 디바이스를 선택하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, 인터페이스 유형을 클릭하여 인터페이스 목록을 확인합니다.

- Firepower 4100/9300의 경우 이름, IP 주소 또는 보안 영역을 사용하여 사전 구성된 데이터 인터페이스가 없으므로 사용할 인터페이스를 활성화하고 구성해야 합니다.
- ISA 3000은 모든 데이터 인터페이스를 포함하는 브리지 그룹이 사전 구성된 상태로 제공되므로 이러한 인터페이스를 구성할 필요가 없습니다. 그러나 BVI에 대한 IP 주소를 수동으로 구성해야 합니다. 브리지 그룹을 분리하려는 경우에는 해당 그룹을 수정하여 개별적으로 처리할 인터페이스를 제거할 수 있습니다. 그러면 별도의 네트워크를 호스팅하도록 해당 인터페이스를 구성할 수 있습니다.

  다른 모델의 경우, 기타 인터페이스의 브리지 그룹을 생성하거나 별도의 네트워크를 구성하거나, 이 두 방법을 섞어서 사용할 수 있습니다.
- Firepower 1010의 경우 Ethernet1/1(외부)을 제외한 모든 인터페이스는 VLAN1(내부)에 할당된 액세스 모드 스위치 포트입니다. 스위치 포트를 방화벽 포트로 변경할 수 있습니다. 새 VLAN 인터페이스를 추가하고 스위치 포트를 해당 인터페이스에 할당하거나 트렁크 모드 스위치 포트를 구성합니다.

각 인터페이스의 편집 아이콘()을 클릭하여 IP 주소 및 기타 설정을 정의합니다.

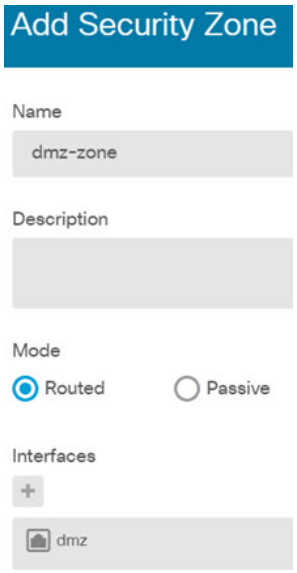
다음 예에서는 인터페이스를 웹 서버와 같이 공개적으로 액세스할 수 있는 자산을 배치하는 DMZ("Demilitarized Zone(비무장지대)")로 사용되도록 구성합니다. 완료되면 **Save(**저장**)**를 클릭합니다.



단계 **3** 새로운 인터페이스를 구성한 경우 목차에서 **Objects(**개체**)**를 선택한 다음 **Security Zones(**보안 영역**)**를 선택합니다.

새로운 영역을 적절히 편집하거나 생성합니다. 정책은 인터페이스가 아니라 보안 영역을 기반으로 구성하기 때문에 각 인터페이스는 하나의 영역에 속해 있어야 합니다. 인터페이스를 구성할 때는 영역에 인터페이스를 배치할 수 없으므로 새 인터페이스를 생성하거나 기존 인터페이스의 용도를 변경한 후에는 항상 영역 개체를 편집해야 합니다.

다음 예에는 dmz 인터페이스에서 새 dmz-zone을 생성하는 방법이 나와 있습니다.

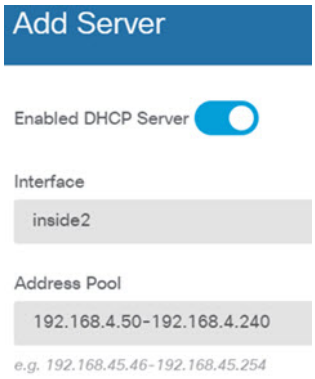


단계 **4** 내부 클라이언트가 DHCP를 사용하여 디바이스에서 IP 주소를 얻게 하려는 경우, 디바이스를 선택한 후 **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**를 선택합니다. **DHCP Servers(DHCP** 서버**)** 탭을 선택합니다.

내부 인터페이스에 이미 DHCP 서버가 구성되어 있지만 주소 풀을 편집하거나 삭제할 수도 있습니다. 다른 내부 인터페이스를 구성한 경우, 이러한 인터페이스에서 DHCP 서버를 설정하는 것은 매우 일반적입니다. +를 클릭하여 각 내부 인터페이스에 서버 및 주소 풀을 구성합니다.

또한, **Configuration(**컨피그레이션**)** 탭에서 클라이언트에게 제공된 WINS 및 DNS 목록을 조정할 수 있습니다.

다음 예에는 주소 풀이 192.168.4.50-192.168.4.240인 inside2 인터페이스에서 DHCP 서버를 설정하는 방법이 나와 있습니다.



단계 **5** 디바이스를 선택한 후 **Routing(**라우팅**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭하고 기본 경로를 구성합니다.

기본 경로는 일반적으로 외부 인터페이스 외에 있는 업스트림 또는 ISP 라우터를 가리킵니다. 기본 IPv4 경로는 any-ipv4(0.0.0.0/0)용인 반면, 기본 IPv6 경로는 any-ipv6(::0/0)용입니다. 사용하는 각 IP

버전에 대해 경로를 생성합니다. DHCP를 사용하여 외부 인터페이스에 대한 주소를 얻으려는 경우, 필요한 기본 경로가 이미 있을 수도 있습니다.

이 페이지에서 정의하는 경로는 데이터 인터페이스 전용입니다. 이러한 경로는 관리 인터페이스에 영향을 주지 않습니다. **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 관리 게이트웨이를 설정합니다.

다음 예에는 IPv4의 기본 경로가 나와 있습니다. 이 예에서 isp-gateway는 ISP 게이트웨이의 IP 주소(ISP에서 주소를 획득해야 함)를 식별하는 네트워크 개체입니다. 이 개체는 **Gateway(**게이트웨이**)** 드롭다운 목록의 아래쪽에서 **Create New Network(**새 네트워크 생성**)**를 클릭하여 생성할 수 있습니다.

단계 **6** **Policies(**정책**)**를 선택하고 네트워크의 보안 정책을 구성합니다.

디바이스 설치 마법사를 사용하면 외부 인터페이스로 이동할 때 모든 인터페이스에 대한 inside-zone, outside-zone 및 인터페이스 NAT 간의 트래픽 플로우가 가능합니다. 새 인터페이스를 구성하는 경우에도 inside-zone 개체에 이러한 인터페이스를 추가하면 이러한 인터페이스에 액세스 제어 규칙이 자동으로 적용됩니다.

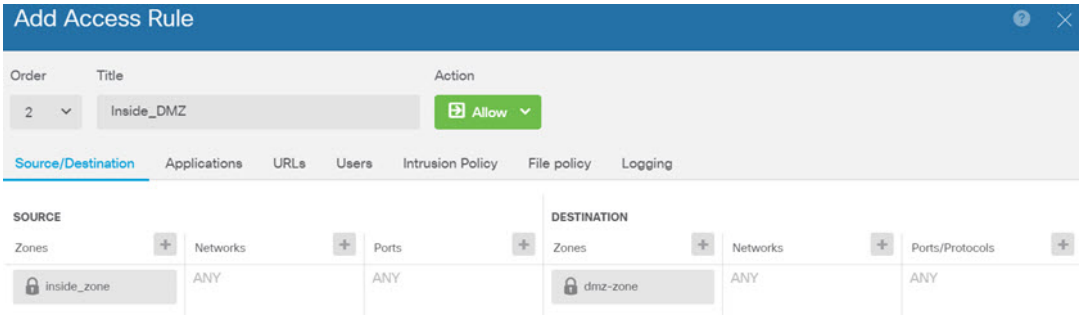
그러나 내부 인터페이스가 여러 개 있는 경우, inside-zone 간의 트래픽 플로우를 허용하기 위해 액세스 제어 규칙이 필요합니다. 다른 보안 영역을 추가하는 경우, 이러한 영역을 오고 가는 트래픽을 허용하는 규칙이 필요합니다. 이렇게 해야 변경 사항이 가장 적습니다.

또한, 다른 정책을 구성하여 추가 서비스를 제공할 수 있으며 NAT 및 액세스 규칙을 조정하여 조직에 필요한 결과를 얻을 수 있습니다. 다음과 같은 정책을 구성할 수 있습니다.

- **SSL Decryption(SSL** 암호 해독**)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다.

- **Security Intelligence(**보안 인텔리전스**)** — 보안 인텔리전스 정책을 사용하여 선택된 IP 주소 또는 URL을 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 차단하면 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco에서는 알려진 유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 차단 목록이 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 차단 목록에서 항목을 추가하거나 제거하기 위해 정책을 수정할 필요가 없습니다.
- **NAT**(Network Address Translation) — NAT 정책을 사용하여 내부 IP 주소를 외부에서 라우팅 가능한 주소로 변환합니다.
- **Access Control(**액세스 제어**)** — 액세스 제어 정책을 사용하여 네트워크에서 어떤 연결이 허용되는지 확인합니다. 보안 영역, IP 주소, 프로토콜, 포트, 애플리케이션, URL, 사용자 또는 사용자 그룹을 기준으로 필터링할 수 있습니다. 액세스 제어 규칙을 사용하여 침입 및 파일(악성코드) 정책을 적용할 수도 있습니다. 이 정책을 사용하여 URL 필터링을 구현할 수 있습니다.
- **Intrusion(**침입**)** — 침입 정책을 사용하여 알려진 위협을 검사합니다. 액세스 제어 규칙을 사용하여 침입 정책을 적용하는 경우에도 침입 정책을 편집하여 특정 침입 규칙을 선택적으로 활성화 또는 비활성화할 수 있습니다.

다음 예에는 액세스 제어 정책에서 inside-zone 및 dmz-zone 간의 트래픽을 허용하는 방법이 나와 있습니다. 이 예에서는 **Logging(**로깅**)(At End of Connection(**연결 종료 시**)**이 선택된 경우)을 제외하고는 다른 어떤 탭에도 옵션이 설정되어 있지 않습니다.



단계 **7** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

네트워크 트래픽을 파악하는 방법

초기 디바이스 설정을 완료하고 나면 인터넷 또는 기타 업스트림 네트워크에 대한 모든 내부 트래픽 액세스를 허용하는 액세스 제어 정책과, 다른 모든 트래픽을 차단하는 기본 작업이 생성됩니다. 추가 액세스 제어 규칙을 생성하기 전에 실제로 네트워크에서 생성되는 트래픽을 파악해 두면 도움이 될 수 있습니다.

device manager의 모니터링 기능을 사용하여 네트워크 트래픽을 분석할 수 있습니다. Device Manager 보고는 다음 질문에 답하는 데 도움이 됩니다.

- 네트워크가 사용되는 용도
- 네트워크를 가장 많이 사용하는 사람
- 사용자가 이동하는 위치
- 사용자가 사용 중인 디바이스
- 가장 많이 적중된 액세스 제어 규칙(정책)

초기 액세스 규칙은 정책, 대상, 보안 영역 등 트래픽에 대한 일부 정보를 제공할 수 있습니다. 그러나 사용자 정보를 파악하려면 사용자의 인증(신원 증명)을 요구하는 ID 정책을 구성해야 합니다. 네트워크에서 사용되는 애플리케이션에 대한 정보를 파악하려면 몇 가지 추가적인 조정을 수행해야 합니다.

다음 절차에서는 트래픽을 모니터링하도록 threat defense 디바이스를 설정하는 방법을 설명하고, 정책을 컨피그레이션 및 모니터링하는 엔드 투 엔드 프로세스를 대략적으로 제시합니다.

참고 이 절차에서는 사용자가 방문하는 사이트의 웹 사이트 카테고리 및 평판 관련 정보는 제공하지 않습니다. 따라서 URL 카테고리 대시보드에서는 의미 있는 정보를 확인할 수 없습니다. 범주 및 평판 데이터를 파악하려면 범주 기반 URL 필터링을 구현하고 URL 라이선스를 활성화해야 합니다. 이 정보만 파악하려는 경우 금융 등 적절한 카테고리에 대한 액세스를 허용하는 새 액세스 제어 규칙을 추가하고, 액세스 제어 정책에서 이를 첫 번째 규칙으로 지정하면 됩니다. URL 필터링 구현에 대한 자세한 내용은 사용 제한 정책(URL 필터링)을 구현하는 방법, 23 페이지를 참조하십시오.

프로시저

단계 **1** 사용자 동작을 파악하려면 연결과 연관된 사용자를 식별할 수 있도록 ID 정책을 구성해야 합니다.

ID 정책을 활성화하면 네트워크를 사용 중인 사용자와 이러한 사용자가 사용하고 있는 리소스에 대한 정보를 수집할 수 있습니다. 이 정보는 사용자 모니터링 대시보드에서 제공됩니다. 이벤트 뷰어에서 표시되는 연결 이벤트에 대해서도 사용자 정보가 제공됩니다.

이 예시에서는 사용자 ID를 가져오기 위한 활성 인증을 구현합니다. 활성 인증을 사용하는 경우 디바이스에는 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 사용자는 HTTP 연결을 위해 웹 브라우저를 사용할 때만 인증을 받습니다.

사용자의 인증 시 장애가 발생해도 웹 연결은 차단되지 않습니다. 인증 장애는 연결을 위한 사용자 ID 정보가 없음을 의미할 뿐입니다. 원하는 경우 실패한 인증으로 표시되는 사용자의 트래픽을 삭제하는 액세스 제어 규칙을 생성할 수 있습니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭한 후 **Identity(ID)**를 클릭합니다.

초기에는 ID 정책이 비활성화되어 있습니다. 활성 인증 사용 시 ID 정책은 AD(Active Directory) 서버를 통해 사용자를 인증하며, 사용자가 사용 중인 워크스테이션의 IP 주소와 사용자를 연결합니다. 그 후에 시스템은 해당 IP 주소의 트래픽을 사용자의 트래픽으로 식별합니다.

b) **Enable Identity Policy(ID** 정책 활성화**)**를 클릭합니다.

c) **Create Identity Rule(ID** 규칙 생성**)** 버튼 또는 **+** 버튼을 클릭하여 활성 인증 사용을 요구하는 규칙을 생성합니다.

이 예시에서는 모든 사용자에 대해 인증을 요구하려 한다고 가정합니다.

d) 규칙의 **Name(**이름**)**을 입력합니다. Require_Authentication 등의 원하는 이름을 선택하면 됩니다.

e) **Source/Destination(**소스/대상**)** 탭에서 기본값을 유지합니다. 이 경우 규칙이 적용되는 기준은 Any(모두)입니다.

보다 제한적인 트래픽 집합으로 정책을 적절하게 제한할 수 있습니다. 그러나 HTTP 트래픽에 대해서만 액티브 인증을 시도하므로 비HTTP 트래픽이 소스/대상 기준과 일치하는지 여부는 관계가 없습니다. ID 정책 속성에 대한 자세한 내용은 다음 주제를 참조하십시오. ID 규칙 구성

f) **Action(**작업**)**에서 **Active Auth(**활성 인증**)**를 선택합니다.

