시스코 Firepower Next Generation Firewall 6.2 Lab v1

마지막 업데이트: 2017 년 10 월 31 일

본 데모에 대하여

사전에 구성되어 있는 이 데모는 아래 내용으로 구성되어 있습니다:

NOTE: 한번에 모든 시나리오를 진행하지 않는게 좋습니다. 이 데모는 총 6 시간 정도 소요됩니다. 어떤 시나리오를 진행할지는 다음 내용을 참고하십시오.

- 전체 진행은 시나리오 1 과 시나리오 2 를 기본적으로 수행해야 합니다. 이 작업은 반드시 완료돼야 하며 순서대로 진행해야 합니다.
- 시나리오 3 ~ 6 은 리모트 접속 VPN 에 대해 보다 자세히 설명합니다. RA VPN 구성에 대한 기본적인 이해를 시나리오 3 을 완료하는 것만으로 충분합니다.
- 시나리오 13 은 시나리오 10 의 정적 NAT 구성을 사용합니다.

필요사항

아래 항목은 랩 진행에 필요한 구성요소입니다

테이블 1. 필요사항

필수	옵션
• 랩탑 컴퓨터	• 시스코 AnyConnect®

솔루션에 대하여

현재 전세계의 소비자, 기업 및 정부는 혁신을 위해 디지털화를 보다 적극적으로 활용함에 따라 이전보다 더 많은 연결성을 이용한 디지털 혁신을 겪고 있습니다. 그러나 우리가 더 많이 연결할 수록 사이버 범죄가 일어날 수 있는 기회도 같이 늘어납니다. 오늘날 이와 같은 환경에서 기업을 보다 효과적으로 운영하기 위해서는, 빠르게 변화하고 있는 환경에서 나날이 진화하고 있는 위협을 차단하기 위한 노력에 더더욱 집중해야 합니다.

전통적으로 IT 팀은 애플리케이션 기반으로 위협차단 기능을 제공해왔던 전통적인 차세대 방화벽(NGFW)과 같이 포인트 솔루션에 대한 패치 작업을 수행해 왔습니다. 하지만 이러한 전통적인 NGFW 은 현재의 위협을 근본적으로 해결하기 위한 컨텍스트 정보 이용, 자동화 및 우선 순위와 같은 기능을 제공 할 수 없습니다. 정교한 해킹 및 멀웨어보다 한 걸음 앞서 나아가려면, 위협에 신속히 대응할 수 있도록 포괄적인 네트워크 가시성, 위협 정보 및 회귀분석 기술을 제공하는 완벽히 통합된 보안 솔루션을 필요로 합니다.

Cisco Firepower 4100 시리즈 NGFW 은 업계 최초로 통합 위협에 초점을 맞춘 차세대 방화벽으로 이와 같은 문제를 해결합니다.

Cisco Firepower NGFW 은 설계 단계부터 조직을 보다 안전하게 지킬 수 있도록 만들어졌습니다. Firepower NGFW 은 운영자가 관리 부담을 줄일 수 있도록 단일 인터페이스를 제공하기 때문에 통합 보안에 따른 운영 비용과 복잡성을 줄여줍니다. 일반적으로 기업내에서 보안 기능이 추가됨에 따라 쌓여만 가는 어플라이언스 및 관리 콘솔 스택은 우리가 원하던 접근 방식이 아닙니다.

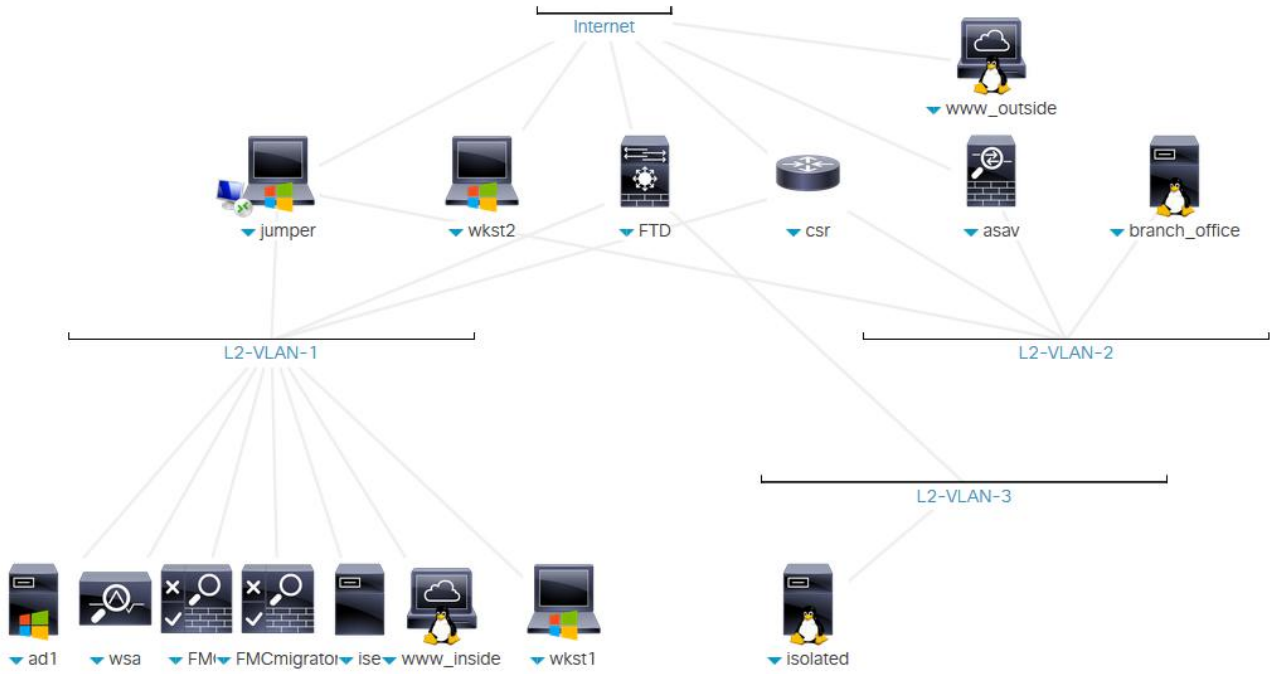
이와 같이 Cisco Firepower NGFW 은 기업이 위협에 실시간으로 대응할 수 있도록 공격을 차단하고, 우선 순위를 정하며 상황을 이해한 뒤 그에 따른 대응을 자동화 할 수 있도록 발전해 왔습니다. Firepower NGFW 은 기존에 알려진 혹은 알려지지 않은 공격에 대하여 포괄적인 네트워크 가시성, 최상의 위협 정보 및 효과적인 위협 방지 기능을 통해 문제를 해결합니다. Firepower NGFW 은 또한 Advanced Malware Protection(AMP) 기능을 통해 공격이 성공한 시점 이전으로 거슬러 올라가 침투한 공격을 신속하게 찾아서 해결할 수 있는 회귀분석 기능을 제공합니다. 이로 인해 시스코 고객은 업계 평균 TTD (시스템에 침투한 공격을 발견하는데까지 소요된 시간, Time-to-Detection)를 크게 감소시켰습니다.

Cisco Firepower NGFW 은 AMP 기능을 엔드 포인트까지 확장시켜 고객의 문제를 해결합니다. 그리고 엔드 포인트 AMP, Threat Grid 및 Cisco ISE (Identity Services Engine)를 플랫폼에 완벽히 통합시킴으로써 네트워크 인프라 뿐만이 아닌 엔드 포인트 영역까지 확장시켜 혁신적인 Firepower 기능을 제공합니다.

구성도

본 데모는 시나리오의 원활한 진행 및 솔루션이 제공하는 기능들의 동작 확인을 위해 사전 설정된 구성요소들을 포함하고 있습니다. 대부분의 구성요소들은 별도 제공되는 관리자 계정을 통해 구성이 가능하고 **토폴로지** 메뉴에 있는 각 구성요소 아이콘을 클릭하면 해당 구성요소에 접근하기 위한 IP 어드레스 및 계정 정보를 확인할 수 있습니다.

Figure 1. dCloud 구성도



dCloud 시작하기

프리젠테이션에 앞서

고객 및 파트너를 대상으로 데모시연을 할 경우 원활한 진행을 위해 본 자료를 가지고 사전에 충분한 연습을 하시기를 권장합니다. 데모 완료 후 새롭게 구성을 해야 하는 경우는 세션을 다시 예약하십시오.

사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.

세션 예약 및 데모환경을 준비하기 위하여 아래 절차를 따라 주십시오.

1. dCloud 세션을 시작. [가이드]

노트: 세션 예약 후 시아리오의 랩이 활성화 되기까지 최대 10 분 소요됩니다.

2. 시스코 dCloud 의 리모트 데스크탑 클라이언트를 이용해 접속하십시오. [가이드]

노트: 시스코 AnyConnect VPN 클라이언트 [가이드] 및 **이용자 컴퓨터에 있는 로컬 RDP 클라이언트**[가이드]를 이용한 접속도 가능합니다.

Jumper: **198.18.133.50**, 이용자명: **administrator**, 패스워드: **C1sco12345**

시나리오 1. REST API 를 이용한 장비 구성

이 시나리오 랩에서는 간단한 방식으로 NGFW 을 구성하며 대부분 REST API python 스크립트를 이용해 진행합니다. 진행하기에 앞서 먼저 예비 단계를 수행해야합니다. 그리고 라우팅 구성은 아직 REST API 를 지원하지 않으므로 직접 수행해야합니다.

스텝

FMC 관리를 위한 NGFW 구성

1. Jumper 데스크탑에서 PuTTY 를 실행합니다. **NGFW** 라는 사전 구성된 세션을 클릭하여 연결합니다. 이용자명은 **admin**, 패스워드는 **C1sco12345** 를 사용하여 로그인하십시오.

노트: 특수 문자 입력이 잘 안되는 경우, Jumper 데스크톱에서 *Strings to cut and paste.txt* 파일을 열어 이용하십시오.

2. **configure manager add fmc.dcloud.local C1sco12345** 커맨드를 입력하십시오.
3. 커맨드 입력 후 뜨는 경고 내용을 확인합니다.
4. 계속할지 묻는 질문에 **yes** 로 대답하십시오. **y** 는 입력하지 마십시오. 만약 **yes** 대신 **y** 를 입력하면 명령 기본값은 **no** 입니다.

NGFW 은 on-box 매니지먼트(Firepower Device Manager 또는 FDM)가 활성화되어 있습니다. 기본 구성이 이렇기 때문에 경고메시지를 받은 것입니다. 참고로 본 데모에서는 on-box 매니지먼트를 실습하는 내용은 포함되어 있지 않지만 수동으로 해볼 수는 있습니다. 다만 현재의 NGFW 구성을 삭제하지 않으면 FDM 에서 FMC 로 전환 할 수 없습니다.

5. 이 PuTTY 세션은 닫지 않고 그대로 둡니다. 랩에서 계속 사용합니다.

FMC 에서 스마트 라이센스 활성화

Smart Licensing 을 사용해야합니다. 이 랩에서는 Built-in 방식의 90 일 평가판 라이센스를 사용합니다.

노트: 본 랩에서는 별도로 커스터마이징된 소프트웨어를 이용합니다. 실제 환경에서는 평가판 라이센스를 이용해 RA VPN 구성을 할 수 없습니다.

1. Jumper 데스크탑에서 Firefox 브라우저를 열어 Firepower Management Center (FMC) 바로가기를 클릭합니다. 로그인 정보는 미리 입력되어 있습니다.
2. **Log In 을** 클릭합니다.
3. FMC 대시보드에서 **System > Licenses > Smart Licenses** 으로 이동하십시오.
4. **Evaluation Mode** 에 클릭하여 메시지가 나타나면 **Yes** 를 클릭하십시오.

NGFW 등록 및 구성을 위해 REST API 스크립트 실행

REST API 를 시연하기 위해, 아래 내용을 수행하는 Python 스크립트를 실행합니다.

1. Access control policy 를 생성.
2. FMC 에 NGFW 을 등록.
3. NGFW 의 인터페이스 구성.

우리가 사용할 스크립트는 데모 교육을 목적으로 제작되었기 때문에 완벽히 짜여져 있지 않습니다. 이 스크립트를 확인하려면 **/usr/local/bin** 에 있습니다**. register_config.py** 라고 불리우며 **connect.py** 에 의해 생성된 **Python** 모듈을 사용합니다. **runapiscript** 명령어는 **register_config.py** 에 대한 심볼릭 링크입니다. 이 스크립트는 가이드의 부록 B 에도 포함되어 있습니다.

4. Jumper 데스크탑에서 PuTTY 를 실행하십시오. **Inside Linux server** 서버 세션을 더블 클릭하십시오. **root**, 패스워드는 **C1sco12345** 를 사용하여 로그인하십시오.

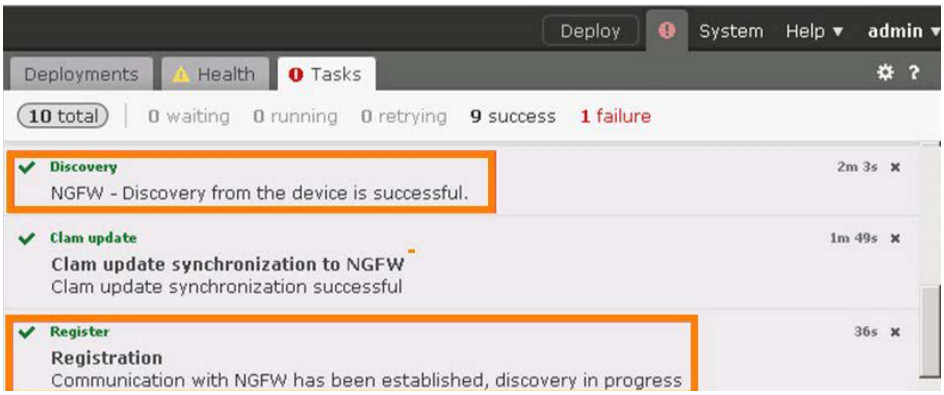
5. Inside Linux 서버 CLI 에서 **runapiscript** 를 실행하십시오.
    a. **Would you like to register the managed device? [y/n] 내용이 표시되면**, **y 를** 입력하고 **<Enter>** 키를 누릅니다.
    b. **enter an access control policy name** 메시지가 표시되면, **NGFW Access Control Policy** 같은 적절한 이름을 입력하십시오.
    c. 확인 메시지가 나타날 때까지 기다립니다.
    d. FMC UI 에서 장치 검색이(device discovery) 완료되었는지 확인한 다음 **y** 를 눌러 계속하거나 **n** 을 눌러 종료하십시오. [y/ n]
    e. 스크립트를 계속하기 전에 다음 단계로 진행하십시오.

노트: Discovery 가 완료 될 때까지 기다리지 않았다면 오류가 발생합니다. 이런 경우, 검색이 완료 될 때까지 기다렸다가 스크립트를 다시 실행하십시오. 그러나 이번에는 장치를 등록 할 것인지 묻는 메시지가 표시되면 **n** 을 입력하십시오.

6. FMC 에서 *Deploy* 버튼 오른쪽에있는 아이콘을 클릭하고 *Tasks* 탭을 선택합니다.
    a. 잠시 기다리십시오. 다음 작업까지 약 1 분 정도 걸립니다.

노트: Task 가 시작되지 않은채 1 분 이상 지속되면, 데모용 스마트 라이센스(demo Smart license)가 활성화됐는지 확인하십시오. 그렇지 않은 경우, 데모 스마트 라이센스를 활성화하고 **runapiscript** 스크립트를 다시 실행하십시오. Access control policy 는 다른 이름을 사용하거나 혹은 스크립트가 작성한 Policy 를 삭제하십시오.

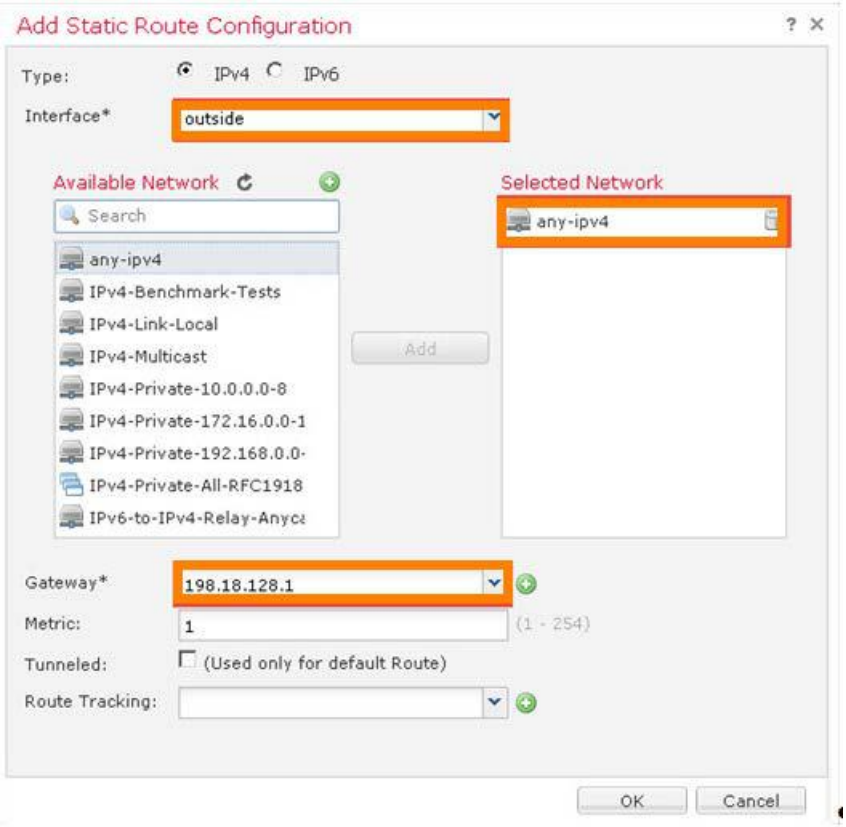
    b. Discovery 작업이 완료 될 때까지 기다립니다. 목록에 실패한 작업이 있는 경우는 걱정하지 마십시오. Registration 및 discovery 작업만 성공하면 됩니다.



7. Inside Linux 서버 CLI 에서 **`runapiscript`** 스크립트를 계속 진행하십시오.
    a. **y** 를 입력하고 **<Enter>** 키를 누릅니다.
    b. 요청시 **Would you like to configure device interfaces? [y/n]**, **y** 를 입력하고 **<Enter>** 키를 누릅니다. 스크립트 동작이 완료될 때까지 기다립니다.
    c. 이 PuTTY 세션은 닫지 않고 그대로 둡니다. 랩에서 계속 사용합니다.

디폴트 라우팅 구성

1. FMC 에서, **Devices > Device Management** 로 이동합니다. 연필 모양의 아이콘을 클릭하여 device 설정을 편집하십시오.
2. Interfaces 탭을 선택합니다. REST API 스크립트가 NGFW 의 inside 및 outside 인터페이스를 구성했는지 확인하십시오.
3. Routing 탭을 선택합니다.
    a. **Static Route** 선택하고 **Add Route** 버튼을 클릭하십시오.
    b. 아래 그림과 같이 outside 인터페이스에서 디폴트 라우팅 경로를 198.18.128.1 로 설정하십시오.
    c. **OK** 를 클릭합니다.



4. **Save** 를 클릭하여 라우팅 구성을 저장하십시오.

노트: 시간을 절약하려면 라우팅을 아직 구성하지 마십시오. 또한 **runapiscript** 스크립트는 시간을 절약하기 위해 인터페이스 구성 배포는 포함하지 않습니다. 다음 랩에서는 더 많은 설정 단계를 수행하며 변경된 내용을 함께 배포합니다.

시나리오 2. 기본 구성

이 연습은 다음 작업으로 구성됩니다:

- 연습에 필요한 오브젝트 생성
- Access control policy 수정
- NAT 정책 생성
- Network discovery 정책 수정
- 구성 변경사항 배포
- 구성한 NGFW 테스트
- 아웃 바운드 연결을 허용하고 다른 연결 시도는 차단함
- 아웃 바운드 연결에서 파일 유형 및 멀웨어 차단 수행
- 아웃 바운드 연결에 침입 차단(intrusion prevention) 기능의 제공

스텝

연습에 필요한 오브젝트 생성

1. **Objects > Object Management** 으로 이동합니다.
    a. **Add Network > Add Object** 를 클릭.
    b. **Name** 에, **Lab_Networks** 를 입력하십시오.
    c. **198.18.0.0/15** 를 입력합니다. 여기에는 랩에서 사용하는 모든 IP 주소를 포함됩니다.
    d. **Save** 를 클릭하십시오.
2. 왼쪽 창에서 **Interface** 를 선택하십시오..
    a. **Add > Security Zone** 을 클릭하십시오.

노트: 인터페이스 오브젝트에는 Security zones 과 Interface groups 두 가지 타입이 있습니다. 주요 차이점은 Interface groups 이 겹칠 수 있다는 것입니다. Access control policy 규칙에는 Security zones 만 사용할 수 있습니다.

    b. **Name** 에, **InZone** 을 입력하십시오. **Interface Type** 드롭 다운 메뉴에서 **Routed** 를 선택하십시오.
    c. Inside interface 를 선택하십시오. **Add** 를 클릭 한 다음 **Save** 을 클릭하십시오.
    d. **Add > Security Zone** 을 클릭하십시오.
    e. Name 에, **OutZone** 을 입력하십시오. Interface Type 드롭 다운 메뉴에서 **Routed** 를 선택하십시오.
    f. Outside interface 를 선택하십시오. **Add** 를 클릭 한 다음 **Save** 을 클릭하십시오.

Access control policy 수정

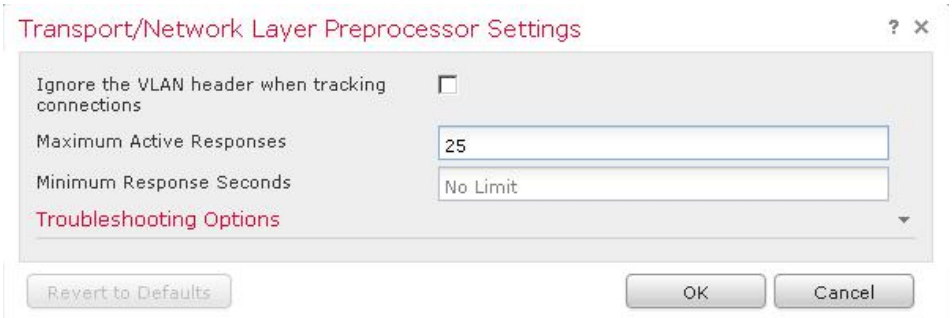
1. **Policies > Access Control > Access Control** 으로 이동하십시오. Access control policy 는 REST API 스크립트를 통해 작성되었습니다.
2. Policy 의 오른쪽에 있는 **연필모양 아이콘**을 클릭하여 Access control policy 를 편집하십시오.
3. **Add Rule** 클릭.
    a. Name 에, **Allow Outbound Connections** 을 입력하십시오.
    b. **Insert** 드롭 다운 목록에서 **into Default** 를 선택하십시오.

노트: 규칙은 정책 내에 세트로 나뉩니다. 두 세트가 미리 정의되어 있습니다:
• 하위 정책의 규칙보다 우선하는 필수(Mandatory) 규칙
• 하위 정책의 규칙 뒤에 평가되는 기본(Default) 규칙
이 연습에서 하위 정책을 만들지는 않습니다. 다만 기본 규칙 세트를 이용하여 해당 규칙이 마지막에 평가되는지를 손쉽게 확인할 수 있습니다.

    c. **Zones** 탭이 이미 선택되어져야 합니다.
        i. **InZone** 을 선택하고 **Add to Source** 를 클릭합니다.
        ii. **OutZone 을** 선택하고 **Add to Destination** 을 클릭합니다.
    d. **Inspection** 탭을 선택하십시오.
        i. **Intrusion Policy** 드롭 다운 목록에서 **Demo Intrusion Policy** 을 선택하십시오.
        ii. **File Policy** 드롭 다운 목록에서 **Demo File Policy** 을 선택하십시오.

노트: 데모 침입 및 파일 정책은 시간을 절약을 위해 사전에 구성되었습니다. 구성 방법에 대한 내용은 부록 A 를 참조하십시오.

    e. **Add** 를 클릭하여 규칙을 추가하십시오.
4. **HTTP Responses** 탭을 선택하십시오.
5. **Block Response Page** 드롭 다운 목록에서 **System-provided** 를 선택하십시오
6. **Advanced** 탭을 선택하십시오.
    a. **연필모양 아이콘**을 클릭하여 **Transport/Network Layer Preprocessor Settings** 를 편집합니다.
    b. **Maximum Active Responses** 텍스트 필드에 25 를 입력합니다.
    c. **OK** 를 클릭하십시오.

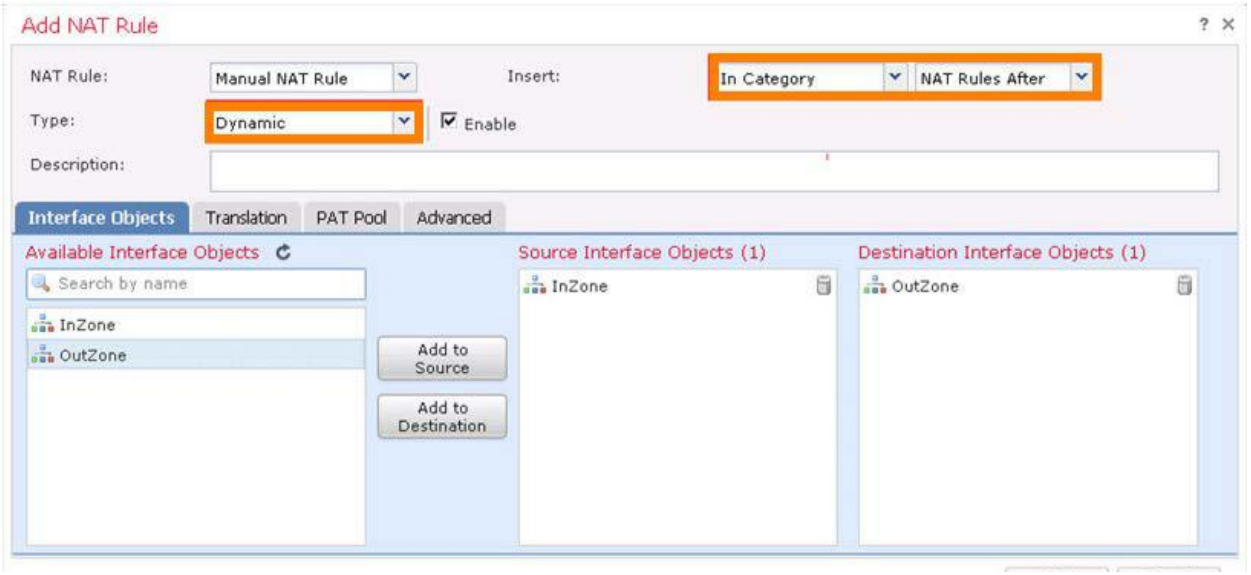


노트: Maximum Active Responses 를 0 보다 큰 값으로 설정하면 TCP 커넥션을 닫고 TCP resets 를 보낼 수 있도록 패킷을 드롭시키기 위한 규칙을 활성화 합니다. 일반적으로 클라이언트와 서버 양쪽으로 TCP resets 이 전송됩니다. 위의 구성을 사용하면 커넥션에서 추가 트래픽이 발생하는 경우 최대 25 개의 액티브 응답(TCP Resets)을 시작할 수 있습니다.
프로덕션 환경에서는 이 설정을 기본값으로 두는 것이 가장 좋습니다. 그에 따라 Resets 이 보내지지 않으며 악성 시스템은 탐지된 사실을 알 수 없습니다. 그러나 테스트와 데모에서는 드롭 규칙과 일치 할 경우 TCP resets 을 보내는 것이 일반적입니다.

7. **Save** 을 클릭하여 Access control policy 변경 사항을 저장합니다.

NAT policy 생성

1. **Devices > NAT** 으로 이동합니다.
2. **New Policy button** 클릭하고 **Threat Defense NAT** 를 선택합니다**.**
    a. Name 에 **Default PAT** 입력합니다.
    b. **NGFW** 를 선택합니다. **Add to Policy** 를 클릭하고 **Save** 를 클릭합니다.
    c. 정책을 편집할 수 있을때까지 잠시 기다립니다.
3. **Add Rule** 를 클릭합니다.
    a. 드롭 다운 목록에서 **In Category** 및 **NAT Rules After** 을 선택하십시오. 이렇게 하면 이 규칙이 auto-NAT (object NAT) 규칙 이후에 평가됩니다.
    b. **Type** 드롭 다운 목록에서 **Dynamic** 을 선택하십시오.
    c. 현재 **Interface Objects** 탭에 있습니다. **InZone** 을 선택하고 **Add to Source** 를 클릭하십시오.
    d. **OutZone 을** 선택하고 **Add to Destination** 클릭합니다.

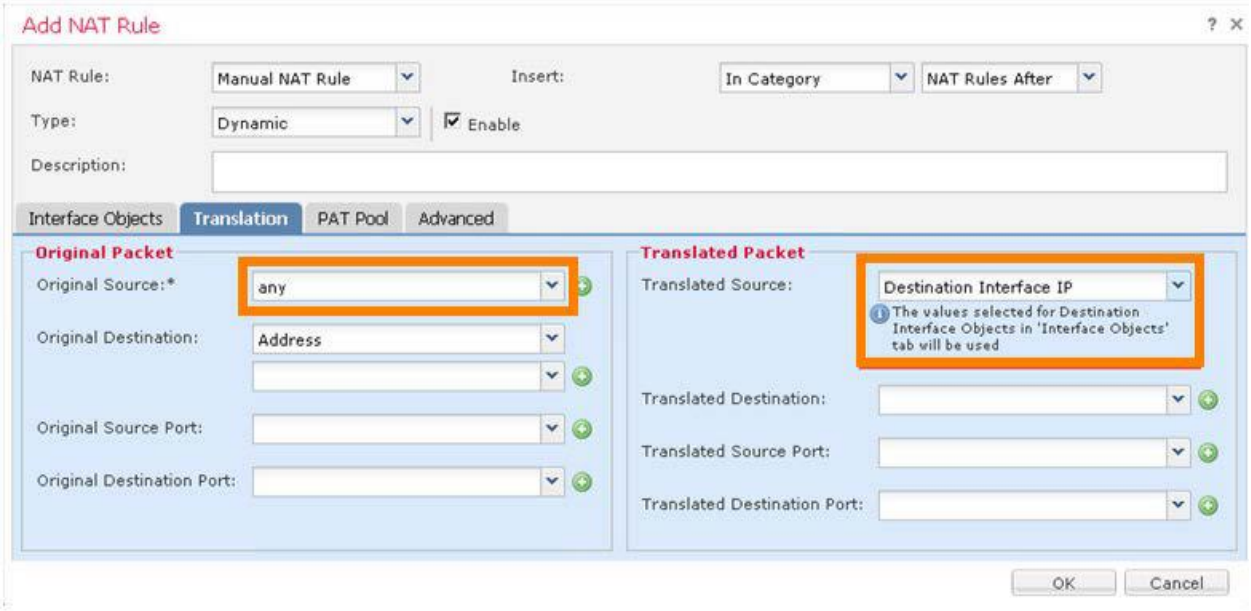


e. **Translation** 탭을 선택하십시오.

f. **Original Source drop-down list** 에 **any** 를 선택하십시오.

g. Translated Source 드롭 다운 목록에서 **Destination Interface IP** 를 선택하십시오.

h. **OK** 를 클릭하여 NAT 정책을 저장하십시오.



4. **Save** 를 클릭하여 NAT policy 저장하십시오.

Network discovery policy 수정

network discovery policy 는 기본값으로 내부 및 외부의 모든 응용 프로그램을 검색하도록 구성되어 있습니다. 호스트 및 사용자 discovery 를 추가하겠습니다. 프로덕션 환경에서는 FMC Firepower 호스트 라이센스를 초과 할 수 있기 때문에 정책을 수정하는 것이 좋습니다.

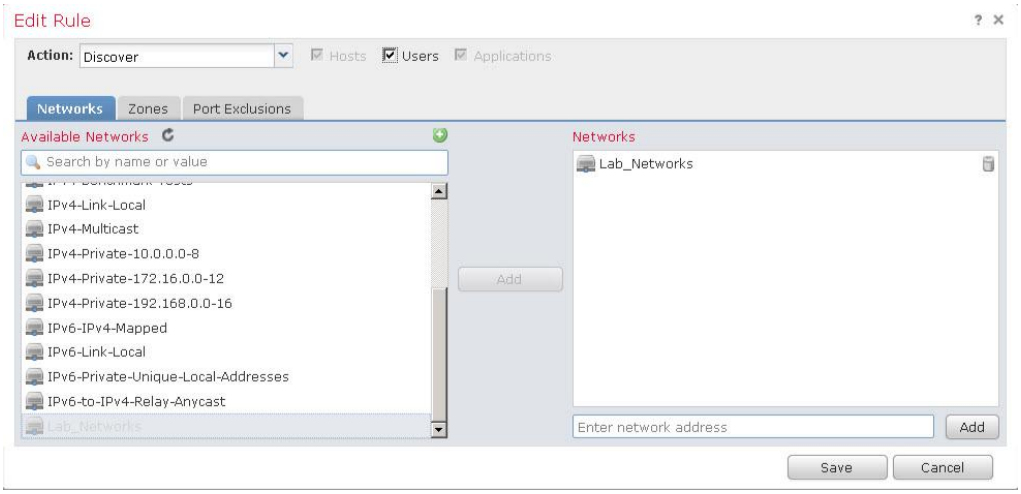
1. **Policies > Network Discovery** 으로 이동하십시오.

   a. 오른쪽에있는 **연필모양 아이콘**을 클릭하여 기존 규칙을 수정하십시오

   b. **Users** 체크 박스를 확인하십시오. 호스트 체크 박스는 auto-check 됩니다.

   c. **0.0.0.0/0** 및 **::/0** 을 모두 삭제하십시오.

2. **Lab_Networks** 네트워크를 선택하고 **Add** 를 클릭하십시오.



3. **Save** 클릭하십시오.

구성변경 내용의 배포

1. FMC 의 오른쪽 위 모서리에있는 **Deploy** 를 클릭합니다.

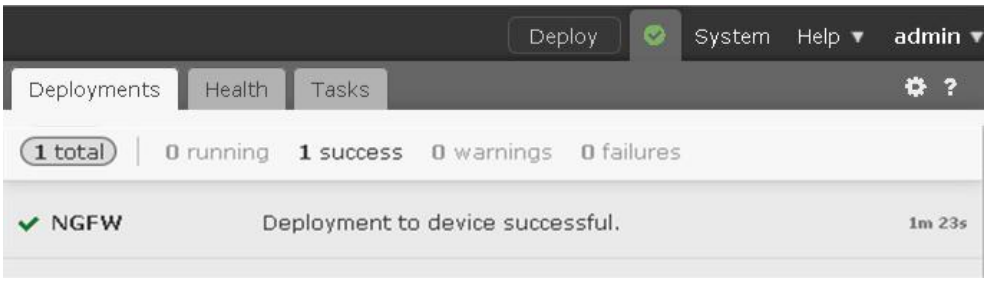
    a. NGFW 디바이스를 체크하고 세부 정보 확인을 위해 목록을 확장합니다.

    b. Device Configuration 오른쪽에있는 **Details** 위를 마우스로 가리키면 다음 그림과 같이 나타납니다.

c. NAT 정책, 네트워크 디스커버리, 인터페이스 및 스태틱 경로 구성 등 **NGFW** 설정이 수정되는지 확인하십시오.

d. **Deploy Button** 클릭하십시오.

e. FMC 의 오른쪽 상단 모서리에있는 **Deploy** 링크 오른쪽에있는 **아이콘**을 클릭하십시오. 배포가 완료 될 때까지 기다립니다.



NGFW 구성 테스트

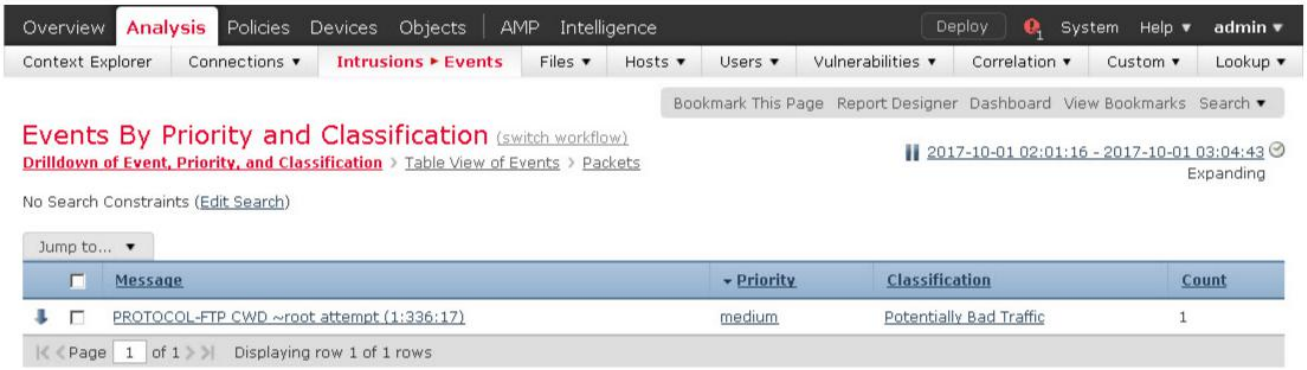
1. **Inside Linux Server** CLI 에서 다음을 수행합니다:
   a. **wget cisco.com** 을 입력하고 성공해야합니다. 이는 NAT 와 라우팅을 확인합니다.
   b. **ping outside** 를 입력하고 성공해야합니다. **Ctrl+C** 를 입력하여 핑을 종료하십시오.
   c. **ftp outside** 를 입력하십시오. 계정명은 **guest** 패스워드는 **C1sco12345** 으로 로그인하십시오.
   d. **cd ~root** 를 입력하십시오. 다음과 같은 메시지가 나타납니다: 421 Service not available, remote server has closed connection. 이것은 IPS 가 작동 중임을 나타냅니다.

노트: FTP 세션이 Hang 상태가 되면 access control policy 에서 active responses 을 활성화하지 않았을 수 있습니다. 만약 이와 같은 상태가 될지 예상했다면 이 문제를 해결할 필요는 없습니다.

   e. **Quit 를 입력하여** FTP 를 종료하십시오.

2. FMC 에서, **Analysis > Intrusions > Events** 로 이동합니다.

노트: 스노트 룰 336 이 트리거 된 것을 관찰하십시오. 데모 침입 정책에서는 이 규칙이 Drop 및 Generate Events(이벤트 생성)로 설정되어 있습니다. Balanced Security and Connectivity 와 같은 시스템 정의 침입 정책에서는 이 규칙이 비활성화됩니다.



노트: 프로덕션 환경에서 이벤트가 표시되지 않는 경우, 먼저 해야할 일은 NGFW 과 FMC 간의 시간 동기화를 확인해야합니다. 그러나 이 랩에서는 evening 프로세스 관련 문제일 가능성이 큽니다. 이 경우 다음과 같이 프로세스를 다시 시작하십시오.

NGFW CLI 에서 다음 명령을 실행합니다.

pmtool restartbytype EventProcessor

Jumper 데스크탑에서 미리 정의 된 PuTTY 세션을 사용하여 FMC 에 연결하십시오. **admin/FPlab12!**으로 로그인하여 다음 명령을 실행하십시오.

sudo pmtool restartbyid SFDataCorrelator

sudo pmtool restartbyid sftunnel

sudo password 는 **FPlab123!** 입니다**.**

a. 왼쪽에 있는 **화살표를 클릭하여** 이벤트 보기로 이동하십시오. 이벤트 세부 사항이 표시되는지 확인하십시오.

b. 이벤트의 왼쪽에 있는 화살표를 클릭하면 보다 자세히 볼 수 있습니다. Snort Rule 의 세부 사항을 포함한 많은 정보가 제공됩니다.

c. **Actions 을 확장하고** 여기에서 Rule 을 비활성화 할 수 있습니다. 하지만 하지 마십시오.

d. **Packet Bytes 를 확장하여** Rule 을 트리거 한 패킷의 내용을보십시오

3. 파일 및 멀웨어 차단 기능을 테스트합니다. 이러한 Wget 명령어는 Jump Desktop 의 Strings 파일에서 순서대로 복사 붙여넣기 하여 사용할 수 있습니다.

a. 컨트롤 테스트로, **WGET 을 사용하여 차단되지 않은 파일을 다운로드**하십시오.
wget -t 1 outside/files/ProjectX.pdf
이 명령어는 성공해야합니다.

b. 다음은 **WGET 을 사용하여** 유형별로 차단 된 파일을 다운로드 해봅니다.
wget -t 1 outside/files/test3.avi

매우 작은 양의 파일만 다운로드 됩니다. 이것은 NGFW 가 첫 번째 데이터 블록을 볼 때 파일 유형을 감지 할 수 있기 때문입니다. Demo File Policy 는 AVI 파일을 차단하도록 구성됩니다.

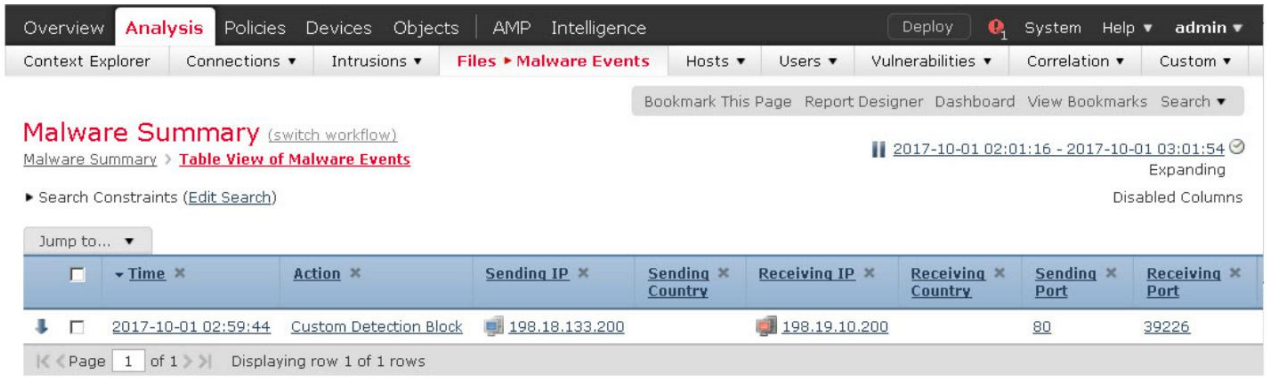
c. 마지막으로 **WGET 을 사용하여 악성 코드를 다운로드하십시오**.
wget -t 1 outside/files/Zombies.pdf

파일의 약 99 %가 다운로드되는지 확인합니다.이것은 NGFW 가 데이터의 SHA 를 계산하기 위해 전체 파일을 필요로 하기 때문입니다. NGFW 는 Hash 가 계산되어 룩업 될 때까지 마지막 데이터 블록을 홀드합니다. Demo File Policy 는 PDF 파일에서 탐지 된 멀웨어를 차단하도록 구성되어 있습니다.

4. FMC 에서 **Analysis > Files > Malware Events** 로 이동합니다.

   a. 파일 Zombies.pdf 가 차단되었음을 확인하십시오.

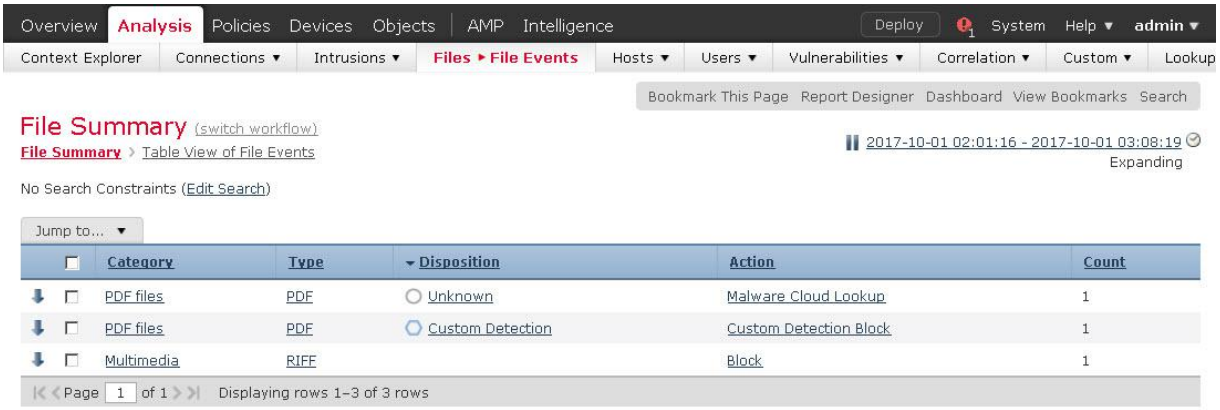
   b. 이벤트를 테이블 보기로 드릴 다운하려면 왼쪽의 화살표를 클릭하십시오. 호스트 **198.19.10.200** 은 빨간색 아이콘으로 표시됩니다. 이것은 Inside Linux Server 입니다. 빨간색 아이콘은 호스트가 IOC 침해 지표에 연관되어 있음을 나타냅니다.