ID 정책 설정을 구성하지 않았다고 가정할 때 일부 설정이 정의되지 않았으므로 Identity Policy Configuration(ID 정책 컨피그레이션) 대화 상자가 열립니다.

g) 활성 인증에 필요한 종속 포털 및 SSL 암호 해독 설정을 구성합니다.

ID 규칙에서 사용자에 대한 활성 인증을 요구하는 경우 사용자는 종속 포털 포트로 리디렉션되며, 이후에는 인증하라는 메시지가 표시됩니다. 종속 포털에는 SSL 암호 해독 규칙이 필요하며, 이러한 규칙은 시스템에서 자동으로 생성합니다. 하지만 SSL 암호 해독 규칙에 사용할 인증서는 선택해야 합니다.

- **Server Certificate(**서버 인증서**)** - 활성 인증 중에 사용자에게 제공할 내부 인증서를 선택합니다. 사전 정의된 셀프 서명한 DefaultInternalCertificate를 선택할 수도 있고, **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭한 다음 브라우저에서 이미 신뢰하는 인증서를 업로드할 수도 있습니다.

  사용자의 브라우저에서 이미 신뢰하는 인증서를 업로드하지 않으면 사용자가 인증서를 허용해야 합니다.

- **Redirect to Host Name(**호스트 이름으로 리디렉션**)** — 활성 인증 요청에 대한 종속 포털로 사용해야 하는 인터페이스의 정규화된 호스트 이름을 정의하는 네트워크 개체를 선택합니다. 개체가 없는 경우, **Create New Network(**새 네트워크 생성**)**를 클릭합니다.

FQDN은 디바이스에 있는 인터페이스 중 하나의 IP 주소로 확인되어야 합니다. FQDN을 사용하면 클라이언트가 인식할 활성 인증에 대한 인증서를 할당할 수 있으므로, IP 주소로 리디렉션될 때 신뢰할 수 없는 인증서 경고가 표시되지 않습니다. 인증서는 인증서의 SAN(Subject Alternate Name)에 FQDN, 와일드카드 FQDN 또는 여러 FQDN을 지정할 수 있습니다.

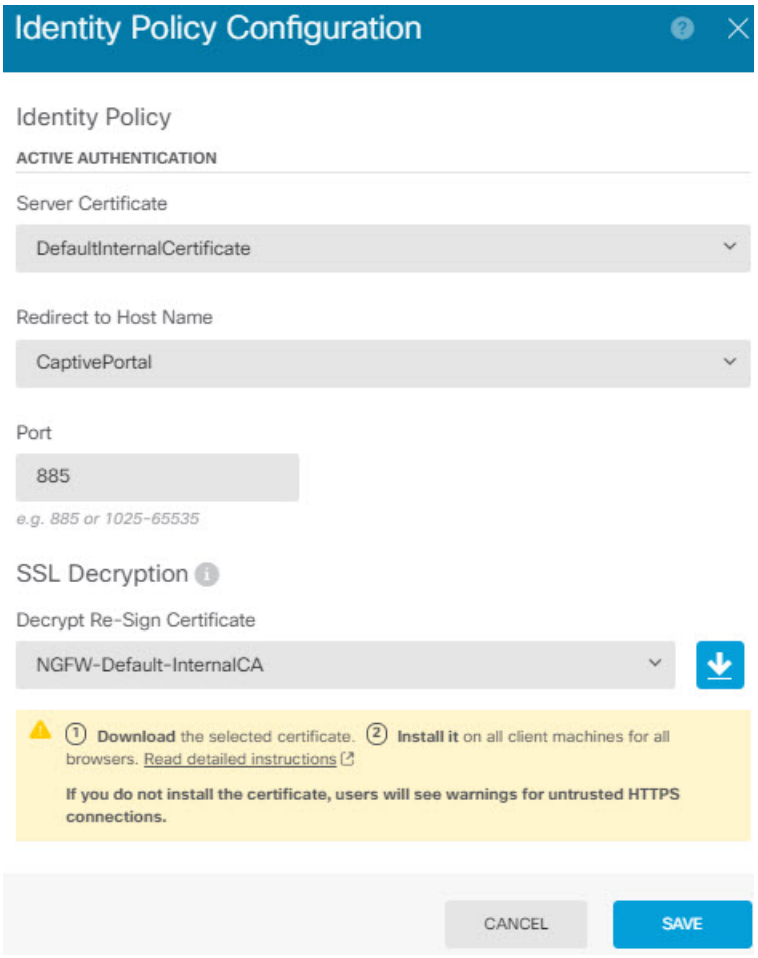
ID 규칙에서 사용자에 대한 활성 인증을 요구하지만 리디렉션 FQDN을 지정하지 않는 경우 사용자는 연결 시 사용한 인터페이스의 종속 포털 포트로 리디렉션됩니다.

- **Port(**포트**)** - 종속 포털 포트입니다. 기본값은 885(TCP)입니다. 다른 포트를 구성하는 경우에는 포트가 1025-65535 범위에 포함되어야 합니다.
- **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)** - 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다. 사전 정의된 NGFW-Default-InternalCA 인증서(기본값)를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다. (SSL 암호 해독 정책을 아직 활성화하지 않은 경우에만 암호 해독 재서명 인증서를 요구하는 메시지가 표시됩니다.)

  클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼()을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드도 참조하십시오.

예제:

이제 ID 정책 컨피그레이션 대화 상자가 다음과 같이 표시됩니다.



h) **Save(**저장**)**를 클릭하여 활성 인증 설정을 저장합니다.

이제 Action(작업) 설정 아래에 Active Authentication(활성 인증) 탭이 나타납니다.

i) **Active Authentication(**활성 인증**)** 탭에서 **HTTP Negotiate(HTTP** 협상**)**를 선택합니다.

이 옵션을 선택하면 브라우저와 디렉토리 서버가 가장 강력한 인증 프로토콜(NTLM->HTTP 기본 순서)을 협상할 수 있습니다.

참고 호스트 이름으로 리디렉션 FQDN을 제공하지 않는 경우 HTTP 기본, HTTP 응답 페이지 및 NTLM 인증 방법에서 인터페이스의 IP 주소를 사용하여 사용자를 종속 포털로 리디렉션합니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. 호스트 이름으로 리디렉션 FQDN 없이 HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다. 인증 방법과 무관하게 일관된 동작을 보장하기 위해 항상 호스트 이름으로 리디렉션 FQDN을 제공하는 것이 좋습니다. 수행할 수 없거나 원치 않는 경우 DNS 서버를 업데이트하고 다른 인증 방법 중 하나를 선택합니다.

j) **AD Identity Source(AD ID** 소스**)**에 대해 **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭합니다.

영역 서버 개체를 이미 생성한 경우에는 해당 개체를 선택하고 서버 구성 단계를 건너뛰면 됩니다.

다음 필드에 내용을 입력하고 **OK(**확인**)**를 클릭합니다.

- **Name(**이름**)** - 디렉토리 영역의 이름입니다.
- **Type(**유형**)** - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- **Directory Username(**디렉터리 사용자 이름**)**, **Directory Password(**디렉터리 비밀번호**)** - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

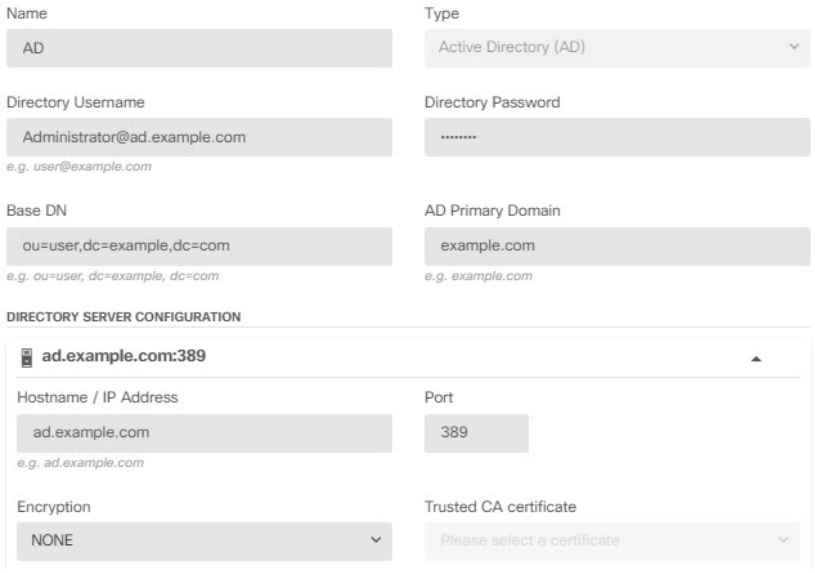
  참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환에 포함되므로 일반 이름 "users" 폴더 아래에 여기서 지정하는 사용자를 구성해야 합니다.

- **Base DN(**기본 **DN)** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정를 참조하십시오.
- **AD Primary Domain(AD** 기본 도메인**)** - 디바이스가 조인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.
- **Hostname/IP Address(**호스트 이름**/IP** 주소**)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.
- **Port(**포트**)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- **Encryption(**암호화**)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 **None(**없음**)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.
  - **STARTTLS**는 암호화 방법을 협상하여 디렉토리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다. 원격 액세스 VPN에 영역을 사용하는 경우에는 이 옵션이 지원되지 않습니다.
  - **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 이 옵션은 포트 636을 사용합니다.

- **Trusted CA Certificate(**신뢰할 수 있는 **CA** 인증서**)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

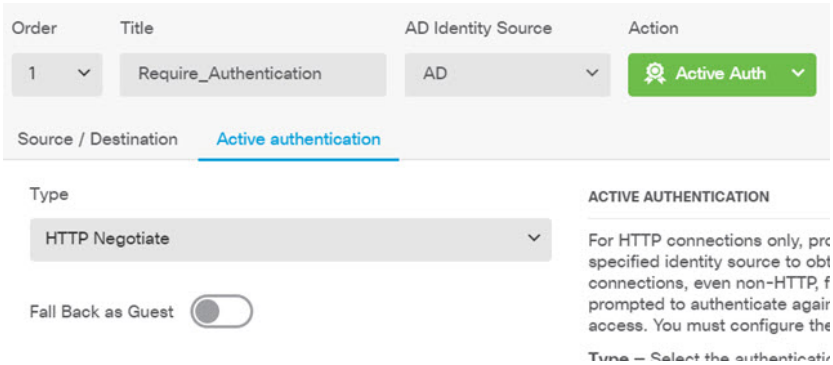
예제**:**

예를 들어 다음 그림에는 ad.example.com 서버에 대해 암호화되지 않은 연결을 생성하는 방법이 나와 있습니다. 여기서 기본 도메인은 example.com이고 디렉터리 사용자 이름은 Administrator@ad.example.com입니다. 모든 사용자 및 그룹 정보는 DN(고유 이름) ou=user,dc=example,dc=com 아래에 있습니다.



k) **AD Identity Source(AD ID** 소스**)**에 대해 방금 생성한 개체를 선택합니다.

규칙이 다음과 유사하게 표시됩니다.



l) **OK(**확인**)**를 클릭하여 규칙을 추가합니다.

이제 창 오른쪽 상단의 **Deploy(**구축**)** 아이콘 버튼에 점이 나타납니다. 이 점은 구축되지 않은 변경 사항이 있음을 나타냅니다. 사용자 인터페이스에서 변경을 수행한다고 해서 디바이스에서

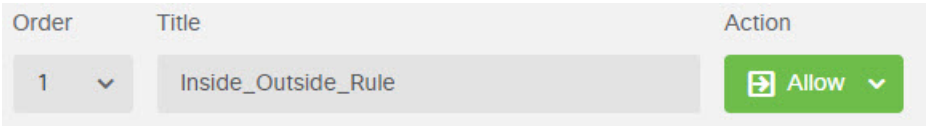
변경 사항이 구성되는 것은 아니며, 변경 사항을 구축해야 합니다. 따라서 관련 변경 집합을 먼저 수행한 후에 변경 사항을 구축하면 부분적으로 구성된 변경 사항 집합이 디바이스에서 실행되는 문제가 발생할 가능성이 없습니다. 이 절차의 뒷부분에서 변경 사항을 구축할 것입니다.

단계 **2** Inside_Outside_Rule 액세스 제어 규칙의 작업을 **Allow(**허용**)**로 변경합니다.

Inside_Outside_Rule 액세스 규칙은 신뢰 규칙으로 생성됩니다. 그러나 신뢰할 수 있는 트래픽은 검사되지 않으므로, 트래픽 일치 기준에 영역, IP 주소 및 포트 외의 기타 조건이나 애플리케이션이 포함되어 있지 않으면 시스템은 신뢰할 수 있는 트래픽의 일부 특성(예: 애플리케이션)을 확인할 수 없습니다. 트래픽을 신뢰하는 대신 허용하도록 규칙을 변경하면 시스템이 트래픽을 완전히 검사합니다.

참고 (ISA 3000) Outside_Inside_Rule, Inside_Inside_Rule 및 Outside_Outside_Rule도 Trust(신뢰)에서 Allow(허용)로 변경하는 것이 좋습니다.

a) **Policies(**정책**)** 페이지에서 **Access Control(**액세스 제어**)**을 클릭합니다.
b) Inside_Outside_Rule 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.
c) **Action(**작업**)**에 대해 **Allow(**허용**)**를 선택합니다.

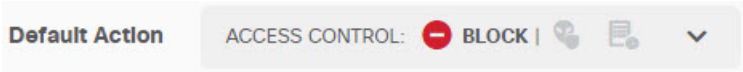


d) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** 액세스 제어 정책 기본 작업에 대해 로깅을 활성화합니다.

연결이 연결 로깅을 활성화하는 액세스 제어 규칙과 일치하는 경우에만 대시보드에 연결 관련 정보가 포함됩니다. Inside_Outside_Rule은 로깅을 활성화하지만 기본 작업에서는 로깅이 비활성화됩니다. 따라서 대시보드에는 Inside_Outside_Rule에 대한 정보만 표시되며 규칙과 일치하지 않는 연결은 대시보드에 반영되지 않습니다.

a) 액세스 제어 정책 페이지 하단의 기본 작업에서 아무 곳이나 클릭합니다.



b) **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.
c) **OK(**확인**)**를 클릭합니다.

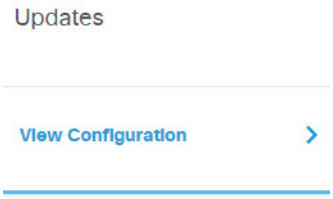
단계 **4** VDB(Vulnerability Database)의 업데이트 일정을 설정합니다.

Cisco는 VDB 업데이트를 정기적으로 제공합니다. 이 업데이트에는 연결에서 사용되는 애플리케이션을 식별할 수 있는 애플리케이션 탐지기가 포함됩니다. VDB는 정기적으로 업데이트해야 합니다. 업데이트는 수동으로 다운로드할 수도 있고 정기 일정을 설정할 수도 있습니다. 다음 절차에서는 일

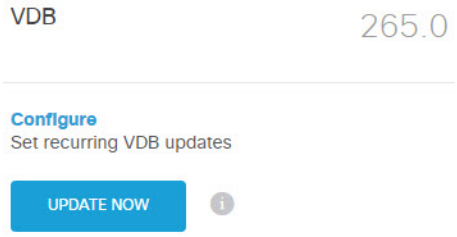
정을 설정하는 방법을 보여줍니다. VDB 업데이트는 기본적으로 비활성화되므로 VDB 업데이트를 받기 위한 작업을 수행해야 합니다.

a) 디바이스를 클릭합니다.

b) 업데이트 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.



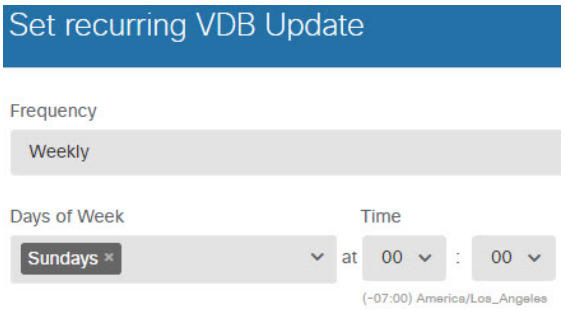
c) VDB 그룹에서 **Configure(**구성**)**를 클릭합니다.



d) 업데이트 일정을 정의합니다.

네트워크에 영향을 주지 않는 시간과 빈도를 선택합니다. 또한 시스템은 업데이트를 다운로드한 후에 자동 구축을 수행합니다. 새 탐지기를 사용하려면 자동 구축을 수행해야 합니다. 따라서 수행하고 저장했지만 구축하지는 않은 컨피그레이션 변경 사항도 구축됩니다.

예를 들어 다음 일정은 매주 일요일 자정(24시간 표기법 사용)에 VDB를 업데이트합니다.



e) **Save(**저장**)**를 클릭합니다.

단계 **5** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 사용자 및 애플리케이션에 대한 정보가 표시됩니다. 이 정보를 평가하여 부적절한 패턴이 있는지 확인하고 허용할 수 없는 사용을 제한하는 새 액세스 규칙을 개발할 수 있습니다.

침입 및 악성코드 관련 정보 수집을 시작하려면 하나 이상의 액세스 규칙에 대해 침입 및 파일 정책을 활성화해야 합니다. 또한 이러한 기능에 대한 라이선스도 활성화해야 합니다.

URL 카테고리 관련 정보 수집을 시작하려면 URL 필터링을 구현해야 합니다.

위협을 차단하는 방법

액세스 제어 규칙에 침입 정책을 추가하여 차세대 IPS(침입 방지 시스템) 필터링을 구현할 수 있습니다. 침입 정책은 네트워크 트래픽을 분석하여 트래픽 콘텐츠와 알려진 위협을 비교합니다. 연결이 모니터링 대상 위협과 일치하는 경우 시스템은 연결을 삭제하여 공격을 방지합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입을 검사하기 전에 수행됩니다. 침입 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책을 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 **allow(**허용**)**하는 규칙에 대해서만 침입 정책을 구성할 수 있습니다. 트래픽을 **trust(**신뢰**)** 또는 **block(**차단**)**하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한 기본 작업이 **allow(**허용**)**인 경우 기본 작업의 일부분으로 침입 정책을 구성할 수 있습니다.

침입 정책은 고급 설정과 침입 및 전처리기 규칙 상태를 설정한 Cisco Talos Intelligence Group(Talos)에서 고안했습니다. Snort 3을 검사 엔진으로 사용하는 경우 Talos 정책을 기반으로 고유한 맞춤형 정책을 생성할 수 있습니다.

허용하는 트래픽의 침입 가능성을 검사하는 것 외에, 보안 인텔리전스 정책을 사용하여 알려진 잘못된 IP 주소에서 나가거나 들어오는 모든 트래픽이나 알려진 잘못된 URL로 나가는 모든 트래픽을 사전에 차단할 수 있습니다.

프로시저

단계 **1** 아직 수행하지 않은 경우 위협 라이선스를 활성화합니다.

침입 정책 및 보안 인텔리전스를 사용하려면 위협 라이선스를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 어카운트에 추가해야 합니다.

a) 디바이스를 클릭합니다.
b) 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

c) 위협 그룹에서 **Enable(**활성화**)**을 클릭합니다.

시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 Disable(비활성화) 버튼으로 변경됩니다.

단계 **2** 하나 이상의 액세스 규칙에 대해 침입 정책을 선택합니다.

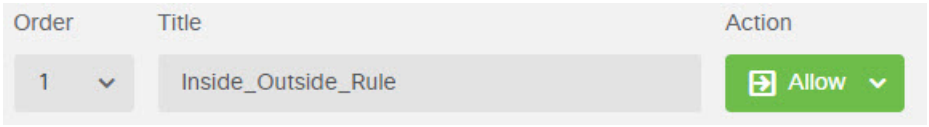
위협을 검사해야 하는 트래픽에 적용할 규칙을 결정합니다. 이 예에서는 Inside_Outside_Rule에 침입 검사를 추가합니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

b) Inside_Outside_Rule 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.

c) **Action(**작업**)**에 대해 **Allow(**허용**)**를 아직 선택하지 않았으면 선택합니다.

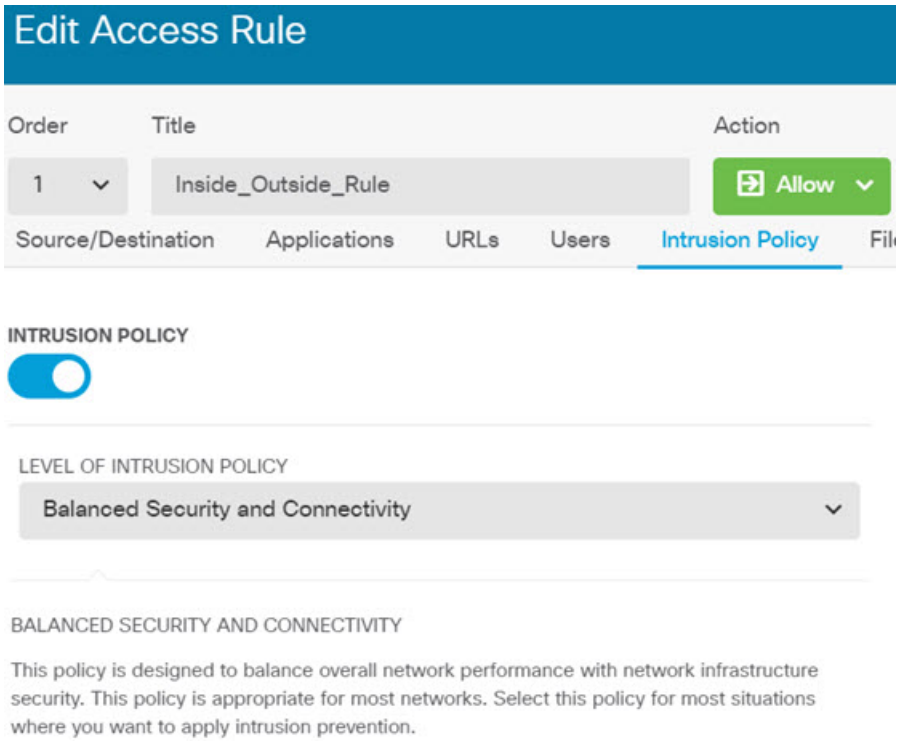


d) **Intrusion Policy(**침입 정책**)** 탭을 클릭합니다.

e) **Intrusion Policy(**침입 정책**)** 토글을 클릭하여 정책을 활성화한 다음 침입 정책을 선택합니다.

Balanced Security and Connectivity(보안과 연결의 균형 유지**)** 정책은 대부분의 네트워크에 적합합니다. 이 정책은 과도하게 적극적이지 않은 적절한 침입 방어 기능을 제공합니다. 침입 방지 기능이 너무 적극적이면 삭제되면 안 되는 트래픽이 삭제될 수 있습니다. 트래픽이 너무 많이 삭제되는지 확인하려는 경우 **Connectivity over Security(**연결이 보안에 우선함**)** 정책을 선택하여 침입 검사의 레벨을 높일 수 있습니다.

적극적인 보안을 적용해야 하는 경우에는 **Security over Connectivity(**보안이 연결에 우선함**)** 정책을 사용해 보십시오. **Maximum Detection(**최대 탐지**)** 정책은 네트워크 인프라 보안을 더욱 강화하며, 사용하는 경우 운영에 더 큰 영향을 미칠 수 있습니다.



f) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** (선택 사항) **Policies(**정책**)** > **Intrusion(**침입**)**으로 이동하여 기어 아이콘을 클릭하고 침입 정책에 대한 시스템 로그 서버를 구성합니다.

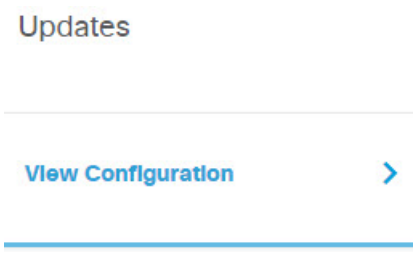
침입 이벤트는 액세스 제어 규칙에 대해 구성된 시스템 로그 서버를 사용하지 않습니다.

단계 **4** 침입 규칙 데이터베이스의 업데이트 일정을 설정합니다.

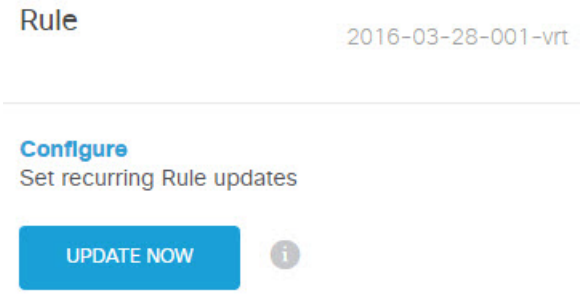
Cisco는 침입 정책이 연결을 삭제해야 하는지 여부를 결정하는 데 사용하는 침입 규칙 데이터베이스에 대한 업데이트를 정기적으로 제공합니다. 규칙 데이터베이스는 정기적으로 업데이트해야 합니다. 업데이트는 수동으로 다운로드할 수도 있고 정기 일정을 설정할 수도 있습니다. 다음 절차에서는 일정을 설정하는 방법을 보여줍니다. 기본값으로 데이터베이스 업데이트는 비활성화되므로 업데이트된 규칙을 받기 위한 작업을 수행해야 합니다.

a) 디바이스를 클릭합니다.

b) 업데이트 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.



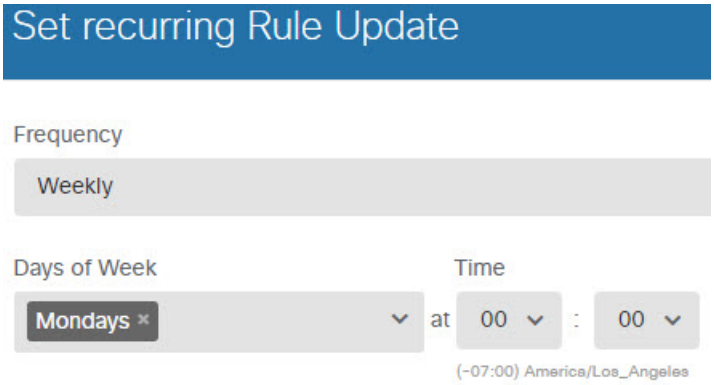
c) 규칙 그룹에서 **Configure(**구성**)**를 클릭합니다.



d) 업데이트 일정을 정의합니다.

네트워크에 영향을 주지 않는 시간과 빈도를 선택합니다. 또한 시스템은 업데이트를 다운로드한 후에 자동 구축을 수행합니다. 새 규칙을 사용하려면 자동 구축을 수행해야 합니다. 따라서 수행하고 저장했지만 구축하지는 않은 컨피그레이션 변경 사항도 구축됩니다.

예를 들어 다음 일정은 매주 월요일 자정(24시간 표기법 사용)에 규칙 데이터베이스를 업데이트합니다.



e) **Save(**저장**)**를 클릭합니다.

단계 **5** 알려진 잘못된 호스트 및 사이트와의 연결을 사전에 삭제하도록 보안 인텔리전스 정책을 구성합니다.

보안 인텔리전스를 사용하여 위협으로 알려진 호스트 또는 사이트와의 연결을 차단하면 시스템이 DPI(Deep Packet Inspection)를 수행하여 각 연결의 위협을 식별하는 데 필요한 시간을 절약할 수 있습니다. 보안 인텔리전스를 사용하면 원치 않는 트래픽을 일찍 차단할 수 있으므로 시스템이 실제로 중요한 트래픽을 처리하는 데 더 많은 시간을 할애할 수 있습니다.

a) **Device(**디바이스**)**를 클릭한 다음 **Updates(**업데이트**)** 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

b) Security Intelligence Feeds(보안 인텔리전스 피드) 그룹에서 **Update Now(**지금 업데이트**)**를 클릭합니다.

c) 또한 **Configure(**구성**)**를 클릭하여 피드에 대해 반복 업데이트를 설정합니다. 대부분의 네트워크에는 기본값인 **Hourly(**매시간**)**가 적절하지만 필요한 경우 빈도를 줄일 수 있습니다.

d) **Policies(**정책**)**를 클릭한 다음 **Security Intelligence(**보안 인텔리전스**)** 정책을 클릭합니다.

e) 정책을 아직 활성화하지 않은 경우 **Enable Security Intelligence(**보안 인텔리전스 활성화**)**를 클릭합니다.

f) **Network(**네트워크**)** 탭에서 차단/삭제 목록에 있는 **+**를 클릭하고 **Network Feeds(**네트워크 피드**)** 탭에서 모든 피드를 선택합니다. 피드 옆의 **i** 버튼을 클릭하면 각 피드의 설명을 확인할 수 있습니다.

아직 피드가 없다는 메시지가 표시되면 나중에 다시 시도하십시오. 피드 다운로드가 아직 완료되지 않은 것입니다. 이 문제가 계속되면 관리 IP 주소와 인터넷 간에 경로가 있는지 확인하십시오.

g) **OK(**확인**)**를 클릭하여 선택한 피드를 추가합니다.