노트: 이 작업은 Malware Block 대신 Custom Detection Block 으로 보고됩니다. 이 랩 환경과 클라우드간 연결에 문제가 있을 수 있기 때문에 Zombies.pdf 를 Custom Detection 목록에 추가했기 때문입니다. 자세한 내용은 부록 A 를 참조하십시오.
원하는 경우 다음을 시도 할 수 있습니다.
wget -t 1 outside/malware/Buddy.exe
이것은 *Malware Block* 으로 보고돼야 합니다. 그러나 이 랩 환경의 특수성으로 인해 클라우드 룩업이 실패할 수 있습니다.
따라서 파일도 차단되지 않을 수 있습니다.

5. **빨간색 컴퓨터 아이콘을 클릭하십시오**. 호스트 프로파일 페이지가 열립니다. 페이지를 살펴본 다음 닫습니다.

6. **Analysis > Files > File Events** 로 이동하십시오**.** 세 가지 파일 이벤트에 대한 정보가 모두 표시되어야합니다.



원하는 경우 세부 정보를 드릴 다운 할 수 있습니다.

시나리오 3. AnyConnect 리모트 액세스 VPN

이 시나리오는 다음 내용으로 구성됩니다:

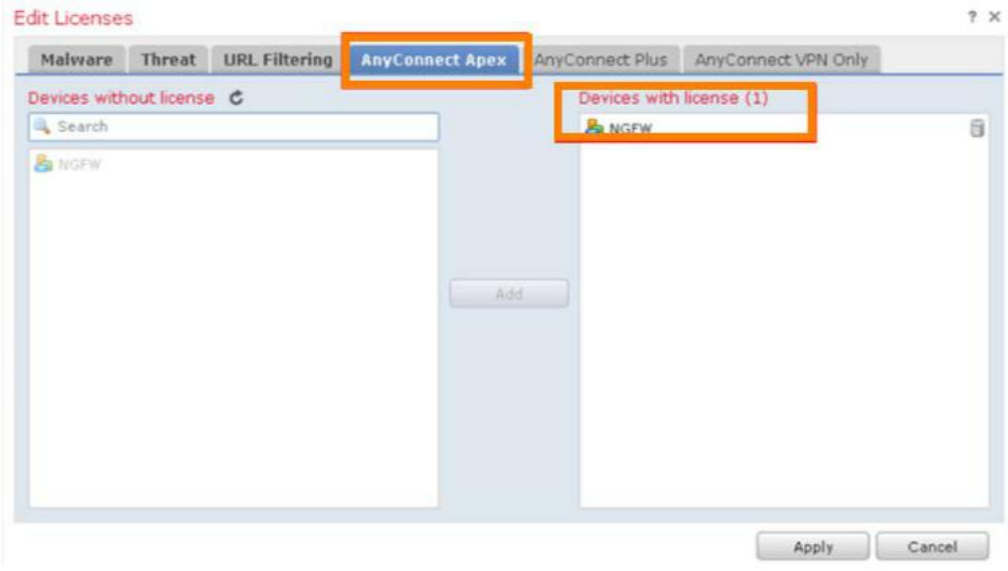
- AnyConnect Smart 라이센스 활성화
- AnyConnect RA VPN 오브젝트 생성하기
- default group policy 수정
- RA VPN 마법사 실행
- 디바이스 인증서 구성
- 인바운드 AnyConnect 액세스를 허용하도록 Access control policy 수정
- NAT exemption 구성
- VPN 로깅 구성
- NGFW RA VPN 구성 배포 및 확인
- 구성 테스트

이 연습의 목적은 Cisco Firepower NGFW 에서 사용할 수 있는 AnyConnect 리모트 액세스 VPN 의 기능을 이해하고 구성하는 것입니다.

스텝

AnyConnect Smart 라이선스 활성화

1. FMC 에서, **System > Licenses > Smart Licenses** 으로 이동하십시오.
    a. **Edit Licenses** 클릭하십시오.
    b. **Edit Licenses** 창에서, **AnyConnect Apex** 탭을 선택하십시오.
    c. **NGFW** 장치를 선택하십시오. **Add** 및 **Apply** 를 클릭하십시오.



AnyConnect RA VPN 오브젝트 만들기

1. Windows 용 AnyConnect 이미지 오브젝트를 생성합니다.

    a. FMC 에서 **Objects > Object Management > VPN > AnyConnect File** 으고 이동하십시오.

    b. **Add AnyConnect File** 를 클릭하십시오 .

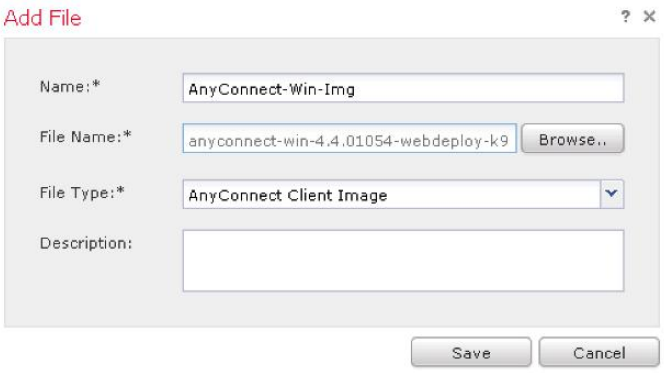
    c. **Name** 에, **AnyConnect-Win-Img** 를 입력하십시오.

    d. **Browse** 를 클릭하여 Jump 데스크톱의 **RA VPN** 폴더로 이동하십시오.

    e. **anyconnect-win-4.4.01054-webdeploy-k9.pkg** 파일을 선택하십시오.

    f. **Open** 을 클릭하십시오. **File Type** 텍스트 필드는 올바른 값으로 미리 채워집니다.

    g. **Save** 클릭.



2. MAC OS 용 AnyConnect 이미지 오브젝트를 새로 만듭니다.

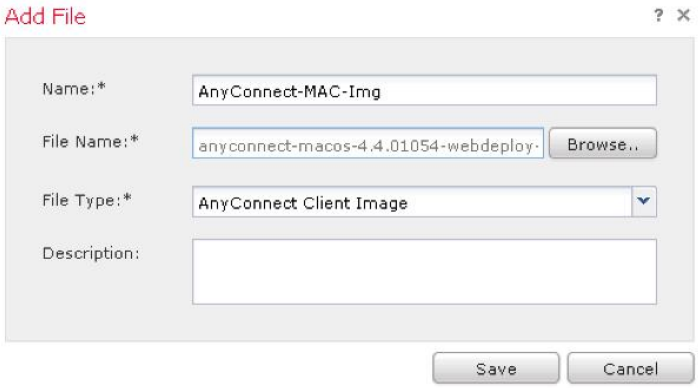
    a. **Add AnyConnect File** 를 클릭하십시오.

    b. **Name** 에, **AnyConnect-MAC-Img** 를 입력하십시오.

    c. **Browse** 를 클릭하여 Jump desktop 의 RA VPN 폴더에서 **anyconnect-macos-4.4.01054-webdeploy-k9.pkg** 파일을 선택하십시오.

    d. **Open** 을 클릭하십시오. **File Type** 텍스트 필드는 올바른 값으로 미리 채워집니다.

    h. **Save** 를 클릭.



3. **AnyConnect** 클라이언트 프로파일 오브젝트를 생성하십시오.

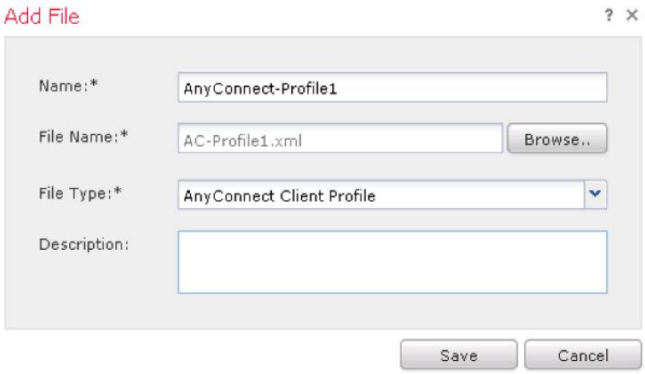
    a. **Add AnyConnect File** 를 클릭합니다.

    b. **Name** 에, **AnyConnect-Profile1** 을 입력하십시오.

    c. **Browse** 를 클릭하여, Jump desktop 의 **RA VPN** 폴더에서 **AC-Profile1.xml** 파일을 선택하십시오.

    d. **Open** 을 클릭하십시오. **File Type** 텍스트 필드에 올바른 값이 미리 채워져 있습니다.

    e. **Save** 를 클릭.



노트: AnyConnect 클라이언트 프로파일은 cisco.com 에 있는 *VPN Profile Editor* 툴을 사용하여 만들 수 있습니다. *VPN Profile Editor* VPN 툴은 Jumper 워크스테이션에도 있습니다. 워크스테이션에서 **Start > All Programs > Cisco > Cisco AnyConnect profile editor > VPN Profile Editor** 로 액세스 할 수 있습니다.

4. IP Pool 을 작성하십시오.

    a. FMC 에서, **Objects > Object Management > Address Pools > IPv4 Pools** 로 이동합니다.

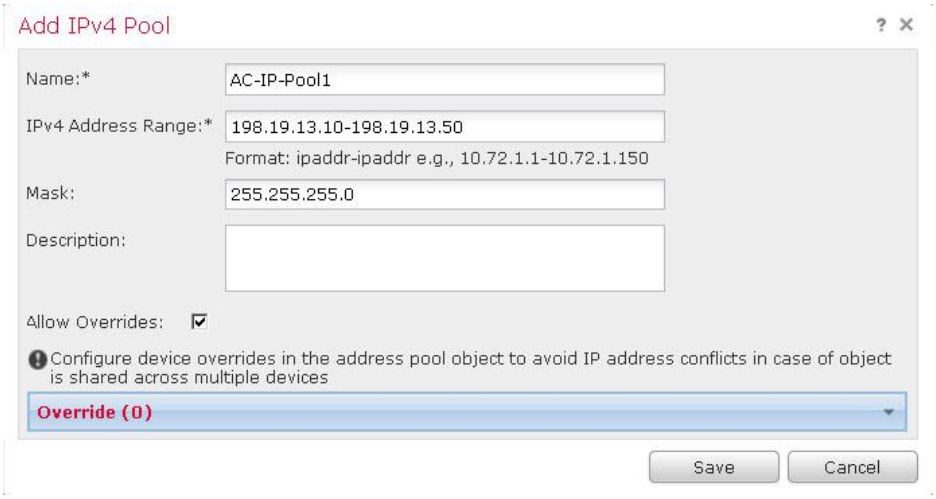
    b. **Add IPv4 Pools** 를 클릭합니다.

    c. Name 에, **AC-IP-Pool1** 을 입력합니다.

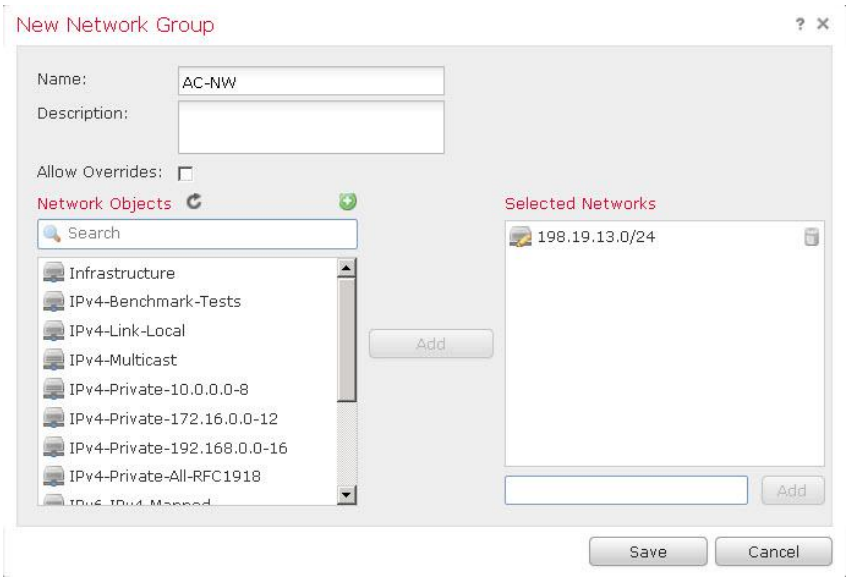
    d. **IPv4 Address Range** 에, **198.19.13.10-198.19.13.50** 을 입력합니다.

    e. Mask 에, **255.255.255.0** 을 입력합니다.

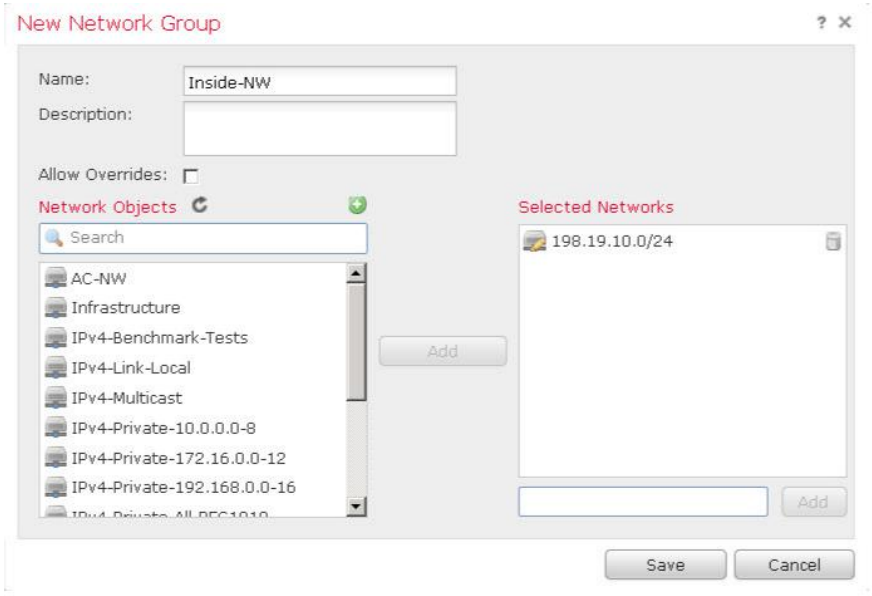
    f. **Save** 를 클릭하십시오.



5. IPv4 pool 에 해당하는 네트워크 오브젝트를 만듭니다.
    a. FMC 에서, **Object > Object Management > Network** 로 이동하십시오.
    b. **Add Network** 을 클릭하여 **Add Group** 을 선택하십시오.
    c. **Name** 에, **AC-NW** 를 입력하십시오.
    d. **Selected Networks** 아래 텍스트 필드에 **198.19.13.0/24** 를 입력하고 **Add** 를 클릭하십시오.
    e. **Save** 를 클릭.

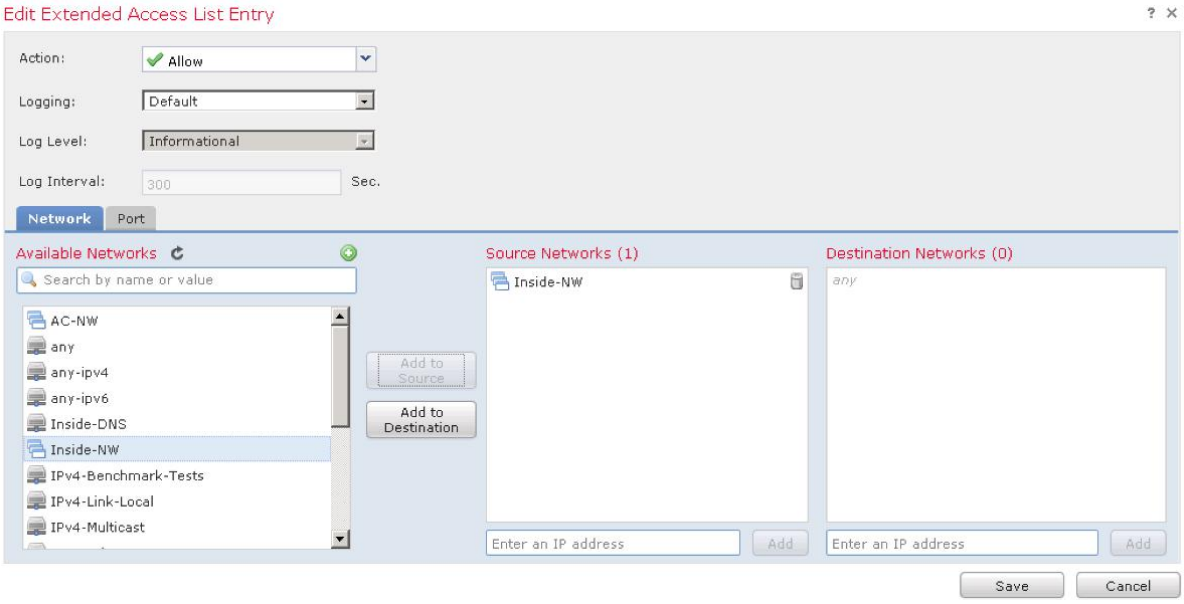


6. 내부 네트워크용 네트워크 오브젝트를 만듭니다.
    a. **Add Network** 을 클릭하여 **Add Group** 을 선택하십시오.
    b. Name 에, **Inside-NW** 를입력하십시오.
    c. **Selected Networks** 아래 텍스트 필드에 **198.19.10.0/24** 를 입력하고 **Add** 를 클릭하십시오.
    d. **Save** 를 클릭.

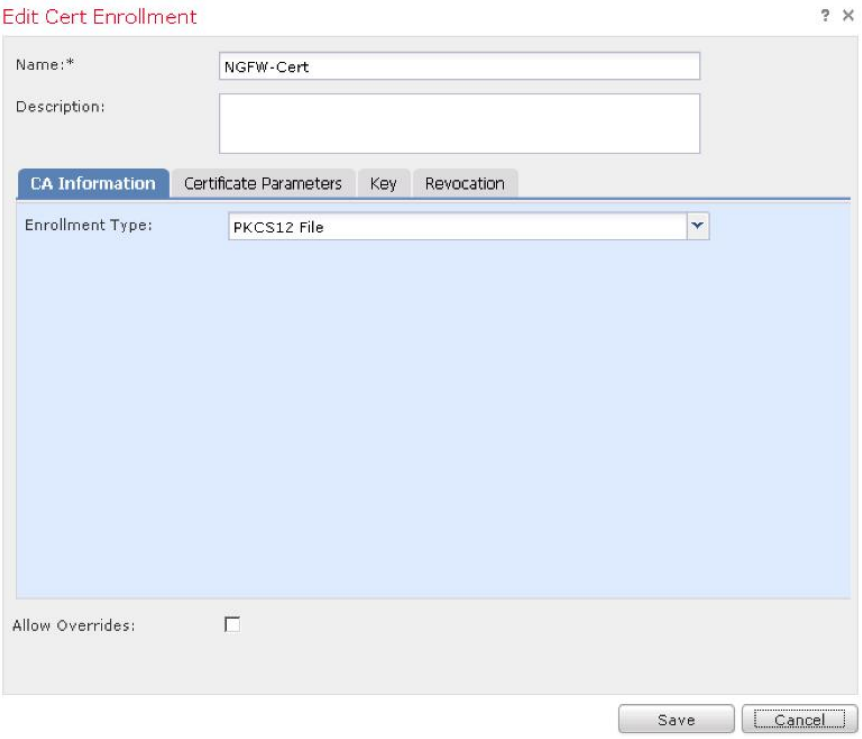


노트: 네트워크 오브젝트 대신 네트워크 오브젝트 그룹을 사용하는 이유가 있습니다. 다음 랩에서 다른 서브넷을 추가하게 됩니다. 네트워크 그룹을 사용하고 있기 때문에 이 오브젝트만 수정하면 됩니다. 액세스 콘트롤 및 NAT 정책을 직접 수정할 필요가 없습니다.

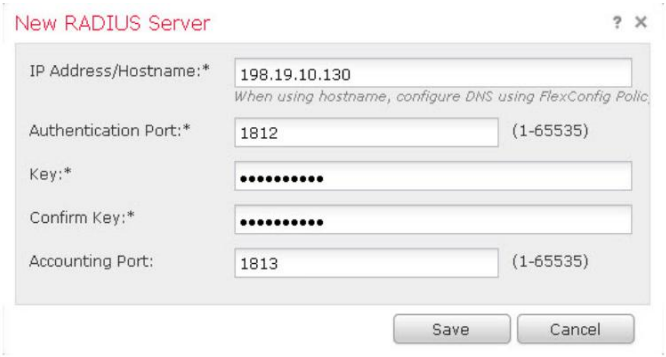
7. RA VPN 의 스플릿 터널 구성을 위해 ACL 을 작성하십시오.
    a. FMC 에서, **Objects > Object Management > Access List > Extended** 로 이동하십시오.
    b. **Add Extended Access List** 를 클릭하십시오.
    c. Name 에, **AC-SplitTunnel1** 을 입력합니다.
    d. **Add** 를 클릭하십시오.
    e. **Available Networks** 에서 **Inside-NW** 를 선택하고 **Add to Source** 를 클릭하십시오.
    f. Add 를 클릭하십시오.
    g. **Save** 를 클릭하십시오.



8. 디바이스 인증서 오브젝트를 작성하십시오.
    a. FMC 에서, **Objects > Object Management > PKI > Cert Enrollment** 로 이동하십시오.
    b. **Add Cert Enrollment** 클릭하십시오.
    c. Name 에, **NGFW-Cert** 를 입력하십시오.
    d. **Enrollment Type** 에, **PKCS12 File** 을 선택하십시오.
    e. **Save** 를 클릭하십시오.



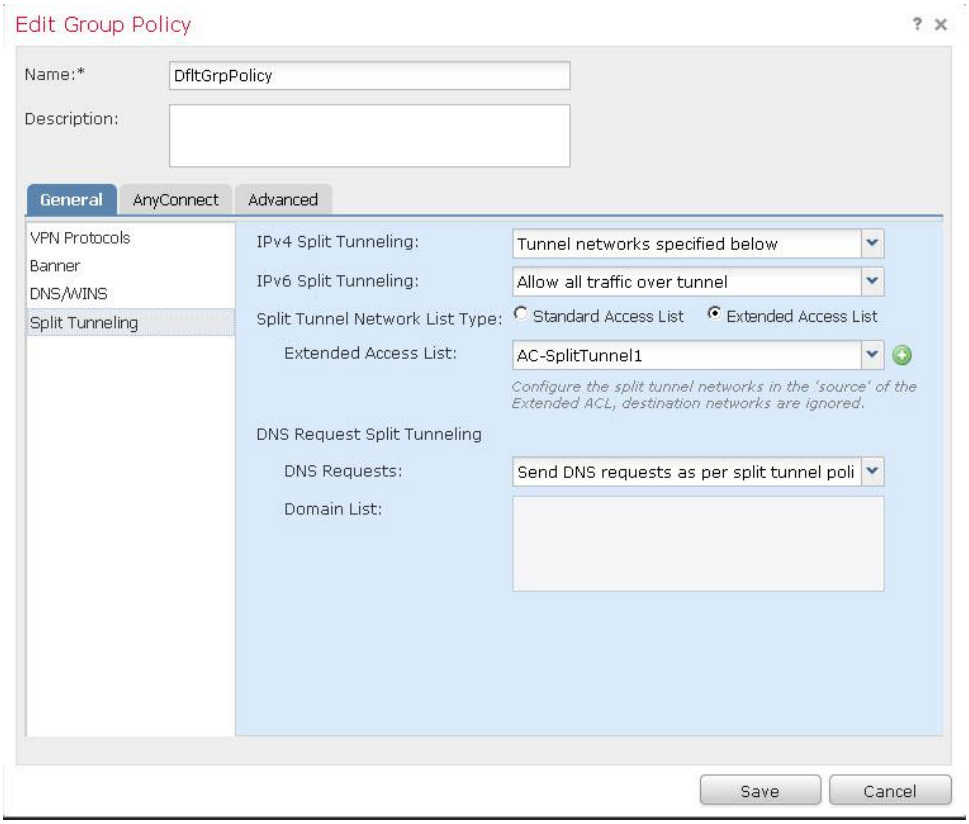
9. ISE RADIUS 서버에 대한 오브젝트를 만듭니다.
    a. FMC 에서, **Object > Object Management > RADIUS Server Group** 으로 이동합니다.
    b. **Add RADIUS Server Group** 을 클릭합니다.
    c. Name 에, **ISE-AAA** 를 입력합니다.
    d. RADIUS 서버 섹션의 (+) 아이콘을 클릭하십시오.
    e. IP Address 에, **198.19.10.130** 을 입력하십시오.
    f. **Key** 및 **Conform Key** 에, **C1sco12345** 를 입력하십시오.
    g. **New RADIUS Server** 페이지에서 **Save** 를 클릭하십시오.
    h. **Add RADIUS Server Group** 페이지에서 **Save** 를 클릭하십시오.



노트: 시간 절약을 위해 ISE 는 모든 랩에 필요한 모든 구성이 사전에 준비되어 있습니다. ISE 구성을 참조하려면 부록 C 를 참조하십시오.

Default group policy 수정

1. FMC 에서, **Objects > Object Management > VPN > Group Policy** 으로 이동하십시오.
2. **DfltGrpPolicy** 를 선택하여 편집을 하십시오.
3. **General** 탭에서 **Split Tunneling** 을 선택하십시오.
    a. **IPv4 Split Tunneling** 에, **Tunnel networks specified below** 를 선택하십시오.
    b. **Extended Access List** 에 체크합니다.
    c. **Access List** 에, **AC-SplitTunnel1** 을 선택하십시오.



4. **General** 탭에서 **DNS/WINS** 을 선택하십시오.

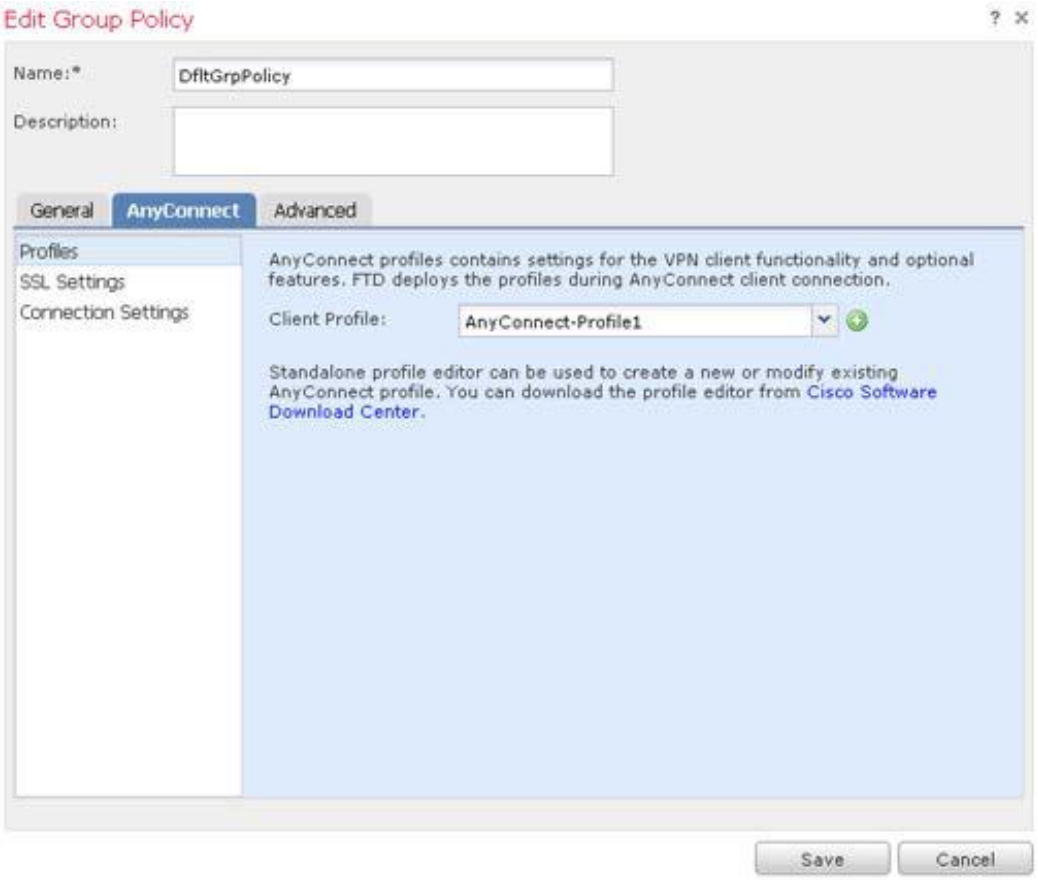
    a. **Primary DNS Server** 에, (+) 아이콘을 클릭하십시오.

    b. **Name** 에 **Inside-DNS** 를 입력하십시오.

    c. **Network** 에 **198.19.10.100** 을 입력하십시오.

    d. **Save** 클릭.

5. **AnyConnect** 탭을 선택하십시오. **Client Profile** 에 **AnyConnect-Profile1** 을 선택하십시오.

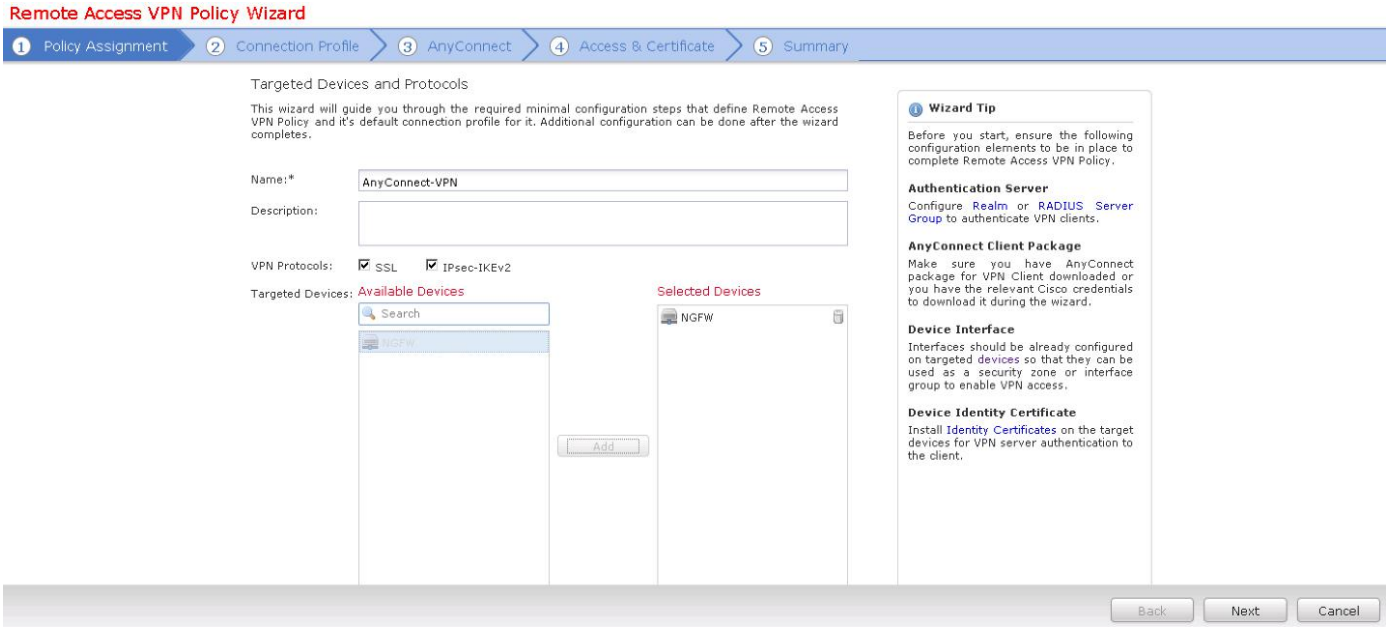


6. **Save** 클릭하여 그룹 정책 변경 사항을 저장합니다.

RA VPN 마법사 실행

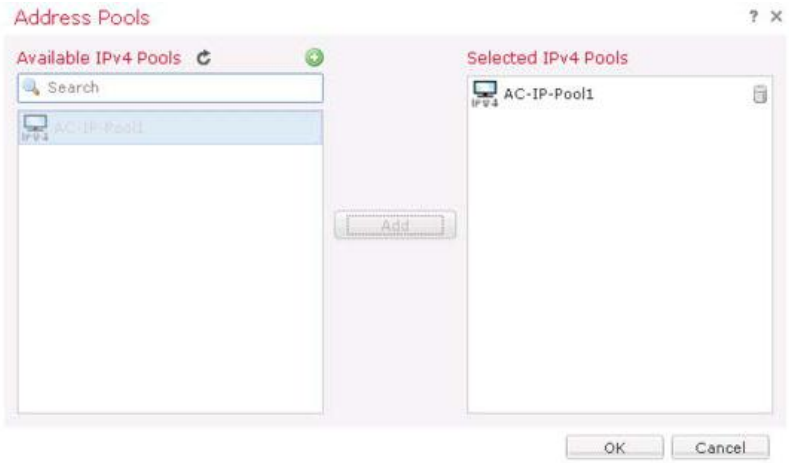
1. FMC 에서 **Devices > VPN > Remote Access** 으로 이동하고 **Add** 를 클릭하십시오. 그러면 마법사가 시작됩니다.

2. **마법사**의 **Policy Assignment** 페이지를 완료하십시오.
    a. **Name** 에, **AnyConnect-VPN** 을 입력하십시오.
    b. **Target Device**s 에서 **NGFW** 를 선택하십시오. **Add** 를 클릭하십시오.
    c. **Next** 를 클릭합니다.

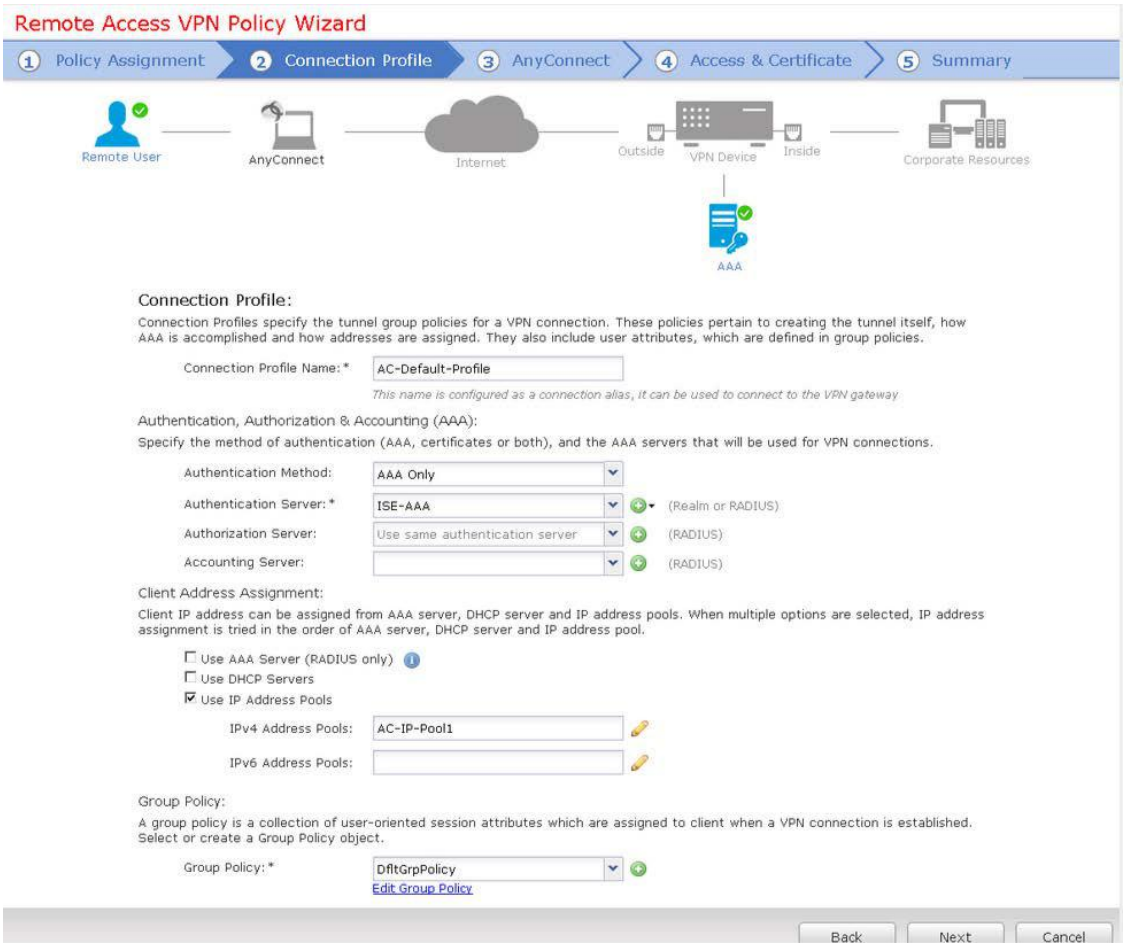


3. **마법사**의 **Connection Profile** 페이지를 완료하십시오.
    a. **Connection Profile Name** 에 **AC-Default-Profile** 를 입력하십시오..
    b. **Authentication Method** 에 **AAA Only** 가 선택되어 있는지 확인하십시오.
    c. 인증 서버의 경우, **ISE-AAA** 를 선택하십시오.

4. **Address Pools** 에서, **IPv4 Address Pools** 을 편집하십시오.
    d. **IPv4 Address Pools** 에서 **AC-IP Pool1** 을 선택하십시오**. Add** 를 클릭한 다음 **OK** 를 클릭하십시오.



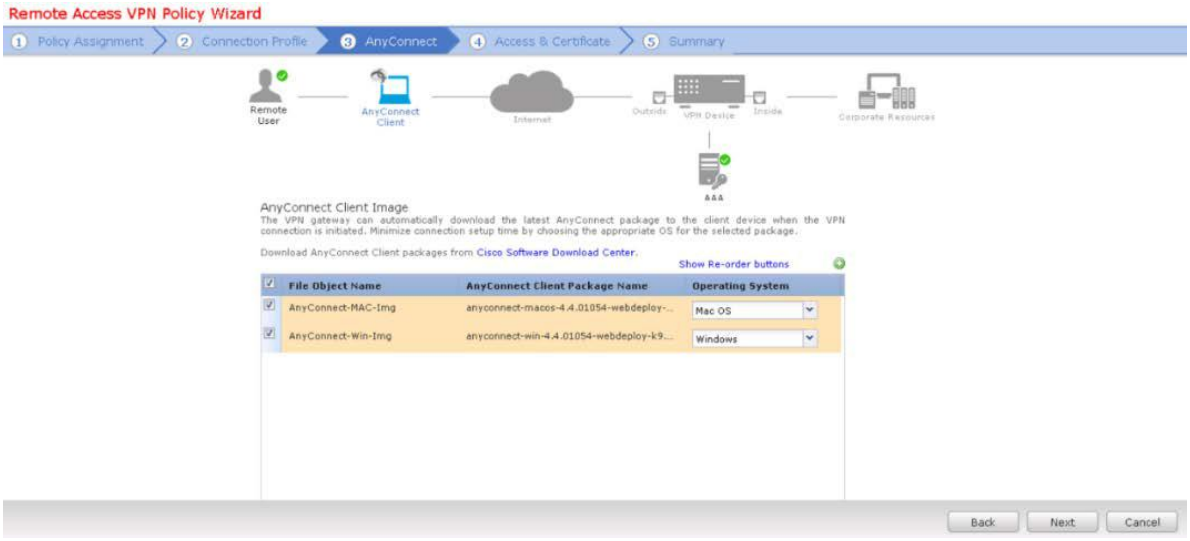
4. **Group Policy** 를 **DfltGrpPolicy** 로 설정되었는지 확인합니다. 그 다음 **Next** 를 클릭하십시오.



5. 마법사의 **AnyConnect** 페이지를 완료하십시오.

   a. Object 체크박스 두 개를 체크합니다.

   b. **Next** 를 클릭하십시오.

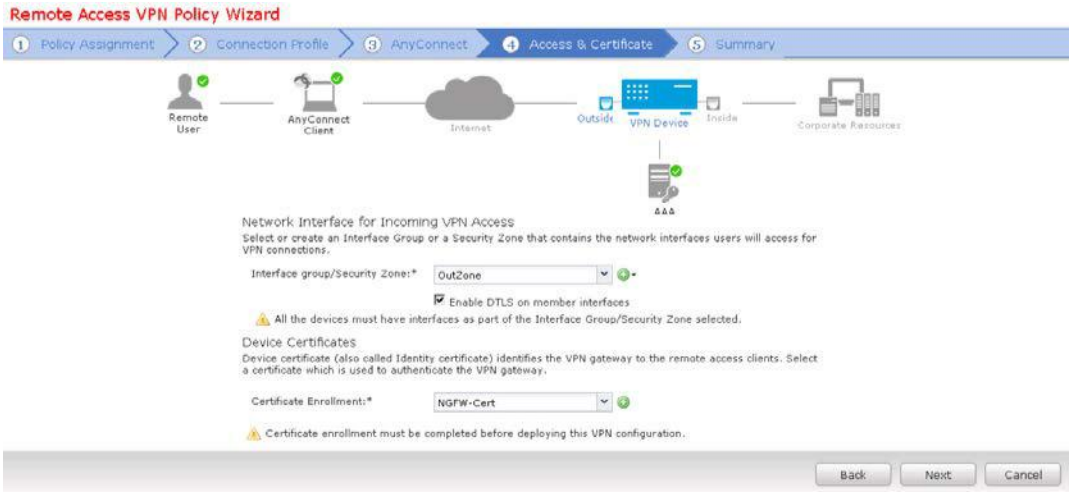


6. 마법사의 **Access & Certificate** 페이지를 완료하십시오.

    a. **Interface group/Security Zone** 에, **OutZone** 을 선택하십시오.

    b. **Certificate Enrollment** 에, **NGFW-Cert** 를 선택하십시오.

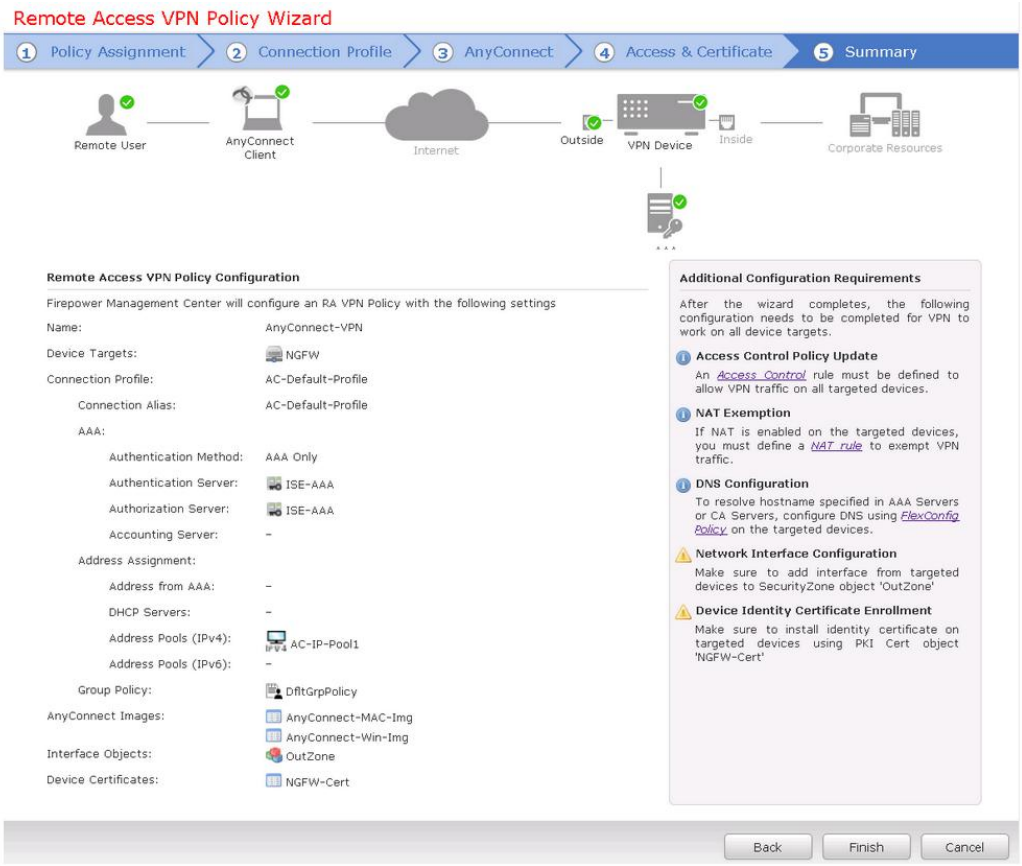
    a. **Next** 를 클릭하십시오.