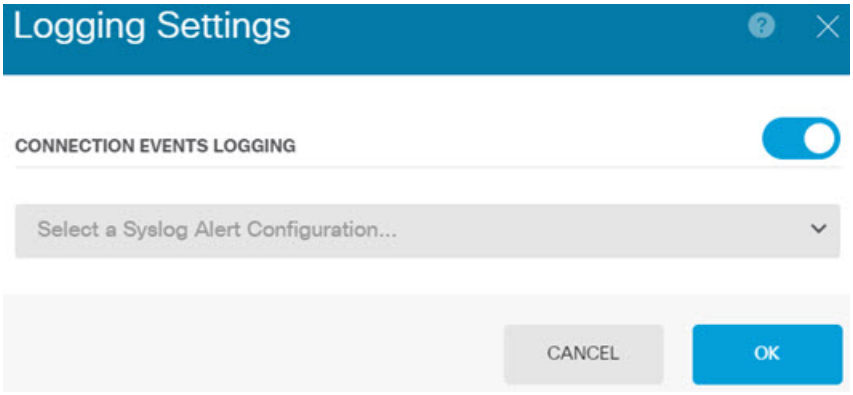
잘못된 IP 주소를 추가로 알고 있다면 **+** > **Network Objects(**네트워크 개체**)**를 클릭하고 해당 주소가 포함된 개체를 추가할 수 있습니다. 목록 아래쪽의 **Create New Network Object(**새 네트워크 개체 생성**)**를 클릭하면 지금 해당 개체를 추가할 수 있습니다.

h) **URL** 탭을 클릭한 다음 차단/삭제 목록에 있는 **+** > **URL Feeds(URL** 피드**)**를 클릭하고 모든 URL 피드를 선택합니다. **OK(**확인**)**를 클릭하여 목록에 추가합니다.

네트워크 목록과 마찬가지로 목록에 자체 URL 개체를 추가해 피드에 없는 추가 사이트를 차단할 수 있습니다. **+** > **URL Objects(URL** 개체**)**를 클릭합니다. 목록 끝에 있는 **Create New URL Object(**새 **URL** 개체 생성**)**를 클릭하면 새 개체를 추가할 수 있습니다.

i) 기어 아이콘을 클릭하고 **Connection Events Logging(**연결 이벤트 로깅**)**을 활성화하여 일치하는 연결에 대해 정책이 보안 인텔리전스 이벤트를 생성하는 정책을 활성화합니다. **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

연결 로깅을 활성화하지 않으면 정책이 예상대로 작업을 수행하고 있는지 여부를 평가하는 데 사용할 데이터가 제공되지 않습니다. 외부 syslog 서버를 정의한 경우에는 해당 서버로도 이벤트가 전송되도록 지금 해당 서버를 선택할 수 있습니다.



j) 필요한 경우 각 탭의 **Do Not Block(**차단 안 함**)** 목록에 네트워크 또는 URL 개체를 추가하여 차단된 목록에 대한 예외를 생성할 수 있습니다.

Do Not Block(차단 안 함**)** 목록은 실제 "허용" 목록이 아닙니다. 예외 목록입니다. 예외 목록의 주소나 URL이 차단 목록에도 나타나는 경우 해당 주소나 URL에 대한 연결을 액세스 제어 정책으로 전달할 수 있습니다. 이 방법을 통해 특정 피드를 차단할 수 있습니다. 그러나 원하는 주소나 사이트가 차단되고 있음이 나중에 확인되는 경우에는 피드를 완전히 제거할 필요 없이 예외

목록을 사용하여 해당 차단을 재정의할 수 있습니다. 이러한 연결은 나중에 액세스 제어 및 침입 정책(구성된 경우)을 통해 평가됩니다. 따라서 침입 검사 중에 위협을 포함하는 연결을 식별하여 차단할 수 있습니다.

Access and SI Rules(액세스 및 SI 규칙) 대시보드와 이벤트 뷰어의 Security Intelligence(보안 인텔리전스) 보기를 사용하면 정책에 의해 실제로 삭제되는 트래픽, 그리고 **Do Not Block(**차단 안 함**)** 목록에 주소나 URL을 추가해야 하는지 여부를 확인할 수 있습니다.

단계 **6** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 공격자, 대상 및 위협에 대한 정보가 표시됩니다(침입이 식별된 경우). 이 정보를 평가하여 네트워크에 추가 보안 조치가 필요한지 아니면 사용 중인 침입 정책의 레벨을 낮춰야 하는지를 결정할 수 있습니다.

보안 인텔리전스의 경우 Access and SI Rules(액세스 및 SI 규칙) 대시보드에서 정책 적중 횟수를 확인할 수 있습니다. 이벤트 뷰어에서도 보안 인텔리전스 이벤트를 확인할 수 있습니다. 트래픽은 검사 가능한 시점 이전에 차단되므로 보안 인텔리전스 차단은 침입 위협 정보에 반영되지 않습니다.

악성코드를 차단하는 방법

사용자가 인터넷 사이트 또는 이메일 등의 기타 통신 방법을 통해 악성 소프트웨어(악성코드)를 유입할 위험성은 항상 존재합니다. 신뢰할 수 있는 웹 사이트 역시 하이재킹되어 이러한 사이트를 의심하지 않는 사용자에게 악성코드를 전파할 수 있습니다. 웹 페이지는 여러 소스에서 제공되는 개체를 포함할 수 있습니다. 이러한 개체에는 이미지, 실행 파일, Javascript, 광고 등이 포함될 수 있습니다. 보안 침해된 웹 사이트의 경우 외부 소스에서 호스팅되는 개체가 통합되어 있는 경우가 많습니다. 철저한 보안을 유지하려면 초기 요청뿐 아니라 각 개체를 개별적으로 확인해야 합니다.

악성코드 방어를 사용해 악성코드를 탐지하기 위해 파일 정책을 사용합니다. 파일 제어를 수행하는 데에도 파일 정책을 사용할 수 있습니다. 그러면 파일에 악성코드가 있는지와 관계없이 특정 유형의 모든 파일에 대한 제어가 가능합니다.

악성코드 방어는 Secure Malware Analytics Cloud를 사용하여 네트워크 트래픽에서 탐지될 가능성이 있는 악성코드의 상태를 검색합니다. 관리 인터페이스에는 Secure Malware Analytics Cloud에 연결하고 악성코드 조회를 수행하기 위한 인터넷으로 연결되는 경로가 있어야 합니다. 디바이스는 적합한 파일을 탐지하면 파일의 SHA-256 해시 값을 사용하여 Secure Malware Analytics Cloud에서 파일의 상

태를 쿼리합니다. 가능한 상태는 **clean(**정상**)**, **malware(**악성코드**)** 또는 **unknown(**알 수 없음**)**(명확한 판정 없음)입니다. Secure Malware Analytics Cloud에 연결할 수 없는 경우의 상태는 **unknown(**알 수 없음**)**입니다.

파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 연결의 파일을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 **allow(**허용**)**하는 규칙에 대해서만 파일 정책을 구성할 수 있습니다. 트래픽을 **trust(**신뢰**)** 또는 **block(**차단**)**하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다.

프로시저

단계 **1** 아직 수행하지 않은 경우 악성코드 및 위협 라이선스를 활성화합니다.

침입 정책에 필요한 위협 라이선스 외에 파일 정책을 사용하려면 악성코드를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 계정에 추가해야 합니다.

a) 디바이스를 클릭합니다.

b) 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

c) 악성코드 그룹에서 **Enable(**활성화**)**을 클릭합니다. 아직 활성화되지 않은 경우 위협 그룹입니다.

시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 Disable(비활성화) 버튼으로 변경됩니다.

단계 **2** 하나 이상의 액세스 규칙에 대해 파일 정책을 선택합니다.

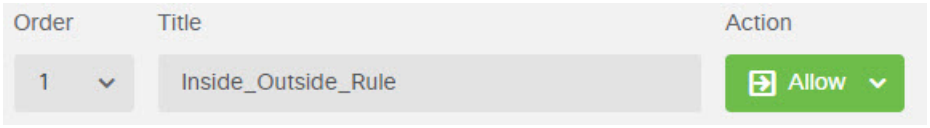
악성코드를 검사해야 하는 트래픽에 적용할 규칙을 결정합니다. 이 예에서는 Inside_Outside_Rule에 파일 검사를 추가합니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

b) Inside_Outside_Rule 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.

c) **Action(**작업**)**에 대해 **Allow(**허용**)**를 아직 선택하지 않았으면 선택합니다.



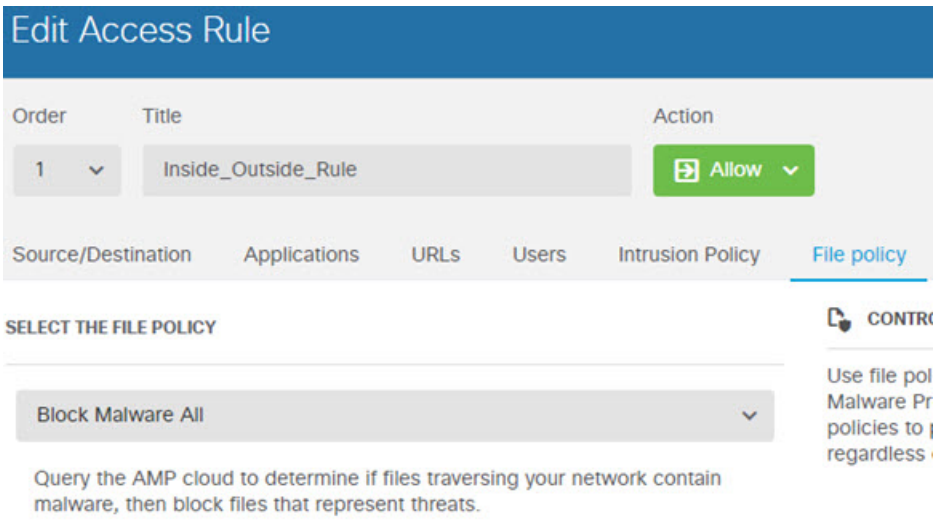
d) **File Policy(**파일 정책**)** 탭을 클릭합니다.

e) 사용하려는 파일 정책을 클릭합니다.

선택할 수 있는 주요 항목은 악성코드로 간주되는 모든 파일을 삭제하는 **Block Malware All(**악성코드 모두 차단**)**이나, 파일 상태를 확인하기 위해 Secure Malware Analytics Cloud를 쿼리하지만 차단은 수행하지 않는 **Cloud Lookup All(**클라우드 모두 조회**)**입니다. 먼저 파일을 평가하는 방법을 확인하려는 경우 클라우드 조회를 사용합니다. 파일을 평가하는 방법이 적절한 경우 나중에 차단 정책으로 전환할 수 있습니다.

악성코드를 차단하는 다른 정책도 제공됩니다. 이러한 정책은 파일 제어와 결합되어 Microsoft Office 또는 Office 및 PDF, 문서 업로드를 차단합니다. 즉, 이러한 정책은 악성코드를 차단할 뿐 아니라 사용자가 다른 네트워크로 이러한 파일 유형을 전송할 수 없도록 합니다. 요구에 맞는 경우 이러한 정책을 선택하면 됩니다.

이 예에서는 **Block Malware All(**악성코드 모두 차단**)**을 선택합니다.



f) **Logging(**로깅**)** 탭을 클릭하고 파일 이벤트 아래에서 **Log Files(**로그 파일**)**이 선택되어 있는지 확인합니다.

기본값으로, 파일 정책을 선택할 때마다 파일 로깅이 활성화됩니다. 이벤트와 대시보드에서 파일 및 악성코드 정보를 확인하려면 파일 로깅을 활성화해야 합니다.

g) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 파일 유형과 파일 및 악성코드 이벤트에 대한 정보가 표시됩니다(파일 또는 악성코드가 전송된 경우). 이 정보를 평가하여 네트워크에 파일 전송과 관련된 추가 보안 조치가 필요한지를 결정할 수 있습니다.

사용 제한 정책**(URL** 필터링**)**을 구현하는 방법

네트워크에 대한 사용 제한 정책이 있을 수 있습니다. 사용 제한 정책은 조직에서 적절한 네트워크 활동과 부적절한 것으로 간주되는 활동을 구별합니다. 이러한 정책은 대개 인터넷 사용량을 중점적으로 파악하며 생산성을 유지하고, 법적 책임을 방지(예: 적대적이지 않은 업무 환경 유지)하고, 웹 트래픽을 전반적으로 제어할 수 있도록 작성되어 있습니다.

URL 필터링을 사용하여 액세스 정책을 통해 사용 제한 정책을 정의할 수 있습니다. 그러면 도박 등의 광범위한 범주를 필터링할 수 있으므로 차단해야 하는 모든 개별 웹 사이트를 식별할 필요가 없습니다. 범주가 일치하는 경우 허용하거나 차단할 사이트의 상대적 평판을 지정할 수도 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, Cisco의 위협 인텔리전스는 새로운 URL, 새로운 범주 및 기존 URL의 새로운 범주와 위험이 적용되어 지속적으로 업데이트되므로 시스템은 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 구축하는 것보다 빠르게 나타났다 사라질 수 있습니다.

다음 절차에서는 URL 필터링을 사용하여 사용 제한 정책을 구현하는 방법을 설명합니다. 이 예에서는 여러 카테고리의 사이트(모든 평판), 위험한 소셜 네트워킹 사이트 및 분류되지 않은 사이트인 badsite.example.com을 차단합니다.

프로시저

단계 **1** **URL** 라이선스를 아직 활성화하지 않은 경우 활성화합니다.

URL 카테고리 및 평판 정보를 사용하거나 대시보드 및 이벤트에서 해당 정보를 확인하려면 URL 라이선스를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 어카운트에 추가해야 합니다.

a) 디바이스를 클릭합니다.
b) 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

c) **URL** 라이선스 그룹에서 **Enable(**활성화**)**을 클릭합니다.

시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 Disable(비활성화) 버튼으로 변경됩니다.

단계 **2** URL 필터링 액세스 제어 규칙을 생성합니다.

차단 규칙을 만들기 전에 먼저 사용자들이 방문하는 사이트의 범주를 확인하고자 할 수 있습니다. 이 경우 금융과 같이 허용 가능한 카테고리에 대해 허용 작업을 사용하여 규칙을 생성할 수 있습니다. URL이 이 카테고리에 속하는지를 확인하려면 모든 웹 연결을 검사해야 하므로 금융 사이트 이외의 사이트에 대해서도 카테고리 정보를 가져옵니다.

하지만 차단할 것임을 이미 알고 있는 URL 카테고리도 있을 수 있습니다. 차단 정책은 검사도 강제 수행하므로 차단된 범주뿐 아니라 차단되지 않은 범주에 대한 연결 관련 범주 정보도 가져오게 됩니다.