7. 마법사의 **Summary** 페이지를 검토하십시오.

    a. 이 페이지에 표시된 구성을 검토하십시오.

    b. **Finish** 를 클릭.

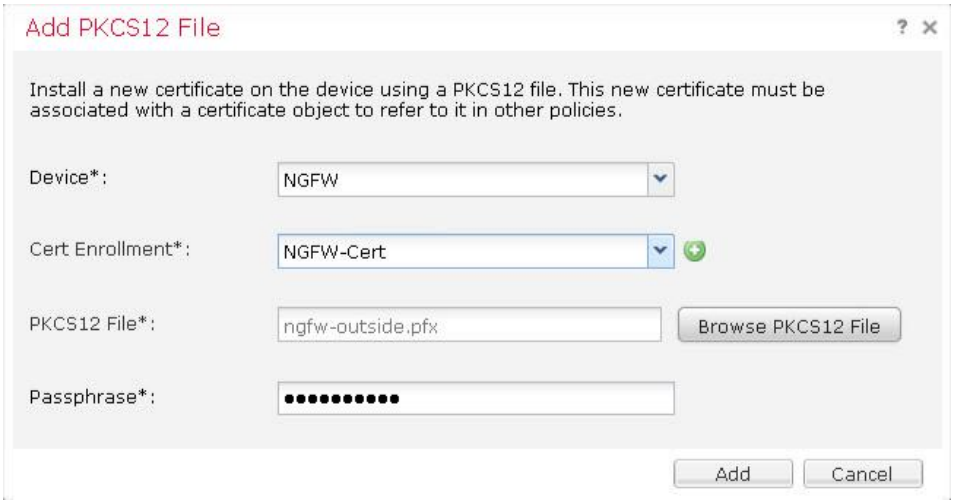


디바이스 인증서 구성

1. FMC 에서, **Devices > Certificates** 으로 이동하십시오.
2. **Add** 클릭하여 **PKCS12 File** 을 선택하십시오.
    a. **Device** 에, **NGFW** 를 선택하십시오.
    b. **Cert Enrollment** 에 **NGFW-Cert** 를 선택하십시오.

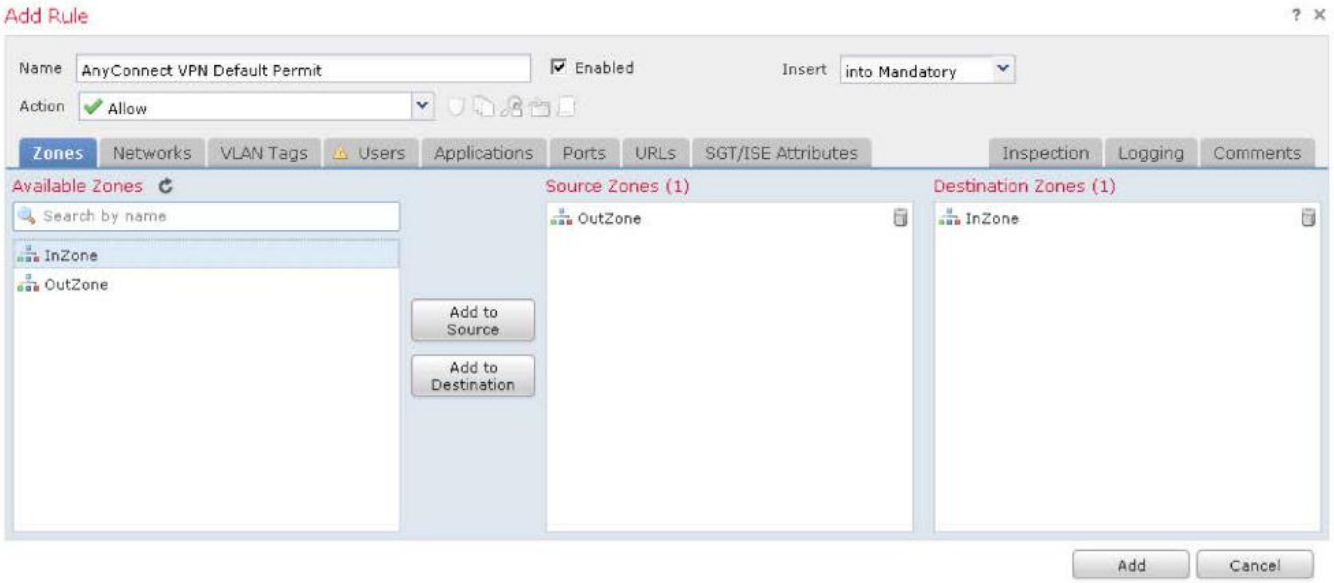
노트: 텍스트 필드 오른쪽에 있는 아래쪽 화살표를 클릭하십시오. 텍스트 영역을 클릭하면 문자열 **admin** 이 표시됩니다. 이는 브라우저 문제입니다.

    c. **PKCS12 File** 은, **Browse PKCS12** 파일을 클릭하십시오. Jumper 데스크탑의 **Certificates** 폴더로 이동하여 **ngfw-outside** 를 선택하십시오. **Open** 을 클릭합니다.
    d. **Passphrase** 에 **C1sco12345** 입력하십시오.
    e. **Add** 를 클릭.



인바운드 AnyConnect 접속 허용을 위한 Access control policy 수정

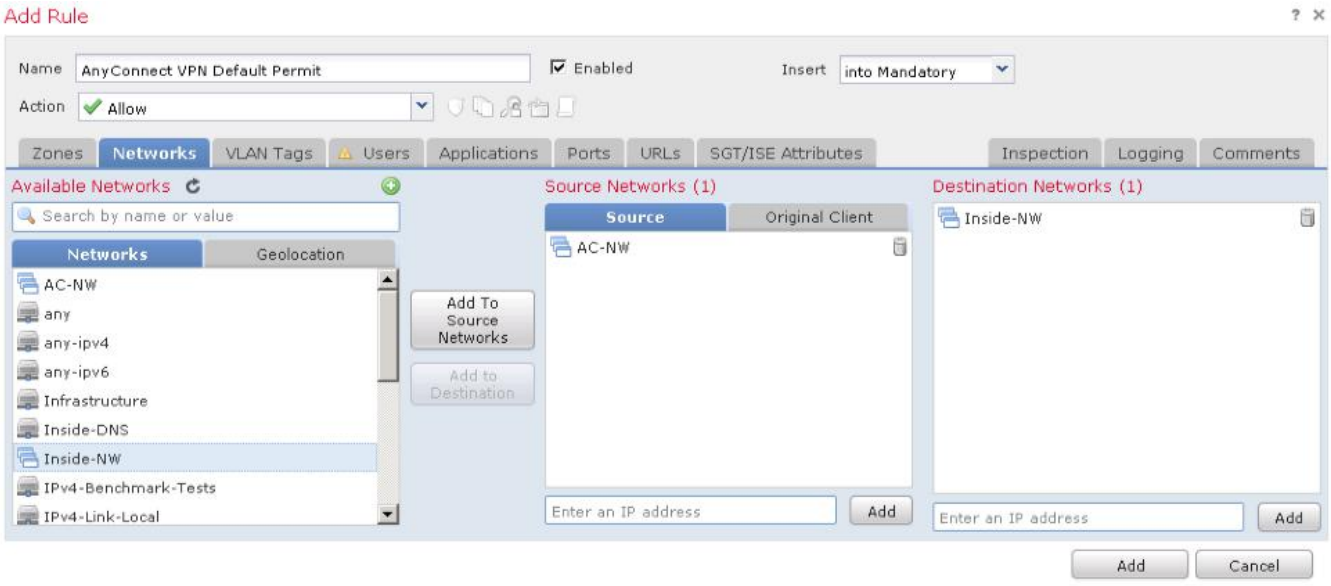
1. FMC 에서, **Policies > Access Control > Access Control** 으로 이동하십시오.
2. Access control policy 를 선택하고 편집하십시오. **Add Rule** 을 클릭합니다.
    a. **Name** 에, **AnyConnect VPN Default Permit** 입력하십시오.
    b. **Insert** 드롭 다운 목록에서 **into Default** 를 선택하십시오.
    c. **Zones** 탭이 이미 선택되어 있어야합니다.
    d. **OutZone** 을 선택한 다음, **Add to Source** 를 클릭하십시오.
    e. **InZone** 을 선택한 다음, **Add to Destination** 을 클릭하십시오.



f. **Networks** 탭을 선택하십시오.

i. **AC-NW** 를 선택한 뒤 **Add to Source** 를 클릭하십시오.

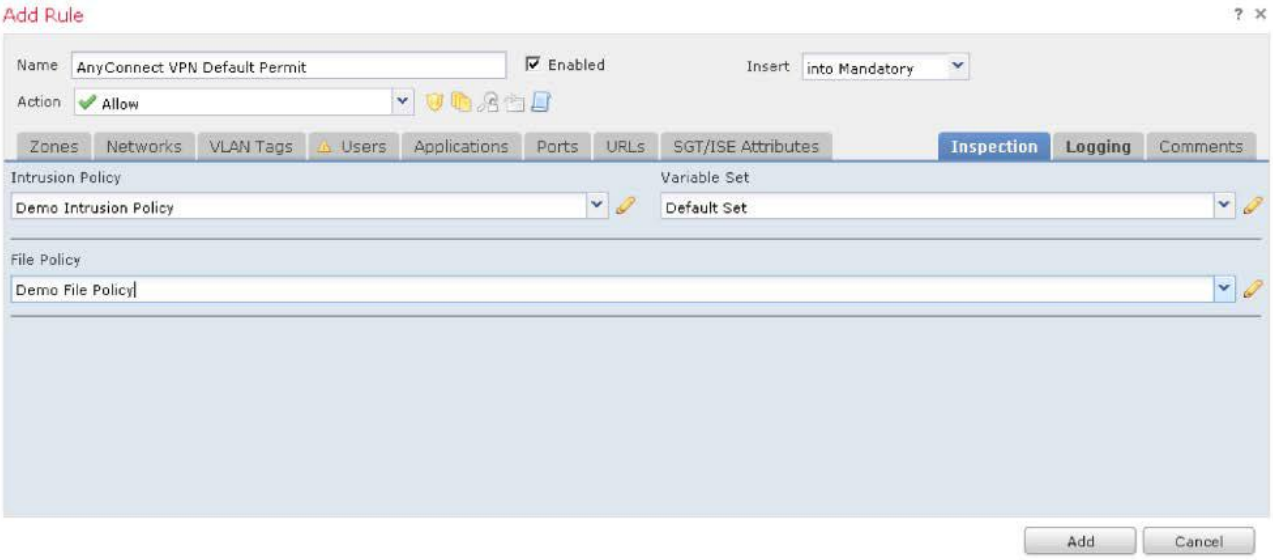
ii. **Inside-NW** 를 선택한 뒤 **Add to Destination** 을 클릭하십시오.



g. **Inspection** 탭을 선택합니다.

i. Intrusion Policy 드롭 다운 목록에서 Demo Intrusion Policy 를 선택하십시오.

ii. File Policy 드롭 다운 목록에서 Demo File Policy 를 선택하십시오.

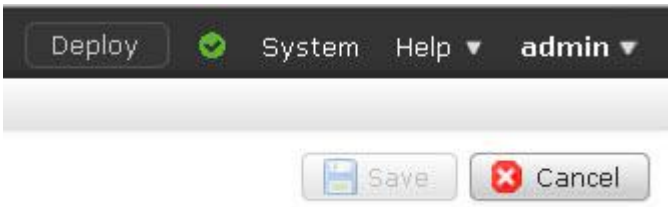


h. **Add** 를 클릭하여 규칙을 추가합니다.

i. **Save** 를 클릭하여 Access control policy 의 변경 사항을 저장하십시오.

NAT exemption 구성

1. FMC 에서, **Devices > NAT** 로 이동하십시오.
2. 기존 **NAT policy** 를 선택하고 편집합니다. 오른쪽 상단에 **Save** 버튼이 회색으로 표시되는지 확인합니다. 그렇지 않은 경우 뒤로 이동했다가 다시 편집을 시도합니다. 이 부분은 알려진 버그입니다.

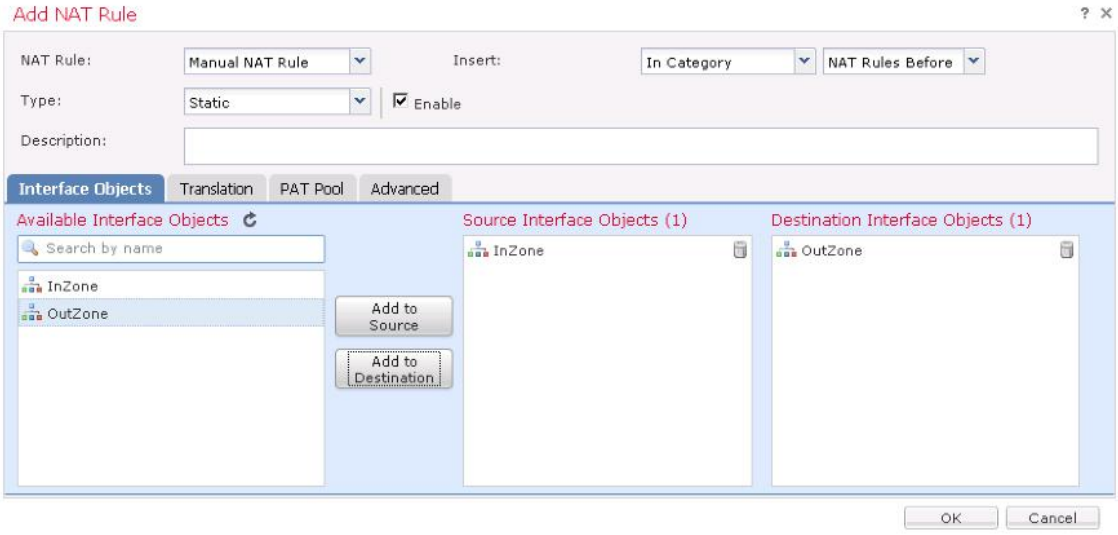


3. **Add Rule** 을 클릭합니다.

a. 클릭하면 Interface Objects 탭으로 이동됩니다.

i. **InZone** 을 선택한 다음 **Add to Source** 를 클릭하십시오

ii. **OutZone** 을 선택한 다음 **Add to Destination** 을 클릭하십시오.



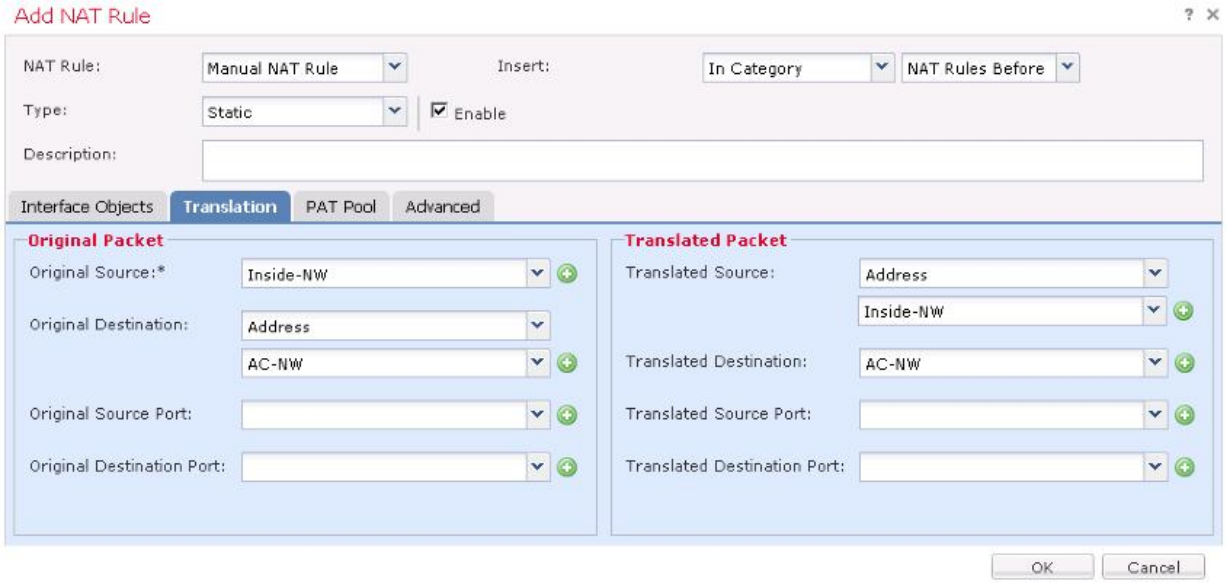
b. **Translation** 탭을 선택하십시오.

i. **Original Source** 에 **Inside-NW** 를 선택하십시오

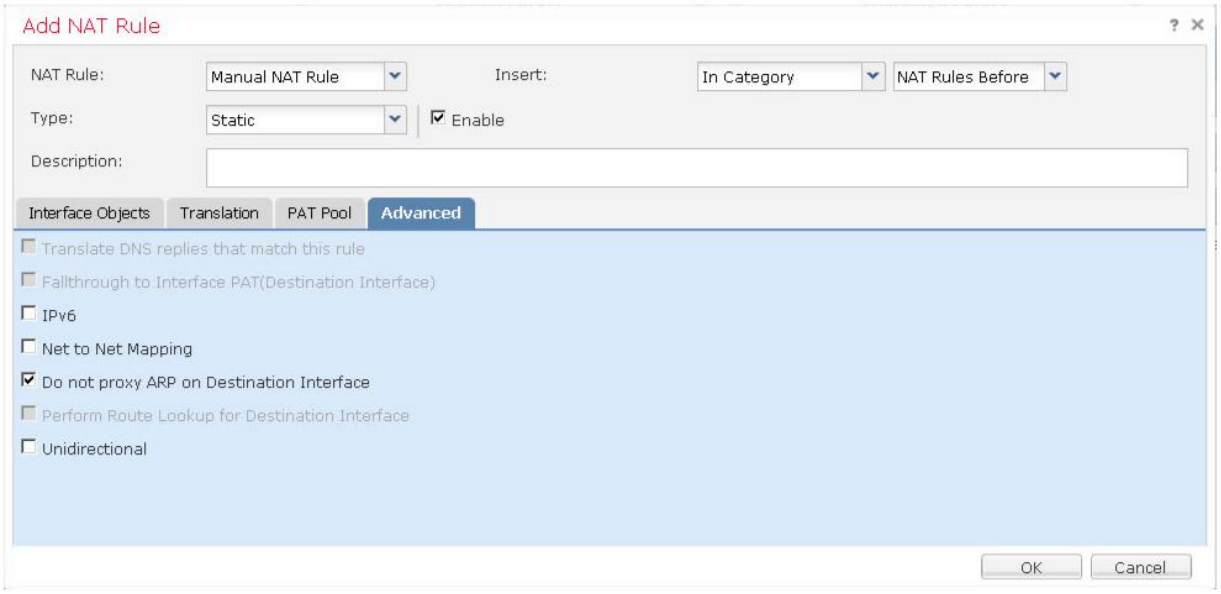
ii. **Original Destination** 에 **AC-NW** 를 선택하십시오

iii. **Translated Source** 에 **Inside-NW** 를 선택하십시오

iv. **Translated Destination** 에 **AC-NW** 를 선택하십시오



c. **Advanced** 탭을 선택하여 **Do not proxy ARP on Destination Interface** 를 선택하십시오.



노트: 이 랩에서는 **Do not proxy ARP on Destination Interface** 를 사용하도록 설정하는 것이 중요합니다. 이 설정을 적용하지 않으면 모든 장치가 In Band 로 관리되어 PoD 액세스에 문제가 생길 수도 있습니다.

d. **OK** 를 클릭하여 NAT 룰을 저장합니다

e. **Save** 를 클릭하여 NAT 정책의 변경 사항을 저장하십시오.

VPN 로깅 구성

트러블 슈팅을 용이하도록 VPN logging 레벨을 informational 로 변경합니다. 랩에서 언제든지 **Device > VPN > Troubleshooting** 로 이동하여 트러블 슈팅을 수행하는데 도움이되는 로그 정보를 볼 수 있습니다.

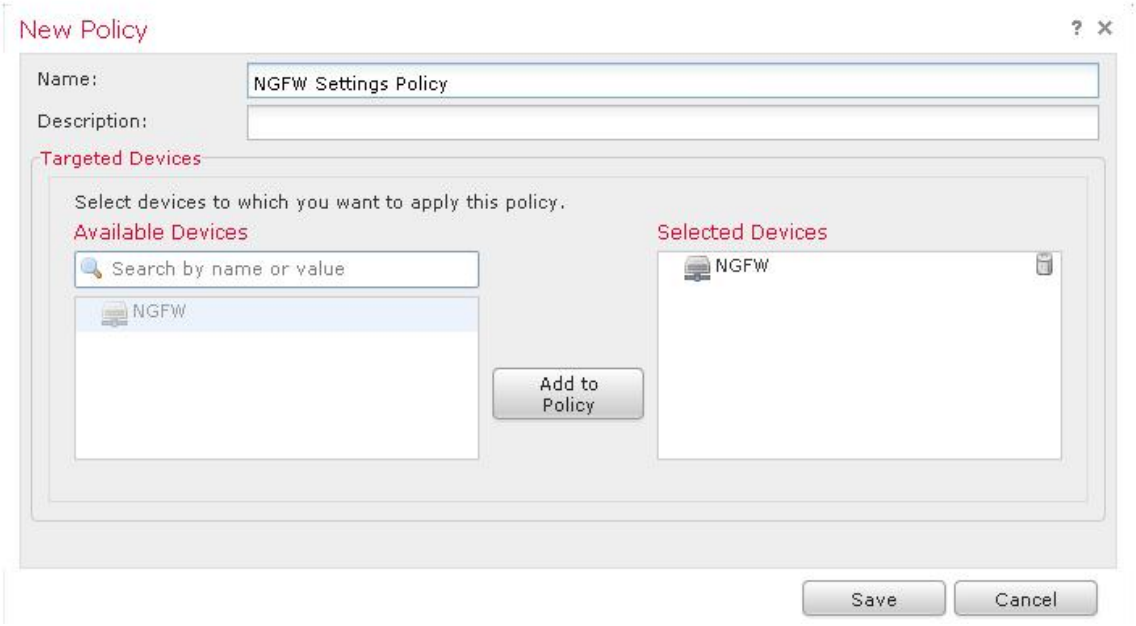
노트: 실제 프로덕션 환경에서는 VPN 로깅 설정을 informational 로 설정하지 않을 수도 있습니다.