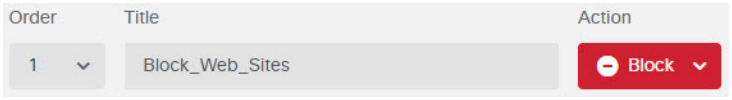
a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

b) **+**를 클릭하여 새 규칙을 추가합니다.
c) 순서, 제목 및 작업을 구성합니다.

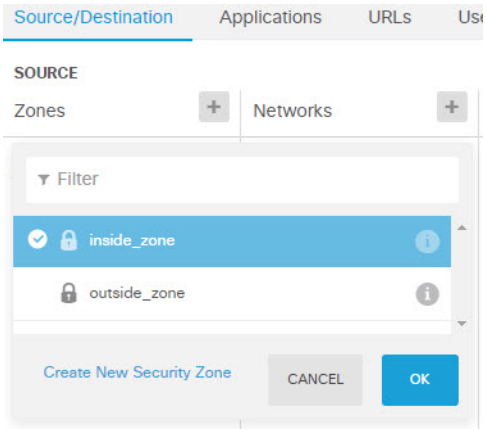
- **Order(**순서**)** - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 소스/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙에서는 초기 디바이스 컨피그레이션 중에 생성한 Inside_Outside_Rule과 같은 소스/대상을 사용합니다. 다른 규칙도 생성했을 수 있습니다. 액세스 제어 효율성을 최대화하려면 특정 규칙을 미리 생성해 두는 것이 좋습니다. 그러면 연결을 허용할지 아니면 삭제할지를 가장 빠르게 결정할 수 있습니다. 이 예시에서는 규칙 순서로 **1**을 선택합니다.

- **Title(**제목**)** - Block_Web_Sites와 같이 의미 있는 이름을 규칙에 지정합니다.
- **Action(**작업**)** - **Block(**차단**)**을 선택합니다.

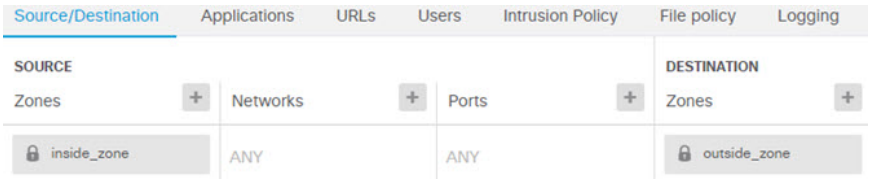


d) **Source/Destination(**소스/대상**)** 탭에서 **Source(**소스**)** > **Zones(**영역**)**의 **+**를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(**확인**)**를 클릭합니다.

기준을 추가하는 과정도 동일한 방식으로 수행합니다. **+**를 클릭하면 열리는 작은 대화 상자에서 추가할 항목을 클릭합니다. 여러 항목을 클릭할 수 있으며, 선택한 항목을 클릭하면 선택이 취소됩니다. 선택한 항목에는 확인 표시가 나타납니다. 그러나 **OK(**확인**)** 버튼을 클릭할 때까지는 정책에 아무 항목도 추가되지 않으므로 항목만 선택하는 것으로는 충분하지 않습니다.



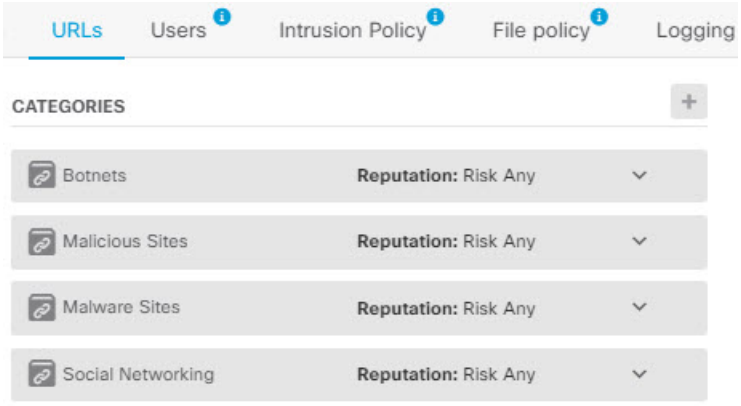
e) 동일한 기술을 사용하여 **Destination(**대상**)** > **Zones(**영역**)**에 대해 **outside_zone**을 선택합니다.



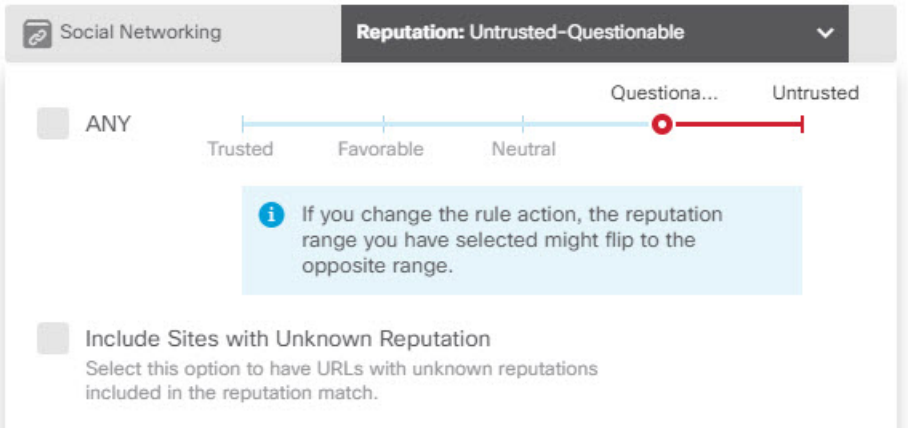
f) **URLs(URL)** 탭을 클릭합니다.

g) 범주의 **+**를 클릭하고 완전히 차단하거나 부분적으로 차단할 범주를 선택합니다.

이 예에서는 봇넷, 악성 사이트, 악성코드 사이트 및 소셜 네트워킹을 선택합니다. 차단해야 할 가능성이 높은 추가 범주도 있습니다. 차단하려는 사이트에 관해 알고 있지만 어떤 카테고리인지 확실하지 않은 경우, **URL to Check(**확인할 **URL)** 필드에 URL을 입력하고 **Go(**이동**)**를 클릭합니다. 그러면 조회 결과를 표시하는 웹 사이트로 이동합니다.



h) 소셜 네트워킹 카테고리에 대해 평판별 차단을 구현하려면 해당 카테고리에 대해 **Reputation: Risk Any(**평판**:** 모든 위험**)**를 클릭하고 **Any(**모두**)**를 선택 취소한 후에 슬라이더를 **Questionable(**의심스러움**)**로 이동합니다. 슬라이더 바깥쪽을 클릭하면 슬라이더가 닫힙니다.



평판 슬라이더의 왼쪽은 허용할 사이트를, 오른쪽은 차단할 사이트를 나타냅니다. 이 경우 평판이 Questionable(의심스러움) 및 Untrusted(신뢰할 수 없음) 범위에 속하는 소셜 네트워킹 사이트만 차단됩니다. 따라서 사용자는 위험성이 적은 흔히 사용되는 소셜 네트워킹 사이트에 액세스할 수 있습니다.

평판을 알 수 없는 URL을 평판 일치에 포함하려면 **Include Sites with Unknown Reputation(**평판을 알 수 없는 사이트 포함**)** 옵션을 선택합니다. 새 사이트는 일반적으로 등급이 지정되지 않으며, 사이트의 평판을 알 수 없거나 확인할 수 없는 다른 이유가 있을 수 있습니다.

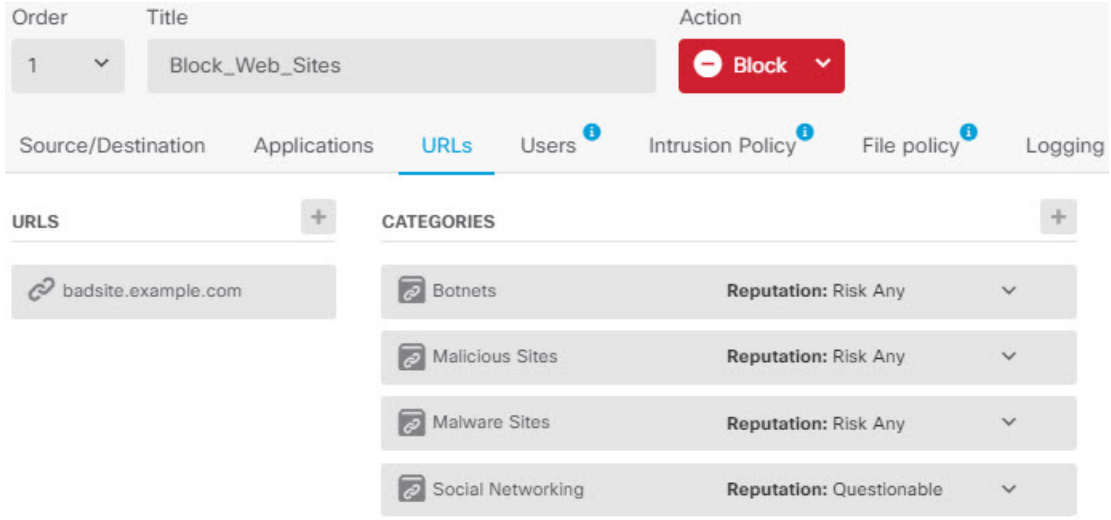
평판을 사용하면 일반적으로는 허용할 범주 내의 사이트를 선택적으로 차단할 수 있습니다.

i) 범주 목록 왼쪽의 **URL** 목록 옆에 있는 **+**를 클릭합니다.
j) 팝업 대화 상자 하단의 새 **URL** 생성 링크를 클릭합니다.
k) 이름과 URL에 모두 **badsite.example.com**을 입력하고 확인을 클릭하여 개체를 생성합니다.

개체 이름은 URL과 동일하게 지정해도 되고 다른 이름을 지정해도 됩니다. URL의 경우 URL의 프로토콜 부분은 포함하지 말고 서버 이름만 추가합니다.

l) 새 개체를 선택한 다음 **OK(**확인**)**를 클릭합니다.

정책을 수정하는 중에 새 개체를 추가하면 목록에 개체가 추가되지만, 새 개체가 자동으로 선택되지는 않습니다.



m) **Logging(**로깅**)** 탭을 클릭하고 **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.

웹 범주 대시보드 및 연결 이벤트로 범주 및 평판 정보를 가져오려면 로깅을 활성화해야 합니다.

n) **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **3** (선택 사항). URL 필터링을 위한 기본 설정을 지정합니다.

URL 라이선스를 활성화하면 시스템에서 웹 범주 데이터베이스에 대한 업데이트를 자동으로 활성화합니다. 시스템은 30분마다 업데이트를 확인하지만, 데이터는 대개 매일 한 번씩 업데이트됩니다. 이러한 업데이트를 적용하지 않으려는 경우에는 업데이트를 끌 수 있습니다.

또한, 분석을 위해 Cisco에 분류되지 않은 URL을 전송하도록 선택할 수도 있습니다. 설치된 URL 데이터베이스에 사이트에 대한 분류가 없어도 Cisco Cloud에는 있을 수 있습니다. 이 경우 클라우드는 범주와 평판을 반환하며, 그러면 범주 기반 규칙을 URL 요청에 올바르게 적용할 수 있습니다. 메모리 제한으로 인해 더 작은 URL 데이터베이스를 설치하는 저가형 시스템에서는 이 옵션을 반드시 선택해야 합니다. 조회 결과에 대해 TTL(Time to Live)을 설정할 수 있습니다. 기본값은 조회 결과를 새로 고치지 않는 Never(안 함)입니다.

a) 디바이스를 클릭합니다.
b) **System Settings(**시스템 설정**)** > **Traffic Settings(**트래픽 설정**)** > **URL Filtering Preferences(URL** 필터링 기본 설정**)**를 클릭합니다.
c) **Cisco CSI**에서 알 수 없는 **URL** 쿼리를 선택합니다.
d) 24시간 등의 적절한 **URL Time to Live(URL Time to Live)**를 선택합니다.
e) **Save(**저장**)**를 클릭합니다.

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 URL 카테고리 및 평판 그리고 삭제된 연결에 대한 정보가 표시되어야 합니다. 이 정보를 평가하여 URL 필터링이 부적절한 사이트만 삭제하는지 또는 특정 범주에 대한 평판 설정을 완화해야 하는지를 확인할 수 있습니다.

범주와 평판을 기준으로 웹 사이트 액세스를 차단할 것임을 사용자에게 미리 알리는 것이 좋습니다.

애플리케이션 사용량을 제어하는 방법

웹은 기업에 애플리케이션을 제공하는 데 흔히 사용되는 플랫폼으로 자리잡았습니다. 브라우저 기반 애플리케이션 플랫폼이 사용될 수도 있고, 기업 네트워크 안팎으로 애플리케이션을 전송하는 방법으로 웹 프로토콜을 사용하는 리치 미디어 애플리케이션이 사용될 수도 있습니다.

Threat Defense 연결을 검사하여 사용 중인 애플리케이션을 확인합니다. 따라서 특정 TCP/UDP 포트만 대상으로 하는 것이 아니라 애플리케이션을 대상으로 하는 액세스 제어 규칙을 작성할 수 있습니다. 그러므로 같은 포트를 사용하는 웹 기반 애플리케이션도 선택적으로 허용하거나 차단할 수 있습니다.

허용하거나 차단할 특정 애플리케이션을 선택할 수도 있지만, 유형/범주/태그/위험/사업 타당성을 기준으로 규칙을 작성할 수도 있습니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플

리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

이 활용 사례에서는 익명성 도구/프록시 범주에 속하는 모든 애플리케이션을 차단합니다.

시작하기 전에

이 활용 사례에서는 네트워크 트래픽을 파악하는 방법, 7 페이지 활용 사례를 완료했다고 가정합니다. 해당 활용 사례에서는 애플리케이션 사용량 정보를 수집하는 방법을 설명합니다. 이 정보는 애플리케이션 대시보드에서 분석할 수 있습니다. 실제로 사용 중인 애플리케이션을 파악하면 효율적인 애플리케이션 기반 규칙을 디자인하는 데 도움이 될 수 있습니다. VDB 업데이트를 예약하는 방법도 해당 활용 사례에 설명되어 있으므로 이 활용 사례에서 반복 설명하지 않습니다. 애플리케이션을 올바르게 식별할 수 있도록 VBD를 정기적으로 업데이트해야 합니다.

프로시저

단계 **1** 애플리케이션 기반 액세스 제어 규칙을 생성합니다.

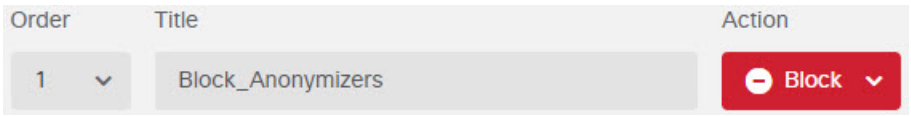
a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

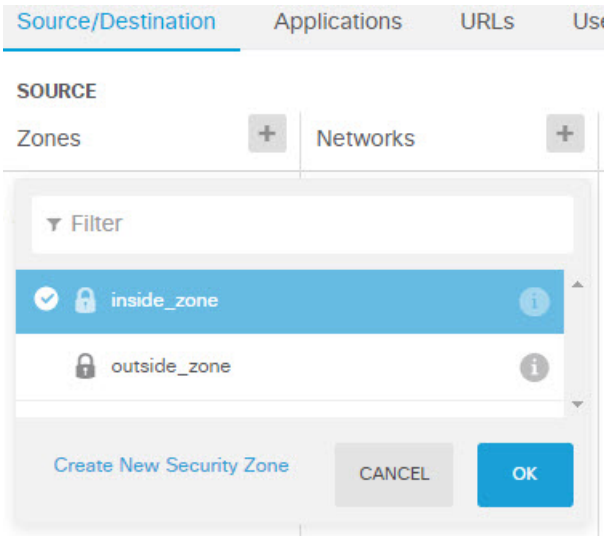
b) **+**를 클릭하여 새 규칙을 추가합니다.

c) 순서, 제목 및 작업을 구성합니다.

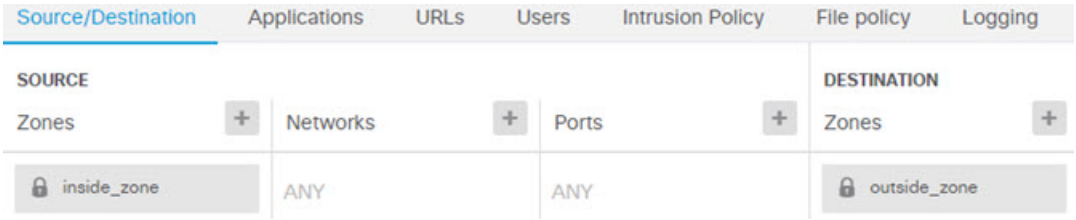
- **Order(**순서**)** - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 소스/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙에서는 초기 디바이스 컨피그레이션 중에 생성한 Inside_Outside_Rule과 같은 소스/대상을 사용합니다. 다른 규칙도 생성했을 수 있습니다. 액세스 제어 효율성을 최대화하려면 특정 규칙을 미리 생성해 두는 것이 좋습니다. 그러면 연결을 허용할지 아니면 삭제할지를 가장 빠르게 결정할 수 있습니다. 이 예시에서는 규칙 순서로 **1**을 선택합니다.
- **Title(**제목**)** - Block_Anonymizers와 같이 의미 있는 이름을 규칙에 지정합니다.
- **Action(**작업**)** - **Block(**차단**)**을 선택합니다.



d) **Source/Destination(**소스/대상**)** 탭에서 **Source(**소스**)** > **Zones(**영역**)**의 **+**를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(**확인**)**를 클릭합니다.



e) 동일한 기술을 사용하여 **Destination(**대상**)** > **Zones(**영역**)**에 대해 **outside_zone**을 선택합니다.



f) **Applications(**애플리케이션**)** 탭을 클릭합니다.

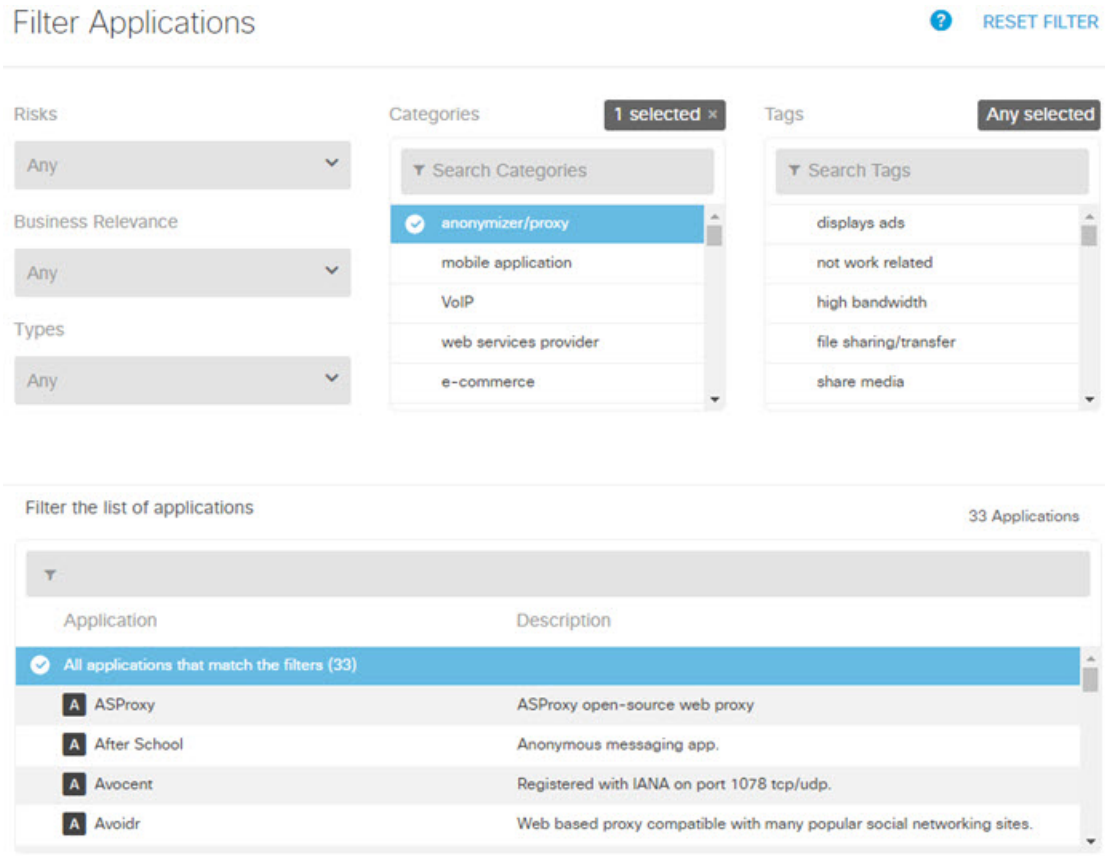
g) 애플리케이션에 대해 +를 클릭하고 팝업 대화 상자 하단의 **Advanced Filter(**고급 필터**)** 링크를 클릭합니다.

애플리케이션 필터 개체를 미리 생성해 두었다가 여기서 애플리케이션 필터 목록을 통해 선택할 수도 있지만, 액세스 제어 규칙에서 기준을 직접 지정하고 필요에 따라 기준을 필터 개체로 저장할 수도 있습니다. 단일 애플리케이션용 규칙을 작성하는 경우가 아니면 고급 필터 대화 상자를 사용하여 애플리케이션을 찾고 적절한 기준을 생성하는 것이 더 쉽습니다.

기준을 선택하면 대화 상자 하단의 애플리케이션 목록이 업데이트되어 기준과 일치하는 정확한 애플리케이션이 표시됩니다. 작성하는 규칙은 이러한 애플리케이션에 적용됩니다.

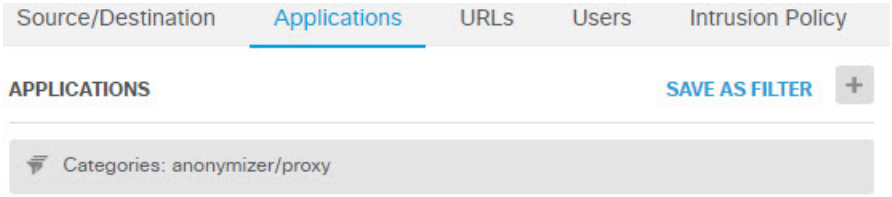
이 목록을 자세히 확인하십시오**.** 예를 들어 위험도가 매우 높은 애플리케이션은 모두 차단하는 경우가 많습니다. 하지만 이 문서를 작성하는 시점에서 Facebook과 TFTP도 위험도가 매우 높은 애플리케이션으로 분류되어 있습니다. 대부분의 조직은 해당 애플리케이션을 차단하기를 원치 않을 것입니다. 시간을 할애하여 다양한 필터 기준을 적용해 보고 선택한 필터와 일치하는 애플리케이션을 확인하십시오. 이러한 목록은 VDB가 업데이트될 때마다 변경될 수 있습니다.

이 예에서는 범주 목록에서 익명성 도구/프록시를 선택합니다.



h) 고급 필터 대화 상자에서 **Add(**추가**)**를 클릭합니다.

필터가 추가되어 애플리케이션 탭에 표시됩니다.



i) **Logging(**로깅**)** 탭을 클릭하고 **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.

이 규칙에 의해 차단되는 연결에 대한 정보를 확인하려면 로깅을 활성화해야 합니다.

j) **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **2** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

단계 **3** **Monitoring(**모니터링**)**을 클릭하고 결과를 평가합니다.

이제 애플리케이션 위젯의 네트워크 개요 대시보드에 삭제된 연결이 표시됩니다. **All(**모두**)/Denied(**거부됨**)/Allowed(**허용됨**)** 드롭다운 옵션을 사용하여 삭제된 애플리케이션만 확인합니다.

Web Applications(웹 애플리케이션**)** 대시보드에서 애플리케이션 정보를 확인할 수도 있습니다. **Applications(**애플리케이션**)** 대시보드에는 프로토콜 관련 결과가 표시됩니다. 특정 사용자가 이러한 애플리케이션 사용을 시도하는 경우, ID 정책을 활성화하고 인증을 요구한다는 가정 하에 연결을 시도하는 사용자와 애플리케이션 간의 상관관계를 파악할 수 있어야 합니다.

서브넷을 추가하는 방법

디바이스에 사용 가능한 인터페이스가 있으면 스위치나 다른 라우터에 유선으로 연결하여 다른 서브넷에 서비스를 제공할 수 있습니다.

서브넷은 여러 가지 이유로 인해 추가할 수 있습니다. 이 활용 사례의 경우에는 다음과 같은 일반적인 시나리오를 위해 서브넷을 연결합니다.

- 서브넷은 프라이빗 네트워크 192.168.2.0/24를 사용하는 내부 네트워크입니다.
- 네트워크의 인터페이스 고정 주소는 192.168.2.1입니다. 이 예에서 실제 인터페이스는 네트워크 전용입니다. 이미 유선으로 연결된 인터페이스를 사용하고 새 네트워크용으로 하위 인터페이스를 생성할 수도 있습니다.
- 디바이스는 DHCP를 사용하여 네트워크의 워크스테이션에 주소를 제공하며, 주소 풀 192.168.2.2-192.168.2.254를 사용합니다.
- 다른 내부 네트워크와 외부 네트워크에 대한 네트워크 액세스가 허용됩니다. 외부 네트워크로 이동하는 트래픽은 NAT를 사용하여 공용 주소를 가져옵니다.

참고 이 예에서는 사용되지 않는 인터페이스가 브리지 그룹의 일부분이 아니라고 가정합니다. 현재 해당 인터페이스가 브리지 그룹 멤버인 경우에는 먼저 브리지 그룹에서 인터페이스를 제거해야 이 절차를 수행할 수 있습니다.

시작하기 전에

새 서브넷의 스위치와 인터페이스에 네트워크 케이블을 물리적으로 연결합니다.

프로시저

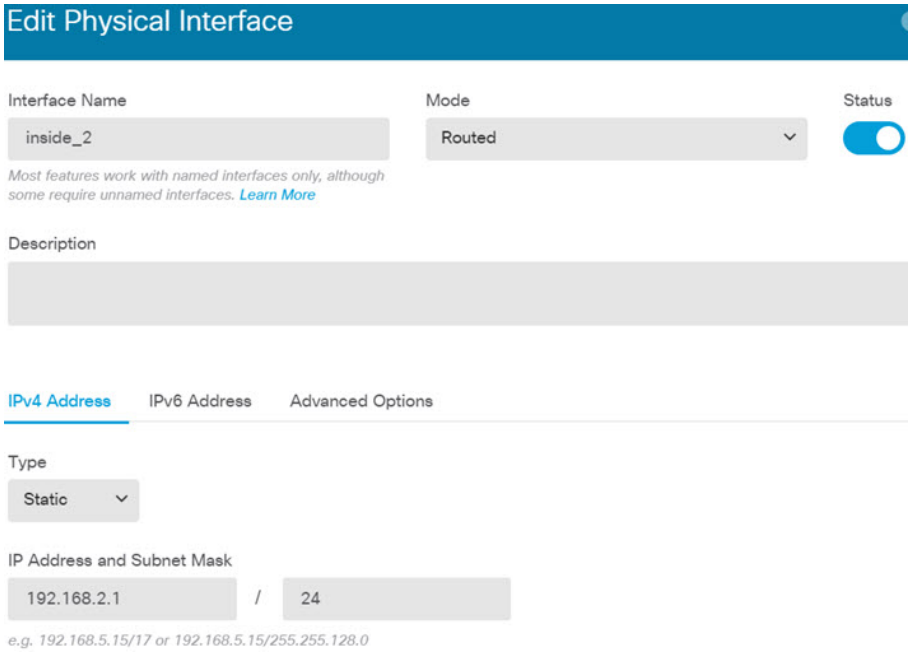
단계 **1** 인터페이스를 구성합니다.

a) **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, 인터페이스 유형을 클릭하여 인터페이스 목록을 확인합니다.

b) 유선으로 연결한 인터페이스 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려놓고 수정 아이콘()을 클릭합니다.

c) 기본 인터페이스 속성을 구성합니다.

- **Name(**이름**)** - 인터페이스의 고유한 이름입니다. 이 예에서 이름은 **inside_2**입니다.
- **Mode(**모드**)** - **Routed(**라우팅**)**를 선택합니다.
- **Status(**상태**)** - 상태 토글을 클릭하여 인터페이스를 활성화합니다.
- **IPv4 Address(IPv4** 주소**)** 탭 - 유형으로 고정을 선택하고 **192.168.2.1/24**를 입력합니다.



d) **Save(**저장**)**를 클릭합니다.

인터페이스 목록에 업데이트된 인터페이스 상태와 구성된 IP 주소가 표시됩니다.

단계 **2** 인터페이스용 DHCP 서버를 구성합니다.

a) 디바이스를 클릭합니다.

b) **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**를 클릭합니다.

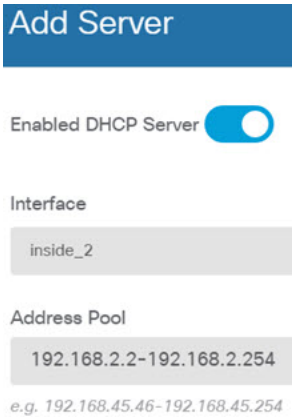
c) **DHCP Servers(DHCP** 서버**)** 탭을 클릭합니다.