1. FMC 에서 **Devices > Platform Settings** 로 이동합니다.

   a. 파란색 텍스트 **Threat Defense Settings Policy** 를 클릭하십시오.

   b. 정책 이름을 **NGFW Settings Policy** 로 지정합니다

   c. **NGFW** 장치를 선택하고 **Add to Policy** 를 클릭하십시오.

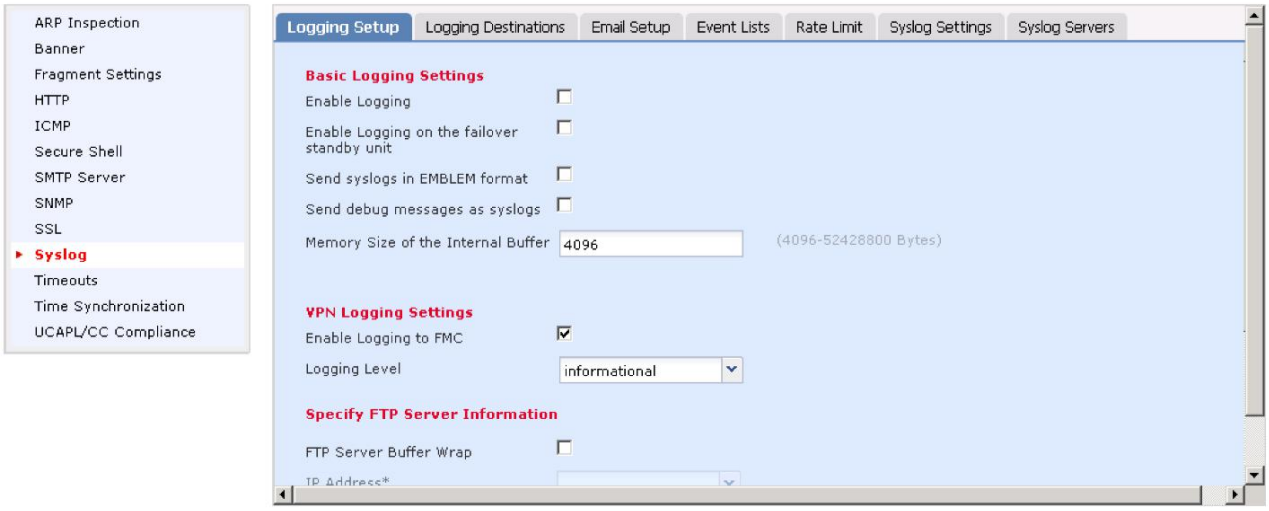


d. **Save** 를 클릭하십시오. 편집 화면이 열릴때까지 기다립니다.

e. 왼쪽 탐색 창에서 **Syslog** 를 선택하십시오.

f. **VPN Logging Settings** 에서 로깅 레벨을 **informational** 로 변경합니다. 프로덕션 환경에서는 errors 또는 alerts 로 설정하는 것이 좋습니다.

g. **Save** 를 클릭합니다.



NGFW RA VPN 설정 확인 및 구성

1. 장치에 정책을 배포합니다.
    a. FMC 에서 **Deploy** 버튼을 클릭합니다.
    b. **NGFW** 를 선택하고 **Deploy** 를 클릭하십시오.
    c. 배포가 완료될 때까지 기다립니다.

2. NGFW CLI 의 PuTTY 세션이 아직 열려 있어야 합니다. 다음 명령어의 일부 또는 전부를 실행하십시오.
    a. **show running-config tunnel-group**
    b. **show running-config group-policy**
    c. **show running-config crypto**
    d. **show running-config ip local pool**
    e. **show running-config nat**

3. NGFW CLI 에서 다음 명령을 실행하여 AAA 를 테스트 합니다.

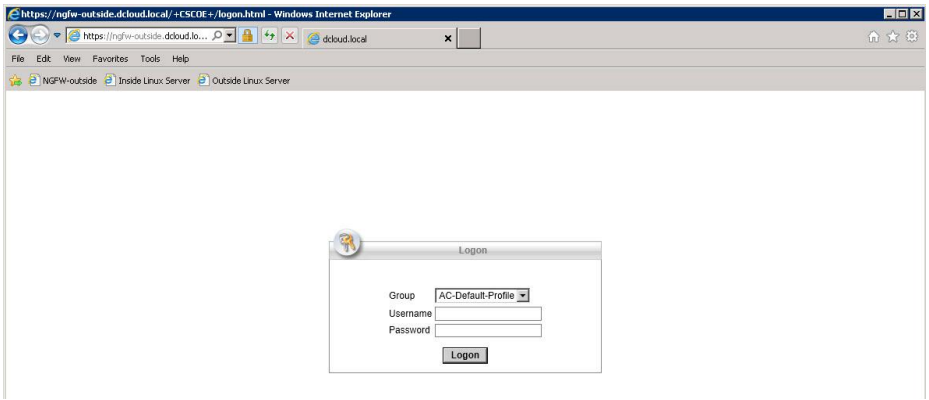
    test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password 'C1sco12345'

    Jumper 데스크탑의 Strings to cut and paste.txt 파일에서 이 명령어를 복사 붙여넣기 할 수 있습니다.

```
> test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password 'C1sco12345'
INFO: Attempting Authentication test to IP address (198.19.10.130) (timeout: 32 seconds)
INFO: Authentication Successful
>
```

구성 테스트

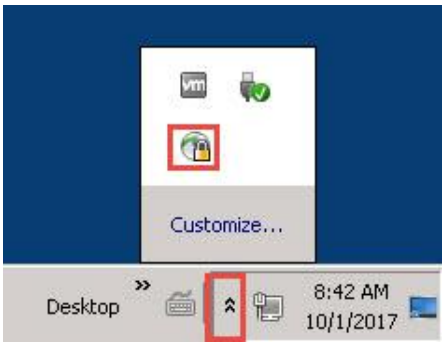
1. Jumper 데스크탑에서 **Remote Desktops** 폴더를 열고 **Outside-PC** 를 더블클릭하십시오.
    a. **Internet Explorer** 를 열고 즐겨찾기에서 **NGFW-outside** 를 클릭하십시오.



    b. **이용자명**에 **ira** 을 입력하고 **패스워드**에 **C1sco12345** 를 입력한 다음 **Logon**.
    c. 페이지 하단의 **Install** 버튼을 클릭하십시오. 메시지가 나타나면 다시 **Install** 를 클릭하십시오.

d. 설치가 완료되면 AnyConnect VPN 이 자동으로 연결됩니다

e. 아래 그림과 같이 Outside-PC 의 오른쪽 하단에서 AnyConnect 클라이언트 UI 를 엽니다.



2. 아래 그림과 같이 톱니바퀴 아이콘을 클릭하여 AnyConnect 클라이언트 UI 의 **Advance Window** 을 엽니다.

a. 클라이언트의 **Statistics** 탭을 선택하십시오.

b. 스플릿 터널링을 확인하려면 **Route Details** 정보 탭을 선택합니다. 198.19.10.0/24 로 향하는 트래픽만 보안 경로를 이용합니다. 즉, 198.19.10.0/24 로 향하는 트래픽만 VPN 을 통해 터널링됩니다. 그리고 198.19.10.100/32 도 보안 경로를 통과한다고 나와 있습니다. 이는 VPN 그룹 정책이 198.19.10.100 을 DNS 서버로 클라이언트에 할당했기 때문입니다.

3. NGFW CLI 에서 **show vpn-sessiondb detail anyconnect** 을 실행하여 세션을 확인합니다.

```
> show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username     : ira                    Index        : 60244
Assigned IP  : 198.19.13.10           Public IP    : 198.18.133.23
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : Clientless: (1)AES256  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (
1)AES256
Hashing      : Clientless: (1)SHA256  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA          1
(Output omitted)
```

4. Outside-PC 에서 명령 프롬프트를 엽니다.
    a. **nslookup inside.dcloud.local** 을 실행합니다. PC-outside 가 198.19.10.100 IP 주소로 내부 DNS 서버를 사용하고 있는지 확인하십시오.

    b. 다음 명령을 실행하십시오.

    ftp inside.dcloud.local

    계정은 **guest**, 패스워드는 **C1sco12345** 를 사용하여 로그인하십시오. 로그인을 통해 내부 서버에 대한 접근성을 확인합니다.

    c. **cd ~root** 입력하면 다음 메시지가 표시됩니다.

    Connection closed by remote host.

    이것은 침입 차단(intrusion protection) 기능이 작동하고 있음을 알려줍니다.

5. Internet Explorer 의 즐겨찾기에서 **Inside Linux Server** 를 클릭합니다.
    a. **Files** 링크를 클릭합니다. **ProjectX.pdf** 링크를 클릭하고 웹 페이지 하단에 **Open** 버튼을 클릭하여 PDF 를 다운로드 할 수 있는지 확인하십시오.

    b. **Zombies.pdf** 링크를 클릭하고 웹 페이지 하단의 **Open** 버튼을 클릭하십시오. 웹 페이지 하단에 아래의 메시지가 표시됩니다. 파일이 네트워크 AMP 에 의해 차단되었기 때문입니다.

6. FMC 에서 **Analysis > Intrusions > Events** 로 이동합니다.
    a. Snort 룰 336 이 트리거된 것을 확인합니다.
    b. **Table View of Events** 로 이동하여 소스 IP 주소가 VPN pool 에서 제공된 것 인지 확인합니다.

7. FMC 에서 **Analysis > Files > Malware Events** 로 이동합니다.
    a. **Zombies.pdf** 가 차단되었는지 확인하십시오.
    b. 멀웨어 이벤트의 Table View 로 이동하여 소스 어드레스가 VPN Pool 에서 나왔는지 확인하십시오.

8. 다음 실습에 앞서 AnyConnect VPN 연결을 끊습니다.

시나리오 4. RADIUS 속성을 이용한 AnyConnect

이 연습은 다음 작업으로 구성됩니다.

- 새 그룹 정책(New group policy) 만들기
- 새로운 IP Pool 만들기
- 액세스 컨트롤(Access control) 및 NAT 정책 수정
- 커넥션 프로파일 수정
- 구성의 배포 및 테스트

이 연습에서는 ISE 의 RADIUS 특성을 사용해 AD 그룹의 이용자를 기반으로 그룹 정책, IP Pool 및 다운로드형 ACL(DACL)을 동적으로 할당합니다.

- RA VPN 사용자가 IT 그룹의 멤버라면 내부 네트워크의 모든 장치(174.16.1.0/24)에 대해 모든 액세스 권한을 가져야 합니다.
- 만약 RA VPN 사용자가 IT 그룹의 멤버 아니라면 아래 두 개의 내부 장치에만 액세스가 가능합니다.
    - 도메인 컨트롤러, ad1.dcloud.local (198.19.10.100)
    - 내부 Linux 서버, inside.dcloud.local (198.19.10.200).
- IT 그룹 멤버인 사용자는 별도의 IP Pool 에서 IP 주소를 제공 받아야합니다.

시간 절약을 위해 ISE 는 랩 실습에 필요한 모든 구성이 사전에 정의되어 있으며 여기에는 AD 그룹 멤버쉽을 기반으로 그룹 정책 및 IP Pool 집합을 포함하고 있습니다. 따라서 새로운 그룹 정책 및 IP Pool 의 이름은 시나리오가 제공하는 이름과 정확히 일치해야 합니다. ISE 구성을 확인하려면 부록 C 를 참조하십시오.

스텝

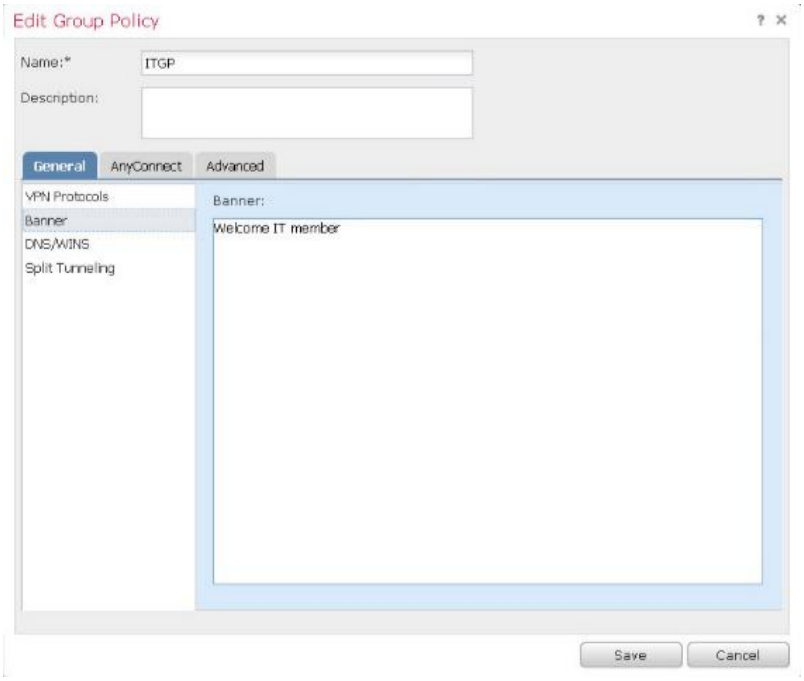
새 그룹 정책 만들기

기본적으로 DfltGrpPolicy 와 같은 그룹 정책을 만듭니다. 실습을 통해 ISE 가 사용자의 Active Directory 그룹을 기반으로 어떻게 그룹 정책을 할당하는지를 보여줍니다. 이 연습에서 별도의 구성을 추가해 보는 것이 더 흥미로울 수 있지만, 이 시나리오에서 다루지는 않겠습니다.

1. FMC 에서 **Object > Object Management > VPN > Group Policy** 로 이동합니다.
2. **Add Group Policy** 를 클릭하십시오.

3. 이름에 ITGP 를 입력하십시오. 기존 ISE 구성 때문에 그룹 이름이 정확해야 합니다.

4. **General** 탭에서 **Banner** 를 선택합니다. **Welcome IT Member** 텍스트를 입력하십시오.



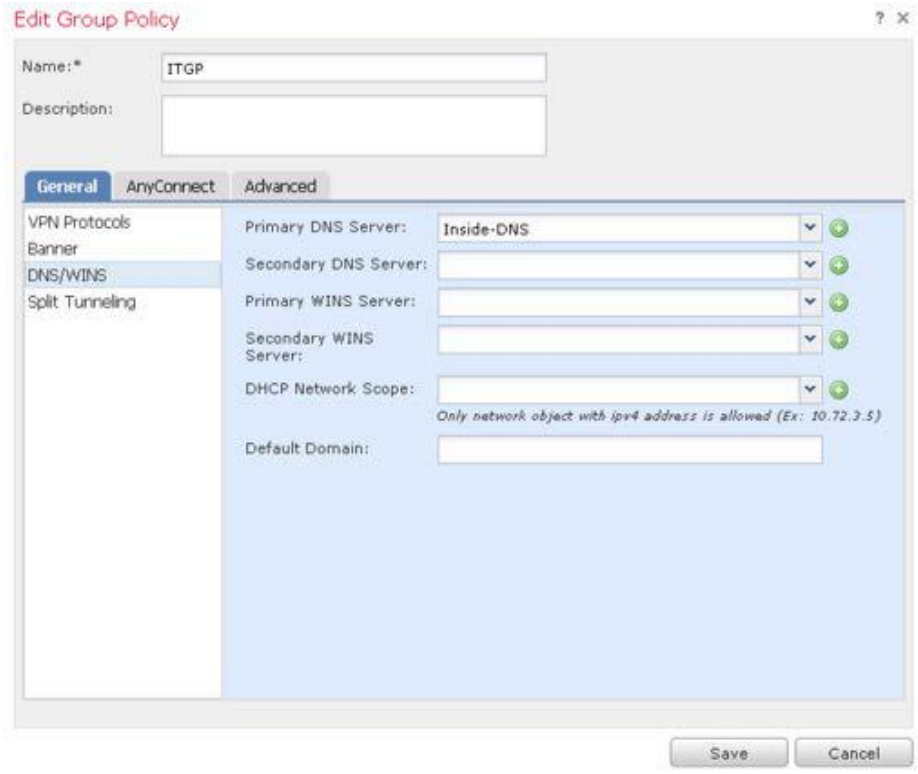
5. **General** 탭에서 **Split Tunneling** 을 선택합니다.

    a. **IPv4 Split Tunneling** 에 **Tunnel networks specified below** 를 선택하십시오.

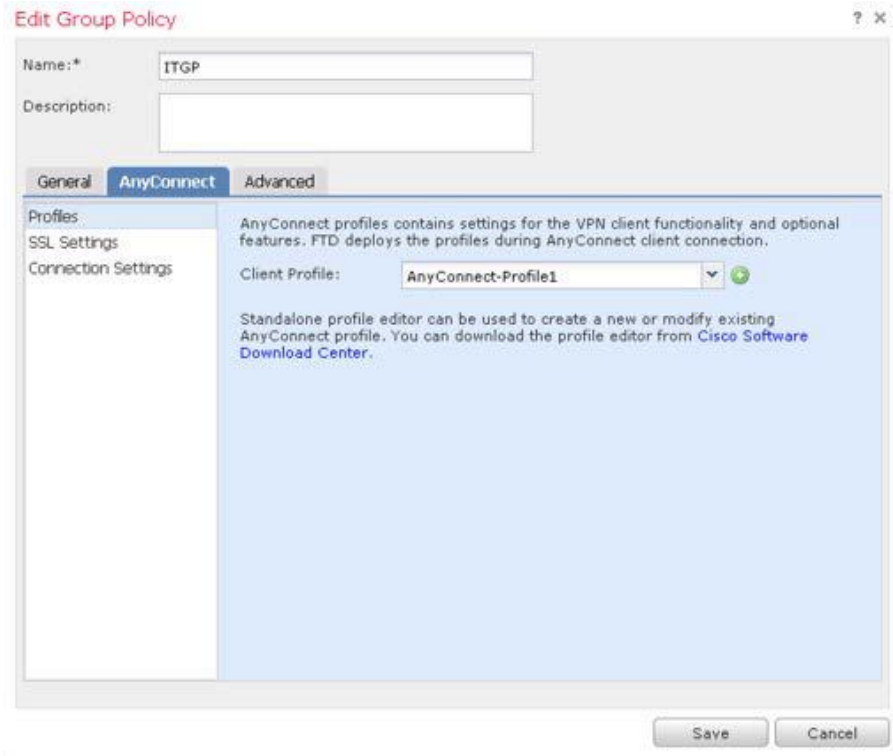
    b. **Extended Access List** 를 선택합니다.

    c. **Access List** 에 **AC-SplitTunnel1** 을 선택하십시오.

6. **General** 탭에서 **DNS/WINS** 선택합니다. **Primary DNS Server** 에 **Inside-DNS** 를 선택하십시오.



7. **AnyConnect** 탭을 선택하십시오 . Client Profile 에 **AnyConnect-Profile1** 을 선택하십시오.



8. **Save** 을 클릭하여 그룹 정책을 저장합니다.

새 IP Pools 만들기

1. IP Pool 을 만듭니다.

    a. FMC 에서 **Objects > Object Management > Address Pools > IPv4 Pools** 로 이동하십시오.

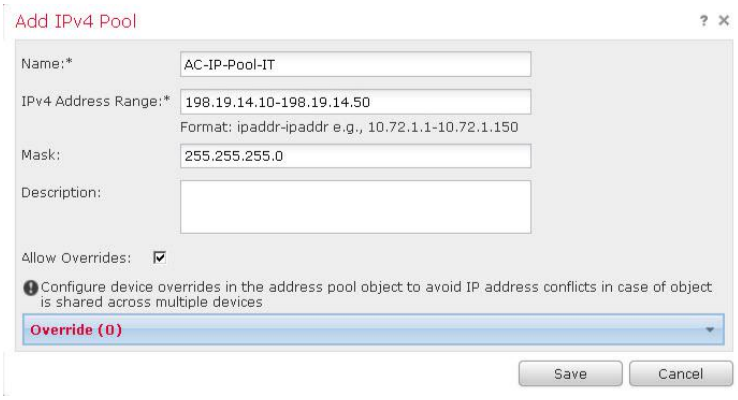
    b. **Add IPv4 Pools** 를 클릭하십시오.

    c. Name 탭에 **AC-IP-Pool-IT** 를 입력하십시오. 기존 ISE 구성 때문에 그룹 이름이 정확해야 합니다.

    d. **IPv4 Address Range** 탭에 **198.19.14.10-198.19.14.50** 을 입력하십시오.

    e. Mask 에 **255.255.255.0** 을 입력하십시오.

    h. **Save** 를 클릭.



액세스 컨트롤 및 NAT 정책 수정

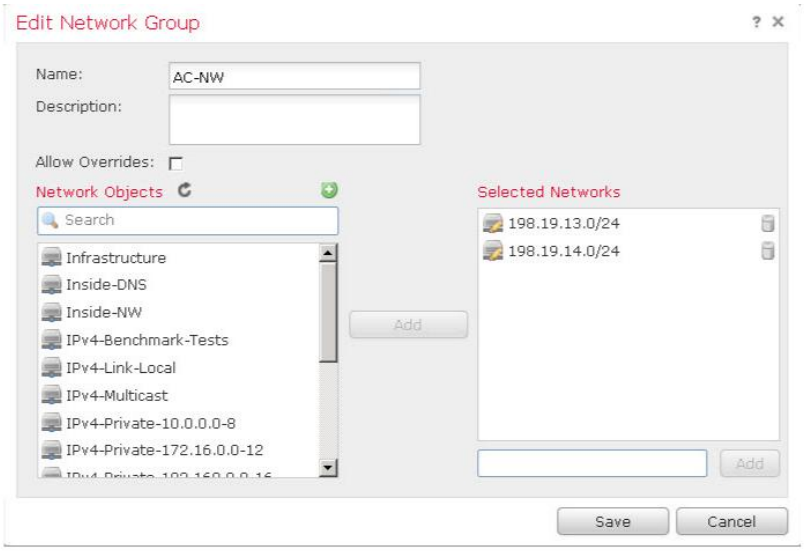
액세스 컨트롤 와 NAT 정책 모두 수정하려면 **AC-NW** 네트워크 그룹의 오브젝트만 수정하면 됩니다.

1. FMC 에서 **Object > Object Management > Network** 으로 이동하십시오.

    a. 네트워크 그룹 **AC-NW** 를 선택하고 편집합니다.

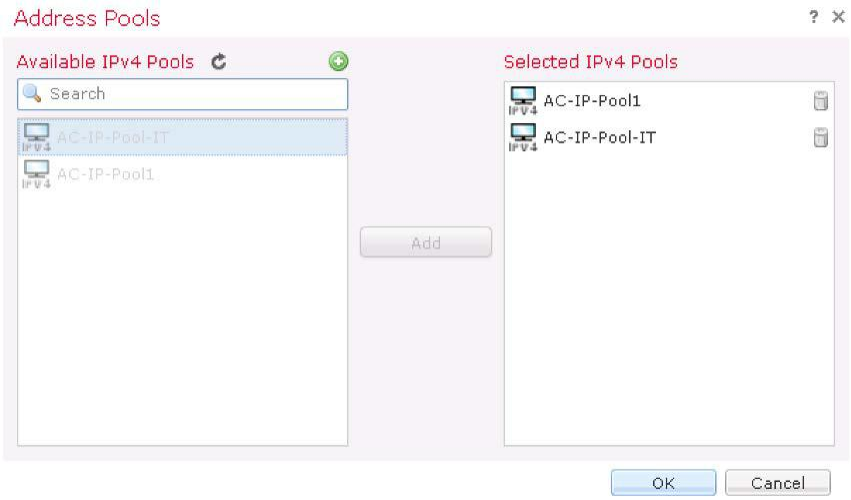
    b. **Selected Networks** 에서 하단 텍스트 필드에 **198.19.14.0/24** 를 입력하고 **Add** 를 클릭하십시오.

    c. **Save** 를 클릭.

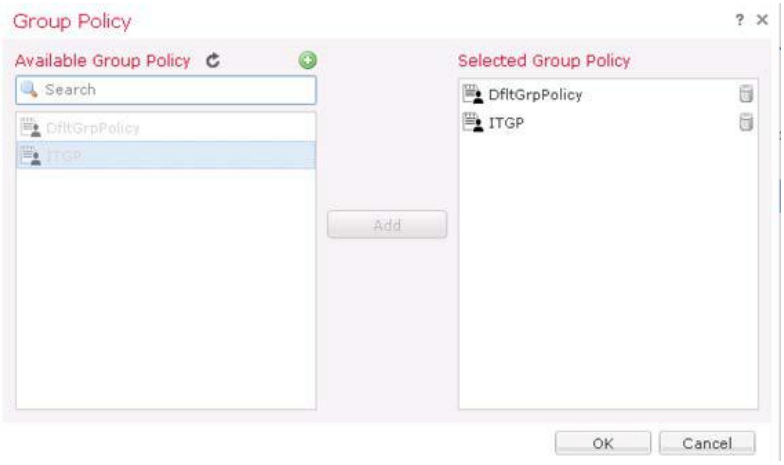


커넥션 프로파일 수정

1. FMC 에서 **Devices > VPN > Remote Access** 로 이동하십시오.
2. **AnyConnect-VPN** 을 편집하십시오. 그 다음 **AC-Default-Profile** 커넥션 프로파일을 선택 및 편집하십시오.
3. 새로 생성된 IP Pool 을 추가합니다.
    a. 클라이언트 **Address Assignment** 탭이 이미 선택되어져 있어야합니다
    b. **Address Pools** 에서 (+) 더하기 아이콘을 클릭하고 **IPv4** 를 선택하십시오.
    c. **AC-IP-Pool-IT** 를 선택하고 **Add** 를 클릭하십시오.



    d. **OK** 를 클릭하십시오.
    e. **Edit Connection Profile** 창에서 **Save** 를 클릭하십시오..
4. 새로 생성된 그룹 정책을 추가합니다
    a. AnyConnect-VPN 페이지의 **Advanced** 탭을 선택하고 왼쪽 탐색 창에서 **Group Policies** 를 선택하십시오.
    b. (+) 아이콘을 클릭하십시오.
    c. **ITGP** 를 선택하고 **Add** 를 클릭합니다.



    d. **OK** 클릭하고 **Save** 를 클릭.

구성 적용 및 테스트

1. NGFW 에 변경 사항을 적용합니다. 완료까지 기다립니다.

2. Outside PC 원격 데스크톱 세션으로 돌아갑니다.
   a. AnyConnect client 에서 Connect 클릭.

   b. 이용자명은 **harry**, 패스워드는 **C1sco12345** 를 사용하여 로그인하십시오. Harry 는 IT 그룹의 멤버가 아닙니다.

   c. AnyConnect 가 연결되면 Outside-PC 명령 프롬프트에서 다음 2 가지 명령을 실행하십시오.
      i. **ping inside.dcloud.local**. 이것은 성공해야 합니다.
      ii. **ping altinside.dcloud.loca**l. 이것은 실패해야 합니다. 왜냐하면 ISE 가 기본적으로 할당하는 DACL 은 도메인 컨트롤러 및 내부 Linux 서버에 대한 액세스만 허용하기 때문입니다.

3. NFGW CLI 에서 다음 명령어를 실행합니다.

   show vpn-sessiondb detail anyconnect

   출력 내용에서 아래 값을 확인하십시오.

   a. Username: **harry**

   b. Assigned IP: **198.19.13.x**

   c. Group Policy: **DfltGrpPolicy**

   d. Filter Name: **#ACSACL#-IP-AC-DACL- Default-x**

```
> show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username     : harry                    Index        : 53216
Assigned IP  : 198.19.13.10             Public IP    : 198.18.133.23
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15410                    Bytes Rx     : 516
Pkts Tx      : 16                       Pkts Rx      : 8
Pkts Tx Drop : 0                        Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy            Tunnel Group : AC-Default-Profile
(Output omitted)

> Filter Name   : #ACSACL#-IP-AC-DACL-Default-598b5954
```

4. Outside- PC 원격 데스크톱 세션으로 돌아갑니다.

   a. AnyConnect VPN 세션 연결 끊기.

   b. AnyConnect VPN 세션을 새로 시작하십시오.

   c. 계정은 **rita**, 패스워드는 **C1sco12345** 로 로그인하십시오. Rita 는 IT 그룹 멤버입니다.

   d. ITGP 에 배너가 구성되어 있는지 확인한 다음 **Accept** 를 클릭하십시오.

   e. AnyConnect 가 연결되면 Outside-PC 명령 프롬프트에서 다음 2 가지 명령을 실행하십시오

      i. **ping inside.dcloud.local**. 이것은 성공해야 합니다.

      ii. **ping altinside.dcloud.local**. 이것도 성공해야 합니다. ISE 가 IT 그룹에 할당한 DACL 는 모든 내부 장치에 대해 액세스를 허용합니다.

5. NFGW CLI 에서 다음 명령을 실행합니다.

   show vpn-sessiondb detail anyconnect

   출력 내용에서 아래 값을 확인하십시오.

   a. Username: **rita**

   b. Assigned IP: **198.18.14.x**

   c. Group Policy: **ITGP**

   d. Filter Name: **#ACSACL#-IP-AC-DACL-IT-x**

```
> show vpn-sessiondb detail anyconnect
Username      : rita                    Index        : 4998
Assigned IP   : 198.19.14.10           Public IP    : 198.18.133.23
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx      : 15375                   Bytes Rx     : 691
Pkts Tx       : 16                      Pkts Rx      : 9
Pkts Tx Drop  : 0                       Pkts Rx Drop : 0
Group Policy  : ITGP                    Tunnel Group : AC-Default-Profile (Output omitted)
  (Output omitted)


> Filter Name   : #ACSACL#-IP-AC-DACL-IT-598b1f19
```

6. AnyConnect VPN 클라이언트의 연결을 끊습니다.

시나리오 5. 클라이언트 인증서를 이용한 AnyConnect

이 연습은 다음 작업으로 구성됩니다.

- 커넥션 프로파일 수정
- 구성 설치 및 테스트

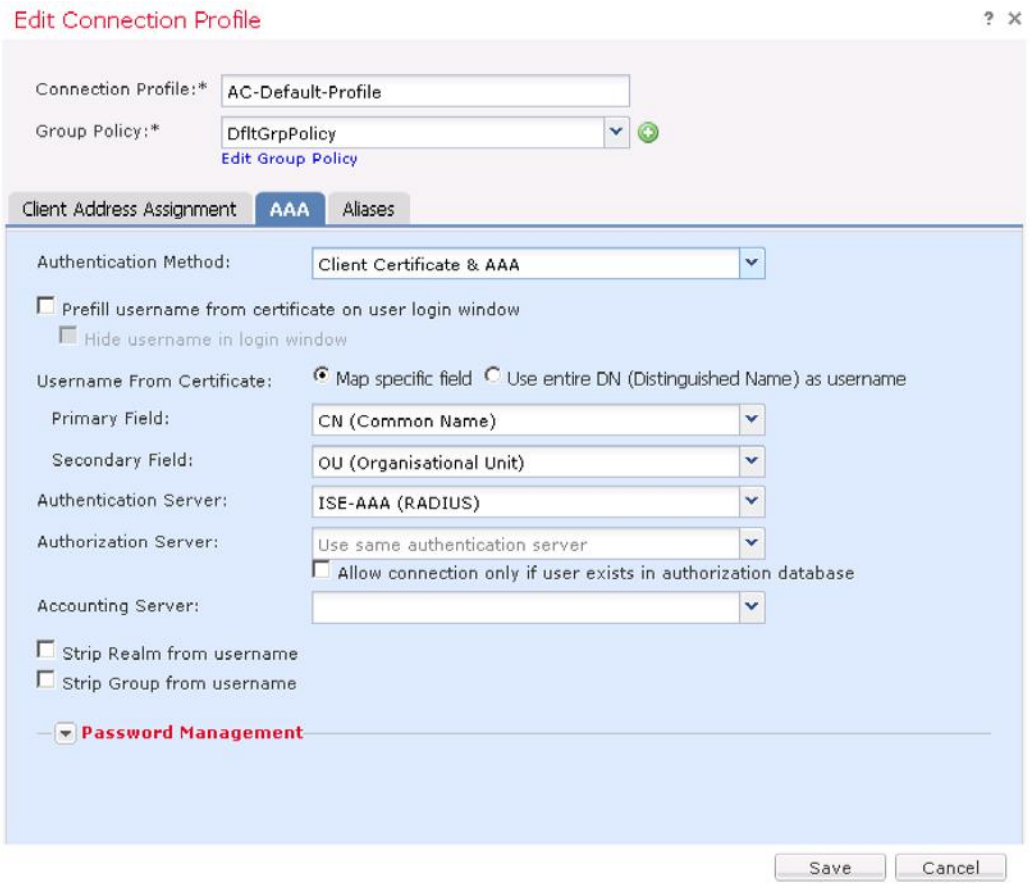
이 연습에서는 사용자가 RA VPN 에 대해 이중 인증 (certificate and AAA)을 구성할 수 있도록 합니다.

노트: 시간을 절약하기 위해 클라이언트 인증서가 Outside-PC 에 미리 설치되어 있습니다.

스텝

커넥션 프로파일 수정

1. FMC 에서 **Devices > VPN > Remote Access. Edit AnyConnect-VPN** 으로 이동하십시오.
    a. **Connection Profile** 에서 **AC-Default-Profil**e 커넥션 프로파일을 선택하고 편집하십시오.
    b. **AAA** 탭을 선택하고 인증 방식인 **Authentication Method** 를 **Client Certificate & AAA** 로 변경하십시오.



    c. **Edit Connection Profile** 페이지에서 **Save** 를 클릭하십시오.
    d. **AnyConnect-VPN** 페이지에서 **Save** 를 클릭하십시오.

구성 적용 및 테스트

1. NGFW 에 변경 사항을 구성합니다. 구성이 완료 될 때까지 기다립니다.

2. Outside-PC 원격 데스크톱으로 돌아갑니다
    a. AnyConnect 클라이언트를 연결하십시오
    b. 계정은 **rita**, 패스워드 **C1sco12345** 로 로그인합니다. 이 랩에서는 이용자가 누구인지 중요하지 않습니다.

3. NFGW CLI 에서 다음 명령을 실행합니다.

    show vpn-sessiondb detail anyconnect

    인증 모드가 **Certificate and userPassword** 인지 확인하십시오.

```
> show vpn-sessiondb detail anyconnect
  (Output omitted)
AnyConnect-Parent:
  Tunnel ID     : 52614.1
  Public IP     : 198.18.133.23
  Encryption    : none                  Hashing       : none
  TCP Src Port : 49286                  TCP Dst Port : 443
  Auth Mode     : Certificate and userPassword


>(Output omitted)
```

4. **AnyConnect VPN 연결을 끊지 마십시오**. 다음 랩 실습으로 바로 이동합니다.

시나리오 6. 모니터링 및 트러블 슈팅

이 연습은 다음 작업으로 구성됩니다.

- 모니터링
- 트러블슈팅

AnyConnect 이용자 활동에 대한 모니터링 및 트러블 슈팅을 위해 FMC 를 사용합니다.

스텝

AnyConnect 이용자 활동 모니터링

이 섹션에서는 AnyConnect 를 통해 로그인한 모든 액티브 사용자를 모니터링할 수 있습니다.

1. FMC 에서 **Overview > Dashboards > Access Controlled User Statistics** 로 이동합니다.
2. **VPN** 탭을 선택하십시오. VPN 트래픽과 관련된 7 개의 위젯이 있습니다.
3. **Analysis > Users > Active Sessions** 으로 이동합니다.
    a. Rita 의 VPN 세션을 볼 수 있습니다.
    b. Rita 의 세션 왼쪽에 있는 체크 박스를 선택하고 로그 아웃(**Logout**.)을 클릭하십시오. 메시지가 나타나면 계속(**Continue**)을 클릭하십시오.

네트워크 디스커버리를 통해 확인된 다른 액티브 세션을 볼 수도 있습니다. 예를 들면, FTP 세션을 통해 발견된 게스트를 볼 수 있습니다. 랩 간소화를 위해 해당 세션은 위 그림에서 제외되었습니다. 사용자 및 사용자가 어떻게 디스커버리됐는지에 대해 자세한 내용을 보려면 Analysis > Users > Users 로 이동하십시오.

4. Outside-PC 에서 Rita 가 로그아웃 되었는지 확인합니다.
5. FMC 에서 **Analysis > Users > User Activity** 로 이동합니다. 이 화면에서는 현재 및 과거의 사용자 세션에 대한 세부 사항을 확인할 수 있습니다. 몇 분 동안 이 페이지에 표시된 정보를 살펴보십시오.

트러블 슈팅

이 세션에서는 NGFW 에서 VPN 이벤트의 Syslog 수준을 수정합니다. 또한 NGFW CLI 에서 몇 가지 기본 트러블슈팅 명령을 실행합니다

1. FMC 에서 **Device > VPN > Troubleshooting** 으로 이동합니다. 기록을보아야합니다. 그렇지 않으면이 페이지에서 시간대를 조정하십시오.
2. NGFW CLI 에서 다음 명령어 중 일부를 실행하여 트러블 슈팅으로 활용할 수 있습니다. RA VPN 의 문제점 해결시 유용하며 참고용으로 포함되었습니다.
    a. **show vpn-sessiondb ?**
    b. **test aaa-server ?**
    c. **debug crypto ca ? (good for trouble-shooting certificate issues)**
    d. **debug crypto ipsec ?**
    e. **debug ldap ?**
    f. **debug aaa ?**

시나리오 7. 시스코 Threat Intelligence Director (TID)

이 연습은 다음 작업을 포함합니다.

- 웹 서버에서 STIX 파일 검색
- 복잡한 지표(Indicator) 및 관련 Observable 분석
- 인시던트를 트리거할 URL 목록을 CTID 에 업로드
- CTID 를 TAXII 피드에 구독
- CTID 인시던트를 생성

CTID 는 타사의 사이버 위협 인텔리전스 지표를 사용할 수 있는 FMC 의 구성 요소입니다. CTID 는 이러한 지표를 분석하여 NGFW 가 탐지 가능한 Observable 을 생성합니다. NGFW 는 Observable 의 탐지 내용을 보고합니다. 그 다음 CTID 는 Observation 이 인시던트를 구성하는지 판단여부를 결정합니다.

두 가지 파일 포맷이 지원됩니다.

- 플랫 파일 - IP 주소, URL 또는 SHA256 해시와 같은 간단한 indicator 목록
- STIX 파일 - 단순 또는 Complex indicator 를 설명하는 XML 파일

이 파일들을 검색하는 방법에는 세 가지가 있습니다.

- FMC UI 가 실행되는 컴퓨터에서 업로드
- 원격 웹 서버의 URL 로부터 검색
- TAXII 피드에서 수신 (STIX 파일만)

이 연습의 목적은 CTID 를 구성하고 테스트하는 것 입니다.

스텝

CTID 가 Observable 을 NGFW 에게 발행하는지 확인

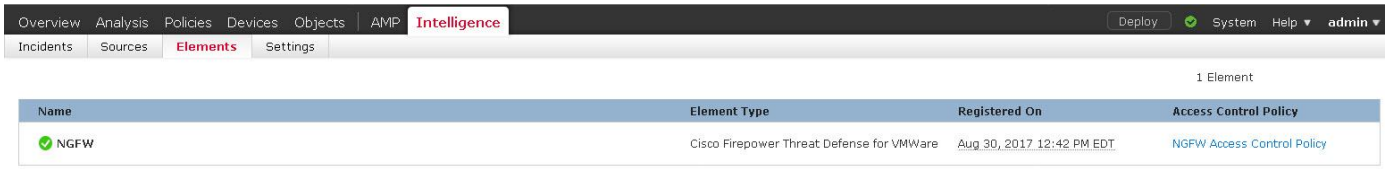
1. **Policies > Access Control > Access Control** 로 이동하십시오.
2. 정책 오른쪽에 있는 **연필모양 아이콘을** 클릭하여 액세스 컨트롤 정책(access control policy)을 편집합니다.
3. **Advanced** 탭을 선택하십시오.

4. **Enable Threat Intelligence Director** 가 기본값으로 활성화되어 있는지 확인합니다.

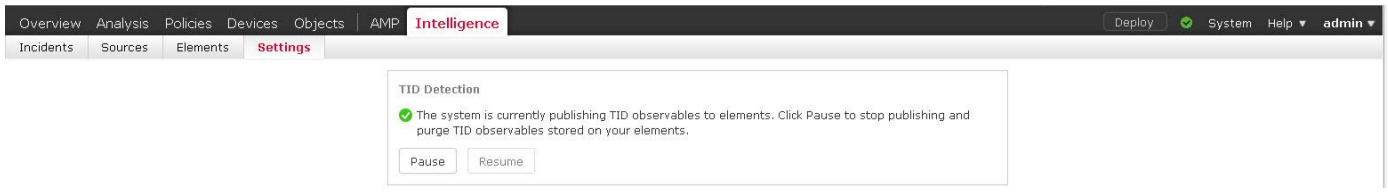
5. 이 고급 설정을 사용하여 액세스 정책(access policy) 레벨에서 CTID 를 사용하거나 사용하지 않도록 설정할 수 있습니다

6. **Intelligence > Elements** 으로 이동하십시오.

7. **NGFW** 가 Element 로 되어 있는지 확인합니다. 이는 CTID 가 NGFW 에게 Observable 을 발행할 수 있음을 보여줍니다.



8. **Intelligence > Settings** 으로 이동합니다. 그리고 시스템이 observable 을 CTID Element 에 발행할 수 있도록 구성되어 있는지 확인합니다.



노트: 여기서 CTID 는 글로벌하게 활성화 또는 비활성화 할 수 있습니다. 일시 중지(Pause)를 클릭하면 모든 Element 에 대한 CTID 발행이 중지됩니다.

웹 서버에서 STIX 파일 검색

1. **Intelligence > Sources > Sources** 으로 이동하십시오.

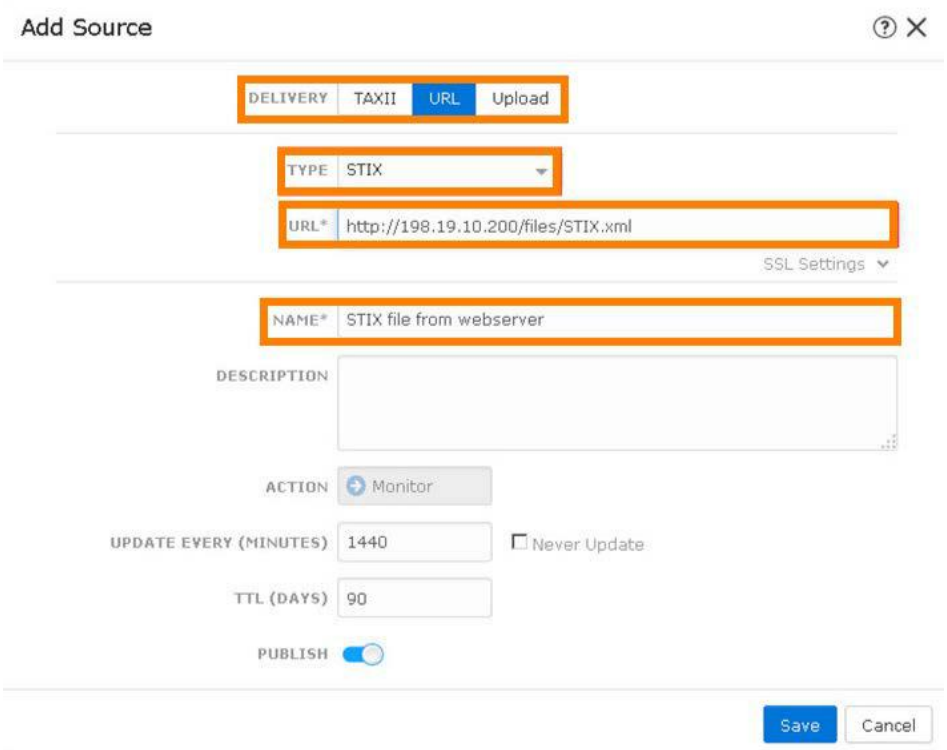
2. 오른쪽의 더하기 기호 (**+**)를 클릭하여 인텔리전스 소스를 추가하십시오.

3. **DELIVERY** 에 **URL** 를 선택하십시오.

4. **TYPE** 에, **STIX** 가 선택되었는지 확인하십시오.

5. **URL** 에 **http://198.19.10.200/files/STIX.xml** 를 입력하십시오.

6. **NAME** 에 **STIX file from webserver** 을 입력하십시오.



7. **Save** 를 클릭.

노트: STIX 파일에 대해 모니터에서 차단으로 액션 변경을 할 수 없습니다. STIX 파일은 Complex Indicators 를 나타내기 때문에 Observable 을 기반으로 한 NGFW 이 Indicator 기준이 충족되었는지를 결정하는 것은 불가능합니다. 그러나 Complex Indicators 에 대해서 개별 observable 을 차단하도록 설정할 수는 있습니다.

8. 몇 초 후에, **Intelligence > Sources > Indicators** 으로 이동합니다. Indicator 가 추가되었는지 확인하십시오.