테이블에 기존 DHCP 서버가 나열됩니다. 기본 컨피그레이션을 사용하는 경우 목록에는 내부 인터페이스용 DHCP 서버가 포함되어 있습니다.

d) 테이블 위의 +를 클릭합니다.

e) 서버 속성을 구성합니다.

- **Enable DHCP Server(DHCP** 서버 활성화**)** - 이 토글을 클릭하여 서버를 활성화합니다.
- **Interface(**인터페이스**)** - DHCP 서비스를 제공할 인터페이스를 선택합니다. 이 예에서는 inside_2를 선택합니다.
- **Address Pool(**주소 풀**)** - 서버가 네트워크의 디바이스에 제공할 수 있는 주소입니다. 192.168.2.2-192.168.2.254를 입력합니다. 네트워크 주소(.0), 인터페이스 주소(.1) 또는 브로드캐스트 주소(.255)는 포함하지 마십시오. 또한 네트워크의 디바이스에 고정 주소가 필요한 경우 해당 주소를 풀에서 제외합니다. 풀은 연속하는 주소의 단일 시리즈여야 하므로 범위 시작이나 끝에서 고정 주소를 선택합니다.



f) **Add(**추가**)**를 클릭합니다.

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	**inside**	Enabled	192.168.1.5-192.168.1.254
2	**inside_2**	Enabled	192.168.2.2-192.168.2.254

단계 **3** 내부 보안 영역에 인터페이스를 추가합니다.

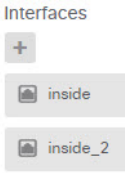
인터페이스에서 정책을 작성하려면 인터페이스가 보안 영역에 속해야 합니다. 보안 영역에 대한 정책을 작성합니다. 그러므로 영역에서 인터페이스를 추가하거나 제거하면 인터페이스에 적용되는 정책이 자동으로 변경됩니다.

a) 주 메뉴에서 **Objects(**개체**)**를 클릭합니다.

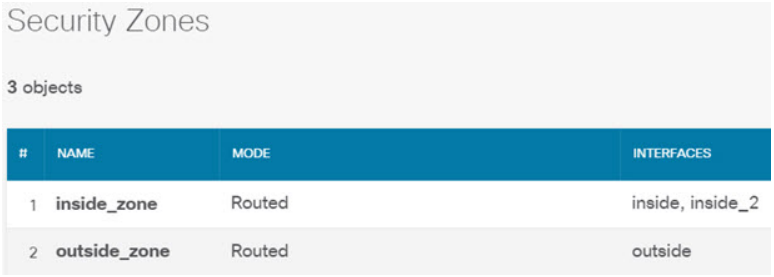
b) 개체 목차에서 **Security Zones(**보안 영역**)**을 선택합니다.

c) **inside_zone** 개체 행 오른쪽의 **Actions(**작업**)** 셀 위에 마우스를 올려놓고 수정 아이콘( )을 클릭합니다.

d) 인터페이스 아래의 +를 클릭하고 inside_2 인터페이스를 선택한 후에 인터페이스 목록에서 **OK(**확인**)**를 클릭합니다.



e) **Save(**저장**)**를 클릭합니다.



단계 **4** 내부 네트워크 간에 트래픽을 허용하는 액세스 제어 규칙을 생성합니다.

트래픽은 인터페이스 간에 자동으로 허용되지 않습니다. 원하는 트래픽을 허용하는 액세스 제어 규칙을 생성해야 합니다. 단, 액세스 제어 규칙의 기본 작업에서 트래픽을 허용하는 경우는 예외입니다. 이 예에서는 디바이스 설정 마법사가 구성하는 차단 기본 작업을 유지했다고 가정합니다. 따라서 내부 인터페이스 간에 트래픽을 허용하는 규칙을 생성해야 합니다. 이러한 규칙을 이미 생성했다면 이 단계를 건너뛰십시오.

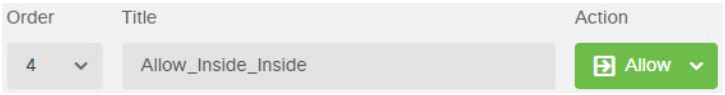
a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.

Access Control(액세스 제어**)** 정책이 표시되는지 확인합니다.

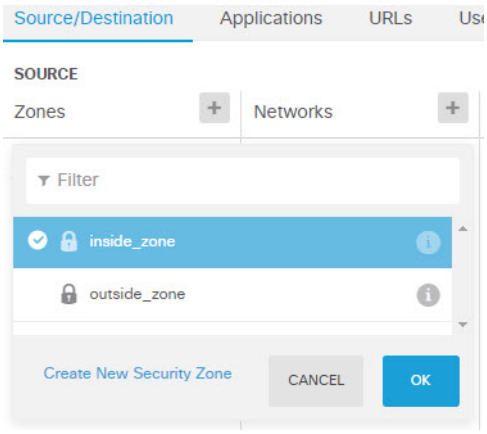
b) +를 클릭하여 새 규칙을 추가합니다.

c) 순서, 제목 및 작업을 구성합니다.

- **Order(**순서**)** - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 소스/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙의 경우에는 고유한 소스/대상 기준을 사용할 것이므로 목록 끝에 규칙을 추가하면 됩니다.
- **Tile(**제목**)** - Allow_Inside_Inside와 같이 의미 있는 이름을 규칙에 지정합니다.
- **Action(**작업**)** - **Allow(**허용**)**를 선택합니다.

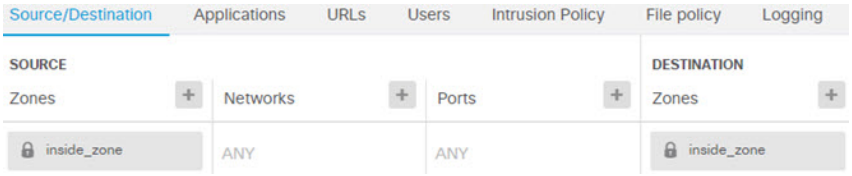


d) **Source/Destination(**소스/대상**)** 탭에서 **Source(**소스**)** > **Zones(**영역**)**의 +를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(**확인**)**를 클릭합니다.



e) 동일한 기술을 사용하여 **Destination(**대상**)** > **Zones(**영역**)**에 대해 **inside_zone**을 선택합니다.

소스와 대상에 대해 같은 영역을 선택하려면 보안 영역이 둘 이상의 인터페이스를 포함해야 합니다.



f) (선택 사항). 침입 및 악성코드 검사를 구성합니다.

내부 인터페이스가 신뢰할 수 있는 영역에 있기는 하지만 사용자는 일반적으로 랩톱을 네트워크에 연결합니다. 따라서 사용자가 의도치 않게 외부 네트워크나 Wi-Fi 핫스팟에서 네트워크 내부로 위협 요소를 유입할 수 있습니다. 그러므로 내부 네트워크 사이를 이동하는 트래픽에서 침입 및 악성코드를 검사할 수 있습니다.

이와 관련하여 다음 사항을 고려하십시오.

- **Intrusion Policy(**침입 정책**)** 탭을 클릭하고 침입 정책을 활성화한 다음 슬라이더를 사용하여 Balanced Security and Connectivity(보안과 연결의 균형 유지) 정책을 선택합니다.
- **File Policy(**파일 정책**)** 탭을 클릭한 후 악성코드 모두 차단 정책을 선택합니다.

g) **Logging(**로깅**)** 탭을 클릭하고 **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.

이 규칙과 일치하는 연결에 대한 정보를 확인하려면 로깅을 활성화해야 합니다. 로깅을 사용하면 대시보드에 통계가 추가되며 이벤트 뷰어에 이벤트가 표시됩니다.

h) **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **5** 새 서브넷에 대해 필요한 정책이 정의되어 있는지 확인합니다.

inside_zone 보안 영역에 인터페이스를 추가하면 inside_zone에 대한 모든 기존 정책이 새 서브넷에 자동으로 적용됩니다. 그러나 시간을 할애하여 정책을 검사해 추가 정책이 필요하지 않은지 확인해야 합니다.

초기 디바이스 컨피그레이션을 완료한 경우에는 다음 정책이 이미 적용되어 있어야 합니다.

- 액세스 제어 - Inside_Outside_Rule은 새 서브넷과 외부 네트워크 간의 모든 트래픽을 허용합니다. 이전 활용 사례를 따른 경우 이 정책은 침입 및 악성코드 검사 기능도 제공합니다. 새 네트워크와 외부 네트워크 간의 일부 트래픽을 허용하는 규칙이 있어야 합니다. 그렇지 않으면 사용자가 인터넷 또는 기타 외부 네트워크에 액세스할 수 없습니다.
- **NAT** - InsideOutsideNATrule은 외부 인터페이스로 이동하는 모든 인터페이스에 적용되며 인터페이스 PAT를 적용합니다. 이 규칙을 유지한 경우 새 네트워크에서 외부로 이동하는 트래픽의 IP 주소가 외부 인터페이스 IP 주소에서 고유한 포트로 변환됩니다. 모든 인터페이스 또는 inside_zone 인터페이스에 적용되는 규칙이 없으면 외부 인터페이스로 이동할 때 새 규칙을 생성해야 할 수 있습니다.
- **ID** - 기본 ID 정책은 없습니다. 그러나 이전 활용 사례를 따른 경우 새 네트워크에 대한 인증을 요구하는 ID 정책이 이미 있을 수 있습니다. 적용되는 ID 정책이 없는 경우 새 네트워크에 대해 사용자 기반 정보를 확인하려면 ID 정책을 생성합니다.

단계 **6** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

다음에 수행할 작업

새 서브넷의 워크스테이션이 DHCP를 사용하여 IP 주소를 받으며, 다른 내부 네트워크 및 외부 네트워크에 연결할 수 있는지 확인합니다. 모니터링 대시보드 및 이벤트 뷰어를 사용하여 네트워크 사용량을 평가합니다.

네트워크에서 트래픽을 능동적으로 모니터링하는 방법

threat defense 디바이스는 대개 액티브 방화벽 및 IPS(Intrusion Prevention System) 보안 디바이스로 구축됩니다. 이 디바이스의 핵심 기능은 부적절한 연결과 위협을 삭제하는 활성 네트워크 보호를 제공하는 것입니다.

그러나 패시브 모드로 시스템을 구축할 수도 있습니다. 이 모드에서는 디바이스가 모니터링되는 스위치 포트의 트래픽을 분석만 합니다. 이 모드는 주로 데모 또는 테스트용입니다. 즉, 디바이스를 액티브 방화벽으로 구축하기 전에 패시브 모드에서 디바이스 사용법을 파악할 수 있습니다. 패시브 구축을 사용하는 경우 네트워크에 나타나는 위협의 종류, 사용자가 탐색 중인 URL 카테고리 등을 모니터링할 수 있습니다.

패시브 모드는 보통 데모나 테스트에만 사용하지만, IDS(침입 탐지 시스템, 방지 기능 없음) 등 필요한 서비스를 제공하는 경우에는 생산 환경에서도 패시브 모드를 사용할 수 있습니다. 패시브 인터페이스와 액티브 방화벽 라우티드 인터페이스를 함께 사용하면 조직에 필요한 서비스 조합을 정확하게 제공할 수 있습니다.

다음 절차에서는 시스템을 패시브 방식으로 구축하여 제한된 수의 스위치 포트를 통해 들어오는 트래픽을 분석하는 방법을 설명합니다.

참고 이 예시는 하드웨어 threat defense 디바이스용입니다. threat defense virtual에도 수동 모드를 사용할 수는 있지만, 네트워크 설정이 다릅니다. 자세한 내용은 Threat Defense Virtual 패시브 인터페이스의 VLAN 구성를 참조해 주십시오. 그렇지 않으면 threat defense virtual에 이 절차가 적용됩니다.

시작하기 전에

이 절차에서는 내부 및 외부 인터페이스를 연결했으며 초기 디바이스 설정 마법사를 완료했다고 가정합니다. 패시브 구축 시에도 시스템 데이터베이스용 업데이트 다운로드를 위한 인터넷 연결이 필요합니다. 또한 관리 인터페이스에 연결하여 device manager를 열 수 있어야 합니다. 내부 또는 관리 포트에 직접 연결하면 됩니다.

또한 이 예에서는**Policies(**정책**)** > **Intrusion(**침입**)** 페이지에서 침입 정책에 대해 시스템 로그를 활성화했다고 가정합니다.

프로시저

단계 **1** 스위치 포트를 SPAN(Switched Port Analyzer) 포트로 구성하고 소스 인터페이스에 대해 모니터링 세션을 구성합니다.

다음 예시에서는 Cisco Nexus Series 스위치의 소스 인터페이스 2개에 대해 SPAN 포트 및 모니터링 세션을 설정합니다. 다른 유형의 스위치를 사용하는 경우 필요한 명령이 달라질 수 있습니다.

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

설정을 확인하려면 다음 명령을 실행합니다.

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
```

```
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

단계 **2** threat defense 인터페이스를 스위치의 SPAN 포트에 연결합니다.

threat defense 디바이스에서 현재 사용하지 않는 포트를 선택하는 것이 가장 좋습니다. 예시 스위치 컨피그레이션을 기준으로 하는 경우 스위치의 이더넷 1/48에 케이블을 연결합니다. 이 인터페이스가 모니터링 세션의 대상 인터페이스입니다.

단계 **3** 수동 모드에서 threat defense 인터페이스를 컨피그레이션하십시오.

a) **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **Interfaces** 또는 **EtherChannel**를 클릭합니다.

b) 수정할 물리적 인터페이스 또는 EtherChannel의 수정 아이콘( )을 클릭합니다.

현재 사용되지 않는 인터페이스를 선택합니다. 사용 중인 인터페이스를 패시브 인터페이스로 변환하려는 경우 먼저 모든 보안 영역에서 인터페이스를 제거하고 해당 인터페이스를 사용하는 다른 모든 컨피그레이션을 제거해야 합니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

d) 다음을 구성합니다.

- **Interface Name(**인터페이스 이름**)** - 인터페이스의 이름(최대 48자)입니다. 영문자는 소문자로 입력해야 합니다. 예를 들어 **monitor**를 입력합니다.
- **Mode(**모드**)** - **Passive(**패시브**)**를 선택합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **4** 인터페이스에 대해 패시브 보안 영역을 생성합니다.

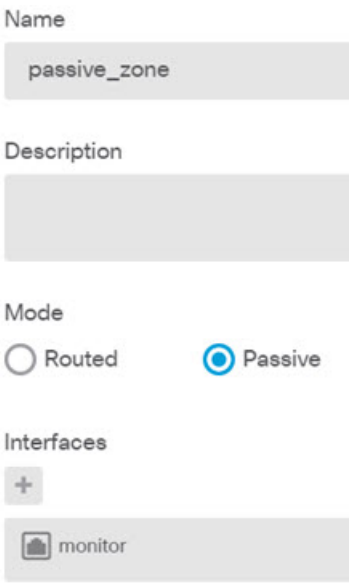
a) 목차에서 **Objects(**개체**)**와 **Security Zones(**보안 영역**)**을 차례로 선택합니다.

b) + 버튼을 클릭합니다.

c) 개체의 **Name(**이름**)** 및 설명(선택 사항)을 입력합니다. 예를 들어 **passive_zone**을 입력합니다.

d) **Mode(**모드**)**로는 **Passive(**패시브**)**를 선택합니다.

e) +를 클릭하고 패시브 인터페이스를 선택합니다.



f) **OK(**확인**)**를 클릭합니다.

단계 **5** 패시브 보안 영역에 대해 액세스 제어 규칙을 하나 이상 구성합니다.

생성하는 규칙의 수와 유형은 수집하려는 정보에 따라 달라집니다. 예를 들어 시스템을 IDS(Intrusion Detection System)로 구성하려는 경우 침입 정책이 할당된 Allow(허용) 규칙이 하나 이상 필요합니다. URL 카테고리 데이터를 수집하려는 경우에는 URL 카테고리 사양이 포함된 규칙이 하나 이상 필요합니다.

Block(차단) 규칙을 생성하면 실제 라우팅 인터페이스에서 시스템이 차단하는 연결을 확인할 수 있습니다. 인터페이스가 패시브이므로 이러한 연결이 실제로 차단되지는 않습니다. 하지만 시스템이 네트워크의 트래픽을 정리한 방식을 명확하게 확인할 수 있습니다.

다음 사용 사례에서는 액세스 제어 규칙의 기본적인 사용법을 다룹니다. 이러한 사용법은 패시브 인터페이스에도 적용됩니다. 생성하는 규칙의 보안 영역으로 패시브 보안 영역을 선택하면 됩니다.

- 위협을 차단하는 방법, 15 페이지
- 악성코드를 차단하는 방법, 20 페이지
- 사용 제한 정책(URL 필터링)을 구현하는 방법, 23 페이지
- 애플리케이션 사용량을 제어하는 방법, 28 페이지

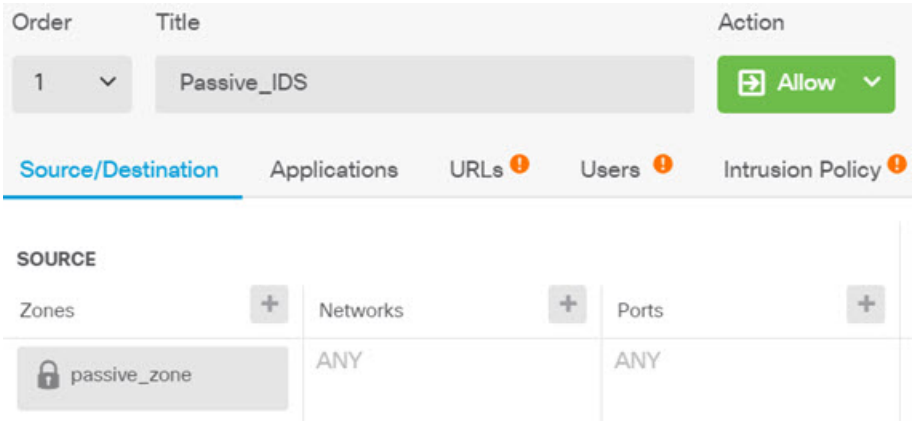
다음 절차에서는 침입 정책을 적용하고 URL 카테고리 데이터를 수집하기 위한 Allow(허용) 규칙 2개를 생성합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.
b) **+**를 클릭하여 모든 트래픽을 허용하되 침입 정책을 적용하는 규칙을 추가합니다.
c) 규칙 순서로 **1**을 선택합니다. 이 규칙은 기본 규칙보다 구체적이지만 기본 규칙과 겹치지는 않습니다. 맞춤형 규칙이 이미 있는 경우 적절한 위치를 선택합니다. 그래야 패시브 인터페이스로의 트래픽이 새로 추가하는 규칙 대신 해당 규칙과 일치하는 상황이 발생하지 않습니다.
d) 규칙의 이름(예: **Passive_IDS**)을 입력합니다.

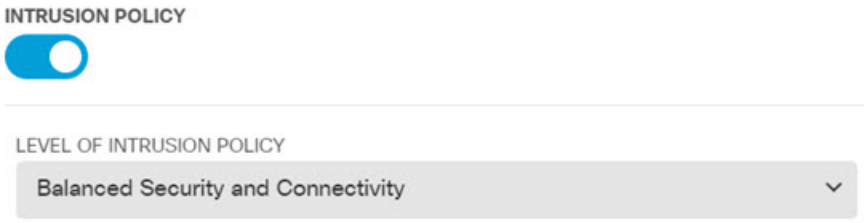
e) **Action(**작업**)**으로 **Allow(**허용**)**를 선택합니다.

f) **Source/Destination(**소스/대상**)** 탭의 **Source(**소스**)** > **Zones(**영역**)** 아래에서 패시브 영역을 선택합니다. 해당 탭의 다른 옵션은 구성하지 마십시오.

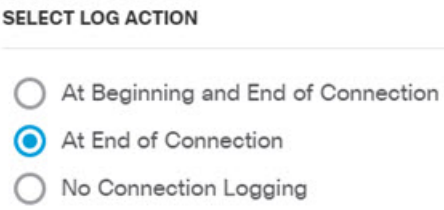
평가 모드에서 실행하는 경우 이 시점에서 규칙은 다음과 같이 표시됩니다.



g) **Intrusion Policy(**침입 정책**)** 탭을 클릭하고 슬라이더를 클릭하여 **On(**켜기**)**으로 전환한 다음 대다수 네트워크에 권장되는 **Balanced Security and Connectivity(**균형 잡힌 보안 및 연결성**)** 정책과 같은 침입 정책을 선택합니다.



h) **Logging(**로깅**)** 탭을 클릭하고 로깅 옵션으로 **At End of Connection(**연결 종료 시**)**을 선택합니다.



i) **OK(**확인**)**를 클릭합니다.

j) +를 클릭하여 시스템이 심층 검사를 수행해 모든 HTTP 요청의 URL 및 카테고리를 확인해야 하도록 하는 규칙을 추가합니다.

이 규칙을 사용하면 대시보드에서 URL 카테고리 정보를 확인할 수 있습니다. 시스템은 처리 시간을 절약하고 성능을 개선하기 위해 URL 카테고리 조건을 지정하는 액세스 제어 규칙이 하나 이상 있을 때만 URL 카테고리를 확인합니다.

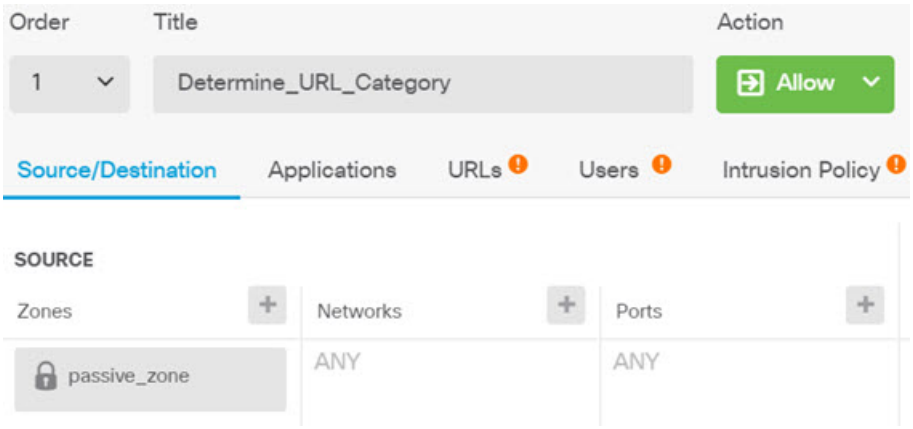
k) 규칙 순서로 **1**을 선택합니다. 그러면 해당 규칙이 이전 규칙(Passive_IDS) 위에 배치됩니다. 지금 생성하는 규칙은 해당 규칙(모든 트래픽에 적용됨) 뒤에 배치하면 어떤 트래픽과도 일치하지 않게 됩니다.

l) 규칙의 이름(예: **Determine_URL_Category**)을 입력합니다.

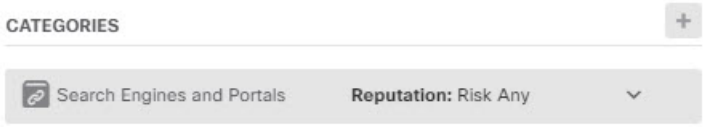
m) **Action(**작업**)**으로 **Allow(**허용**)**를 선택합니다.

Block(차단**)**을 선택할 수도 있습니다. 둘 중 어떤 작업을 선택하든 이 규칙을 추가하는 목표는 달성됩니다.

n) **Source/Destination(**소스/대상**)** 탭의 **Source(**소스**)** > **Zones(**영역**)** 아래에서 패시브 영역을 선택합니다. 해당 탭의 다른 옵션은 구성하지 마십시오.



o) **URLs(URL)** 탭을 클릭하고 **Categories(**카테고리**)** 머리글 옆의 +를 클릭한 다음 원하는 카테고리를 선택합니다. 예를 들어 **Search Engines and Portals(**검색 엔진 및 포털**)**를 선택합니다. 선택적으로 평판도를 선택할 수도 있고 기본값인 Any(모두)로 유지할 수도 있습니다.



p) **Intrusion Policy(**침입 정책**)** 탭을 클릭하고 슬라이더를 클릭하여 **On(**켜기**)**으로 전환한 다음 첫 번째 규칙에 대해 선택한 것과 같은 침입 정책을 선택합니다.

q) **Logging(**로깅**)** 탭을 클릭하고 로깅 옵션으로 **At End of Connection(**연결 종료 시**)**을 선택합니다.

그러나 작업으로 **Block(**차단**)**을 선택한 경우에는 **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다. 차단된 연결 자체가 종료되지는 않으므로 연결 시작 시에만 로그 정보가 제공됩니다.

r) **OK(**확인**)**를 클릭합니다.

단계 **6** (선택 사항). 다른 보안 정책을 구성합니다.

다음 보안 정책을 구성하여 트래픽에 어떤 영향을 주는지를 확인할 수도 있습니다.

- **Identity(ID)** - 사용자 정보를 수집합니다. 소스 IP 주소와 연관된 사용자를 식별할 수 있도록 ID 정책의 규칙을 구성할 수 있습니다. 패시브 인터페이스용 ID 정책 구현 프로세스는 라우팅 인터

페이스용 프로세스와 같습니다. 네트워크 트래픽을 파악하는 방법, 7 페이지에 설명된 사용 사례를 따르십시오.

- **Security Intelligence(**보안 인텔리전스**)** - 알려진 잘못된 IP 주소와 URL을 차단합니다. 자세한 내용은 위협을 차단하는 방법, 15 페이지를 참조해 주십시오.

참고 패시브 인터페이스의 암호화된 트래픽은 모두 암호 해독 불가로 분류되므로 SSL 암호 해독 규칙은 적용되지 않으며 패시브 인터페이스에 적용되지 않습니다.

단계 **7** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭합니다.

구축이 완료될 때까지 기다리거나 **OK(**확인**)**를 클릭하고 나중에 작업 목록 또는 구축 기록을 확인할 수 있습니다.

단계 **8** 모니터링 대시보드를 사용하여 네트워크를 통해 들어오는 트래픽과 위협의 종류를 분석합니다. threat defense 디바이스가 원치 않는 연결을 능동적으로 삭제하도록 하려는 경우, 모니터링하는 네트워크에 대해 방화벽 보호를 제공하는 액티브 라우팅 인터페이스를 컨피그레이션할 수 있도록 디바이스를 재구축하십시오.

추가 예시

사용 사례 장의 예시와 더불어, 특정 서비스를 설명하는 일부 장에도 예시 컨피그레이션이 나와 있습니다. 다음과 같은 예시를 확인할 수 있습니다.

액세스 제어

- TrustSec SGT(Security Group Tag)를 사용하여 네트워크 액세스를 제어하는 방법

NAT(Network Address Translation)

IPv4 주소에 대한 **NAT**

- 내부 웹 서버에 대한 액세스 제공(고정 자동 NAT)
- FTP, HTTP 및 SMTP용 단일 주소(포트 변환 고정 자동 NAT)
- 대상에 따라 다른 변환(동적 수동 PAT)
- 대상 주소 및 포트에 따라 다른 변환(동적 수동 PAT)
- DNS 회신 수정, 외부의 DNS 서버
- DNS 회신 수정, 호스트 네트워크의 DNS 서버

- NAT에서 사이트 대 사이트 VPN 트래픽 제외

IPv6 주소에 대한 **NAT**

- NAT64/46 예: 내부 IPv6 네트워크 및 외부 IPv4 인터넷
- NAT64/46 예: 내부 IPv6 네트워크와 외부 IPv4 인터넷 및 DNS 변환
- NAT66 예, 네트워크 간의 고정 변환
- NAT66 예, 간단한 IPv6 인터페이스 PAT
- DNS 64 회신 수정

RA VPN(Remote Access Virtual Private Network)

- RADIUS CoA(Change of Authorization) 구현 방법
- Duo LDAP를 사용하여 이중 인증을 구성하는 방법
- 원격 액세스 VPN 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝)
- 원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법
- 그룹별로 RA VPN 액세스를 제어하는 방법
- RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법
- Secure Client 아이콘 및 로고를 맞춤화하는 방법

사이트 대 사이트 **VPN(Virtual Private Network)**

- NAT에서 사이트 대 사이트 VPN 트래픽 제외
- 외부 사이트 대 사이트 VPN 사용자에게 외부 인터페이스를 통해 인터넷 액세스를 제공하는 방법(헤어피닝)
- 사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법

SSL/TLS 암호 해독

- 예: 네트워크에서 이전 SSL/TLS 버전 차단

FlexConfig 정책

- 전역 기본 검사를 활성화/비활성화하는 방법
- FlexConfig 변경 사항을 실행 취소하는 방법
- 고유한 트래픽 클래스에 대한 검사를 활성화하는 방법

가상 라우팅

- 중복된 어드레스 스페이스가 있는 여러 가상 라우터에 인터넷 액세스를 제공하는 방법

- 여러 가상 라우터를 통해 원거리 서버로 라우팅하는 방법
- RA VPN 액세스를 다른 가상 라우터의 내부 네트워크에 허용하는 방법
- 사이트 간 VPN을 통해 여러 가상 라우터의 네트워크에서 트래픽을 보호하는 방법