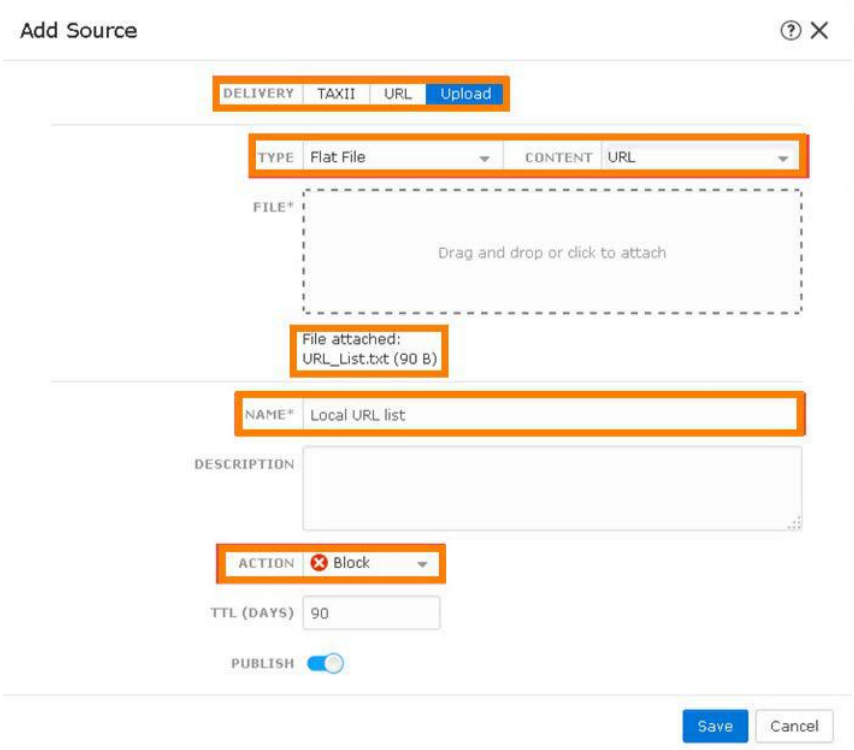
9. **Weatherman PUA 의** indicator 이름을 클릭하십시오. Indicator 세부 내용을 살펴봅니다.

10. **Close** 를 클릭하여 indicator 의 세부 내용 페이지를 닫습니다.

11. **Intelligence > Sources > Observables** 으로 이동합니다. 두 개의 **SHA-256** 과 한 개의 **IPv4** observable 이 추가되었는지 확인하십시오.

인시던트를 트리거하는 URL 목록을 CTID 에 업로드

1. **Intelligence > Sources > Sources** 으로 이동한 후, 오른쪽에 있는 더하기 기호 (+)를 클릭하여 인텔리전스 소스를 추가하십시오.
2. **DELIVERY** 에 **Upload** 을 선택하십시오.
3. **TYPE** 에 **Flat File** 을 선택하면 **CONTENT** 드롭 다운 목록이 나타납니다
4. **CONTENT** 에 **URL** 을 선택하십시오
5. **FILE** 영역을 클릭하고, Jump 데스크톱의 **Files** 폴더에서 **URL_LIST.txt** 를 선택하십시오.
6. **NAME** 에 **Local URL list** 를 입력합니다.
7. **ACTION** 은 **Block** 을 선택합니다.



8. **Save** 를 클릭합니다.
9. 몇 초 후, **Intelligence > Sources > Indicators** 으로 이동하십시오. 두 개의 URL indicator 가 추가되었는지 확인하십시오.
10. **Intelligence > Sources > Observables** 으로 이동하십시오. 두 개의 URL observable 이 추가되었는지 확인하십시오.

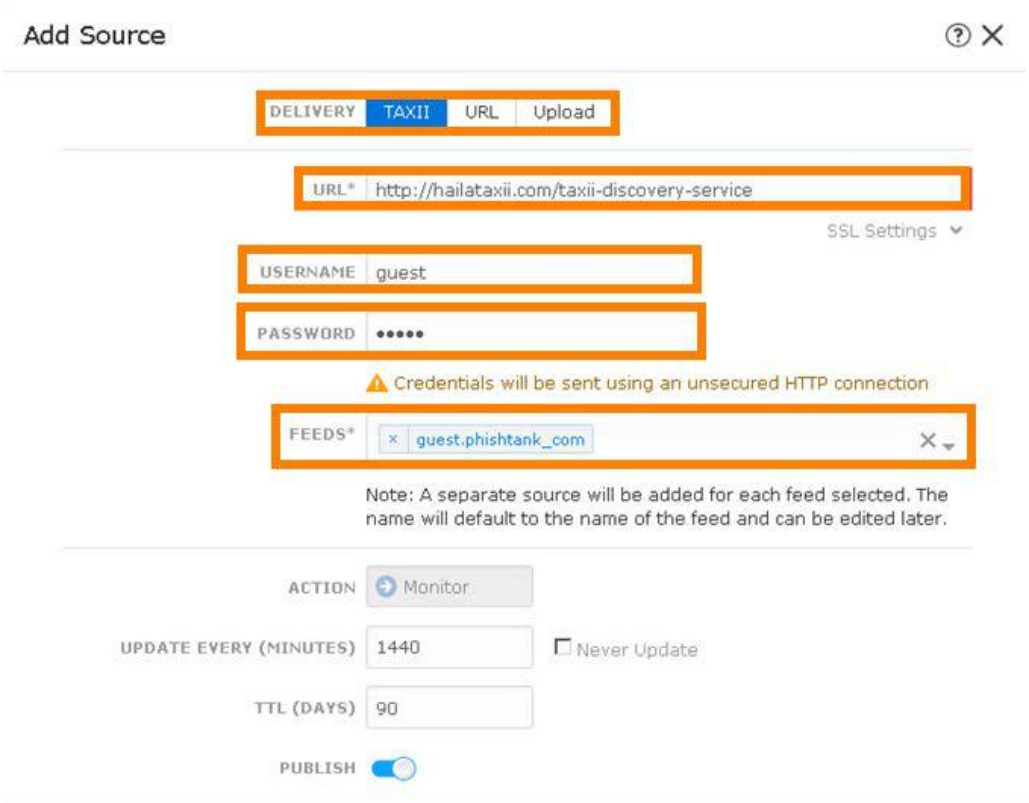
TAXII 피드에 CTID 구독

노트: 여기에 사용된 TAXII 피드는 Hail a TAXII 피드입니다.이 피드에 문제가 있는 경우는 Alien Vault 를 사용할 수 있습니다. 자세한 내용은 부록 D 를 참조하십시오.

1. **Intelligence > Sources > Sources** 으로 이동한 후 오른쪽에 있는 더하기 기호 (+)를 클릭하여 인텔리전스 소스를 추가하십시오.
2. **DELIVERY** 에는 **TAXII** 를 선택하십시오.
3. **URL** 에 **http://hailataxii.com/taxii-discovery-service** 를 입력하십시오.
4. **USERNAME** 에 **guest** 를 입력하십시오.
5. **PASSWORD** 에 **guest** 를 입력하십시오.
6. **FEEDS 로 guest_phishtank_com** 을 선택하십시오.

노트: FEED 의 드롭 다운 목록이 나타나기 까지 몇 초 정도 걸릴 수 있습니다.

7. 화면이 아래 그림과 같은지 확인하십시오.

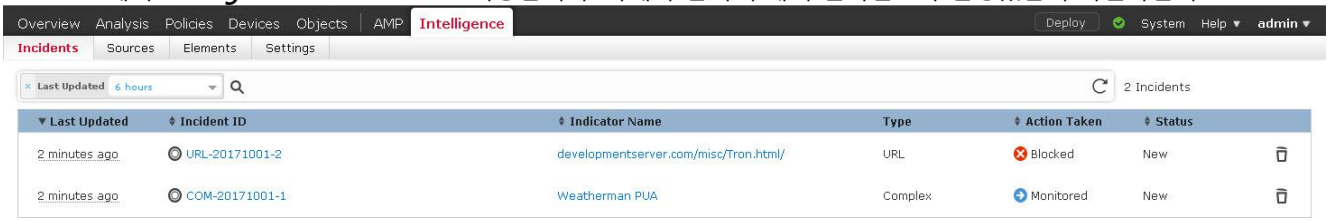


8. **Save** 를 클릭합니다.

9. 이 소스에 대한 상태 열이 **Parsing** 으로 바뀔 때까지 기다립니다. **Parsing** 완료까지 오랜 시간이 소요되기 때문에 기다리지는 마십시오.
10. **Intelligence > Sources > Indicators** 로 이동합니다. 여러 개의 URL indicator 가 추가되었는지 확인하십시오.
11. **Intelligence > Sources > Observables** 로 이동합니다. 여러 개의 URL observable 이 추가되었는지를 확인하십시오.

CTID 인시던트의 생성

1. FMC 에는 obervable 을 NGFW 과 5 분에 한 번씩 동기화하는 데몬이 있습니다. 따라서 observable 이 센서(NGFW)로 발행되기 까지 몇 분이 걸릴 수 있습니다. 이 스텝에서는 특정 observable 에 대한 발행을 확인하는 방법을 살펴봅니다. NGFW CLI 에서 다음을 수행하십시오.
    a. Expert 모드로 들어가려면 **expert** 를 입력하십시오.
    b. **ls -d /var/sf/*download** 를 입력하십시오. 나열된 디렉토리가 여러 개 있습니다.
    admin@ngfw:~$ ls -d /var/sf/*download
    /var/sf/clamupd_download /var/sf/iprep_download /var/sf/sifile_download
    /var/sf/cloud_download/var/sf/sidns_download /var/sf/siurl_download
    이 중에 4 개는(iprep_download, sidns_download, sifile_download and siurl_download) 보안 인텔리전스 및 CTID 에서 사용됩니다.
    c. **grep developmentserver /var/sf/*download/*lf** 를 입력하십시오.
    admin@ngfw:~$ grep developmentserver /var/sf/*download/*lf
    /var/sf/siurl_download/731625d4-9512-11e7-915c-
    7e7252ae92ac.lf:developmentserver.com/misc/Tron.html/
    이 부분이 보이지 않으면 잠시 기다렸다가 다시 시도하십시오. 다음 단계로 진행하기 전에 이 부분이 게시될 때까지 기다려야 합니다. 계속 실패하면 CTID 소스를 삭제하고 다시 추가하십시오.
    d. **grep 198.18.133.200 /var/sf/*download/*lf** 를 입력하십시오
    admin@ngfw:~$ grep 198.18.133.200 /var/sf/*download/*lf
    /var/sf/iprep_download/730f187a-9512-11e7-915c-7e7252ae92ac.blf:198.18.133.200
    이 부분이 보이지 않으면 잠시 기다렸다가 다시 시도하십시오. 계속하기 전에 게시 될 때까지 기다려야합니다. 계속 실패하면 CTID 소스를 삭제하고 다시 추가하십시오.
    e. **exit** 를 입력하여 Expert 모드를 종료합니다.
2. Inside Linux 서버 CLI 에서는:
    a. **wget -t 1 outside/files/ProjectX.doc** 을 실행하며 이 부분은 성공해야 합니다.
    b. **wget -t 1 developmentserver.com/misc/Tron.html** 을 실행하고 이 부분은 차단되야 합니다.
3. FMC 에서 ***Intelligence > Incidents*** 로 이동합니다. 아래와 같이 두개의 인시던트가 발생했는지 확인하십시오.



4. 해당 인시던트를 드릴 다운하여 세부 사항을 확인하십시오.
5. URL indicator 에 대한 인시던트가 있는지 확인하십시오. 해당 인시던트의 세부 사항을 같이 확인합니다.

시나리오 8. FlexConfig

이 시나리오 연습은 아래 작업으로 구성됩니다.

- 사용자 정의 FlexConfig 오브젝트 만들기
- 시스템 정의 FlexConfig 오브젝트에서 사용되는 텍스트 오브젝트 수정
- FlexConfig 정책 생성 및 구성
- 변경 사항 배포 및 구성 테스트

FlexConfig 는 FTD 에서 Lina (ASA) 구성에 직접 구성을 배포 할 수 있게 해주는 기능입니다. 이 기능을 사용하여 FTD 에서 아직 사용할 수없는 기능을 따로 구성할 수 있게 합니다. 이 실습에서는 아래의 두 가지를 테스트합니다.

- 사용자 정의 FlexConfig 오브젝트를 사용하여 EIGRP 를 구성합니다.
- 시스템 정의 FlexConfig 오브젝트를 사용하여 SIP 검사를 비활성화합니다.

노트: EIGRP 구성을 위한 별도의 시스템 정의 FlexConfig 오브젝트가 있습니다. 시간이 지남에 따라 변경될 수 있는 구성의 경우는 이러한 오브젝트를 사용하는 것이 좋습니다. 그러나 본 실습에서는 FlexConfig 가 제공하는 단순성 및 가치 확인을 위해 별도의 사용자 정의 FlexConfig 오브젝트를 사용합니다.
시스템 정의 FlexConfig 오브젝트는 FTD 를 NetFlow 데이터의 소스로 구성하는데 사용됩니다.

사용자 정의 FlexConfig 오브젝트 만들기

1. FMC UI 에서 **Objects > Object Management** 로 이동하십시오.
2. 왼쪽 창의 아래쪽에 있는 **FlexConfig** 에서 **FlexConfig Object** 를 선택합니다.
3. **Add FlexConfig Object** 를 클릭하십시오.
    a. Name 에 **myEIGRP** 를 입력합니다.
    b. 메인 텍스트 영역에 다음 명령어을 입력하십시오. 넷 마스크는 / 24 가 아니라 / 18 입니다.
    ```
    router eigrp 10
     network 198.18.128.0 255.255.192.0
    ```
    c. **Save** 를 클릭합니다.

시스템 정의 FlexConfig 오브젝트를 위한 텍스트 오브젝트 수정

1. FMC UI 의 **Object Management** 페이지에 있어야합니다.
2. **Default_Inspect_Protocol_Disable** 이라는 Flex 오브젝트의 오른쪽에 있는 돋보기 아이콘을 클릭하십시오. 이 오브젝트는 편집 할 수는 없지만 필요한 경우 복사는 할 수 있습니다.

노트: FlexConfig 오브젝트는 Apache Velocity 언어로 작성됩니다. 이 언어는 loops 및 if 를 지원하며 #로 시작하며 이 부분은 코멘트가 아닙니다. 출력에 포함되는 리터럴 텍스트가 아님을 나타냅니다. 코멘트는 ##로 시작합니다.
이 FlexConfig 오브젝트는 **disableInspectProtocolList** 라는 텍스트 오브젝트를 loops 합니다. 우리는 이 텍스트 오브젝트를 편집합니다.

---

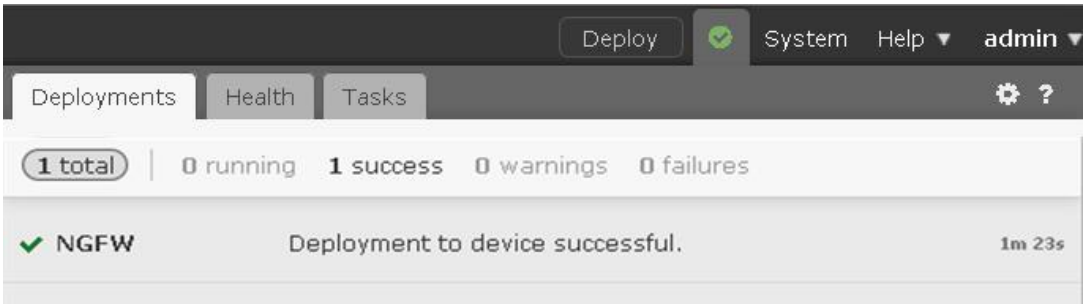
3. **Close** 를 클릭하십시오.
4. **Object Management** 페이지의 왼쪽 탐색 창 맨 아래에 있는 **FlexConfig** 에서 **Text Object** 를 선택합니다.
5. **disableInspectProtocolList** 라는 텍스트 오브젝트를 편집하십시오.
6. 이 변수는 여러 값을 취합니다. 값을 **1** 로 놔둡니다.
7. **sip** 값을 입력하십시오.
8. **Save** 를 클릭하십시오.

FlexConfig 정책 생성 및 구성

1. **Devices > FlexConfig** 로 이동합니다. **New Policy**.를 클릭합니다.
    a. **Name** 에 **NGFW Flex Policy** 를 입력하십시오.
    b. **NGFW** 디바이스을 선택하고 **Add to Policy** 를 클릭하십시오
    c. **Save** 를 클릭합니다.
2. 편집을 위해 정책이 열릴때까지 잠시 기다리십시오.
    a. 왼쪽 열의 **User Defined** 에서 **myEIGRP** 를 선택하십시오.  를 클릭하여 FlexConfig 오브젝트를 정책에 추가하십시오.
    b. 왼쪽 열의 **System Defined** 에서 **Default_Inspect_Protocol_Disable** 을 선택하십시오.  를 클릭하여 FlexConfig 오브젝트를 정책에 추가합니다.
    c. **Save** 를 클릭하십시오.
3. **Preview Config** 를 클릭합니다.
    a. **Select Device** 드롭 다운 목록에서 **NGFW** 를 선택하십시오.
    b. 잠시 기다리면 변경한 구성 내용이 나타납니다. 명령어 구성이 올바른지 확인하십시오. 또한 몇 가지 불필요한 VPN 명령어가 표시됩니다. 이 부분은 구성에 영향을 미치지 않으며 향후 릴리즈에서 수정될 예정입니다.
    c. **Close** 을 클릭하십시오.

변경 사항 배포 및 구성 테스트

1. NGFW CLI 에서 **show running-config policy-map** 을 실행합니다. SIP 검사가 활성화 상태인지 확인하십시오.
2. Inside Linux 서버 세션에서 **ping 204.44.14.1** 을 입력하십시오. 이것은 실패해야 합니다.
3. 변경 사항을 적용하십시오. 배포가 완료될 때까지 기다립니다.



4. NGFW CLI 에서 **show running-config policy-map** 을 실행하십시오. 이제는 SIP 검사가 비활성화 되었는지 확인합니다.
5. NGFW CLI 에서 다음 명령을 실행하십시오.
    a. **show eigrp neighbors** 를 실행하십시오. FTD 와 CSR 라우터간에 adjacency 가 형성되었는지 확인하십시오.
    b. **show eigrp topology** 를 실행하십시오. EIGRP 경로가 수신되었는지 확인하십시오.
    c. **show route eigrp** 를 실행하십시오. NGFW 가 이제 라우팅 테이블에 학습된 EIGRP 경로를 가지고 있는지 확인하십시오.
6. Inside Linux Server 세션에서 **ping 204.44.14.1** 을 입력하십시오. 이제는 성공해야 합니다.

시나리오 9. ASA 에서 NGFW 로 마이그레이션

이 시나리오는 아래 작업으로 구성됩니다

- FMC 를 마이그레이션 도구로 변환.
- ASA 오브젝트 마이그레이션.
- NAT 및 지원되지 않는 기능의 마이그레이션 및 오브젝트 재사용을 탐색.

이 연습의 목적은 마이그레이션 도구 사용에 익숙해지도록 하는 것입니다.

- 구성 방법
- 사용 방법

FMC 를 마이그레이션 도구로 변환하면 두 가지 구성이 마이그레이션됩니다. 오브젝트 flattening 및 지원되지 않는 기능의 처리 방법을 비롯한 마이그레이션의 여러 측면이 나타납니다.

스텝

FMC 를 마이그레이션 도구로 변환

1. Jump 데스크탑에서 PuTTY 를여십시오. **Migrator** 라는 미리 구성된 세션을 더블 클릭하십시오. 계정은 **admin**, 패스워드는 **C1sco12345** 입니다.

노트: 마이그레이션 수행에 필요한 도구는 수정된 FMC 입니다. 수정은 스크립트를 통해 실행됩니다. 이 FMC 는 일반적으로 VM 버전의 FMC 로 프로덕션 환경의 FMC 와 분리되어 있으며 프로덕션 환경의 FMC 를 마이그레이션 도구로 사용해서는 안됩니다.

2. **`sudo enableMigrationTool.pl`**.를 입력합니다.
    a. 메시지가 나타나면 패스워드로 **`C1sco12345`** 를 입력하십시오.
    b. 경고문을 주의 깊게 읽으십시오!
    c. 계속할 것인지 묻는 질문에 **Y** 를 입력하십시오.
    d. 스크립트가 완료 될 때까지 기다립니다. 이 작업은 1 분 이내로 완료됩니다.

3. Firefox 브라우저에서 새 탭을 엽니다.
    a. 즐겨찾기에서 **Migration Tool** 을 클릭하십시오. **Advanced** 및 **Add Exception** 를 클릭하십시오. 메시지가 나타나면 **Confirm Security Acceptation** 을 클릭하십시오.

노트: 마이그레이션 도구로 사용될 이 FMC 는 설치 후에 수정되지 않았습니다. 지금까지 사용한 이 FMC 는 사전에 구성된 설정이었습니다. 이 사전 구성에는 신뢰할 수있는 인증서가 포함하고 있습니다. 자세한 내용은 부록 A 를 참조하십시오.

    b. **계정은 admin**, 패스워드 **C1sco12345** 로 로그인하십시오.

c. 아래와 같이 UI 의 맨 위에 빨간색 배너가 표시되는지 확인하십시오.

MIGRATION TOOL INSTALLED / You are limited to ASA conversions only

ASA 오브젝트 마이그레이션

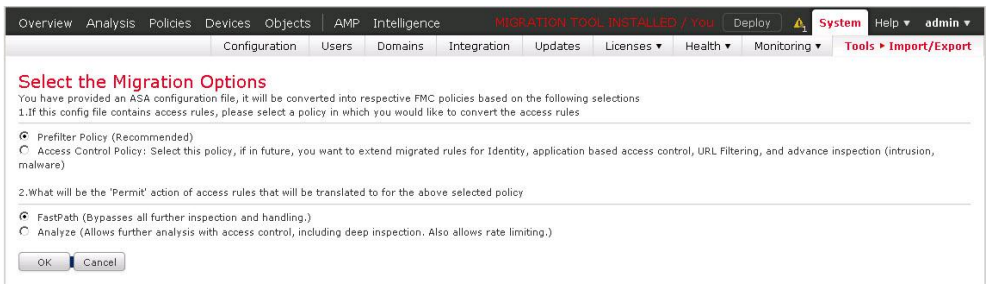
이 연습의 목표는 다음과 같습니다.

- 마이그레이션 과정을 학습.
- 네트워크 및 서비스 오브젝트, 오브젝트 그룹이 어떻게 마이그레이션되는지 이해하기.

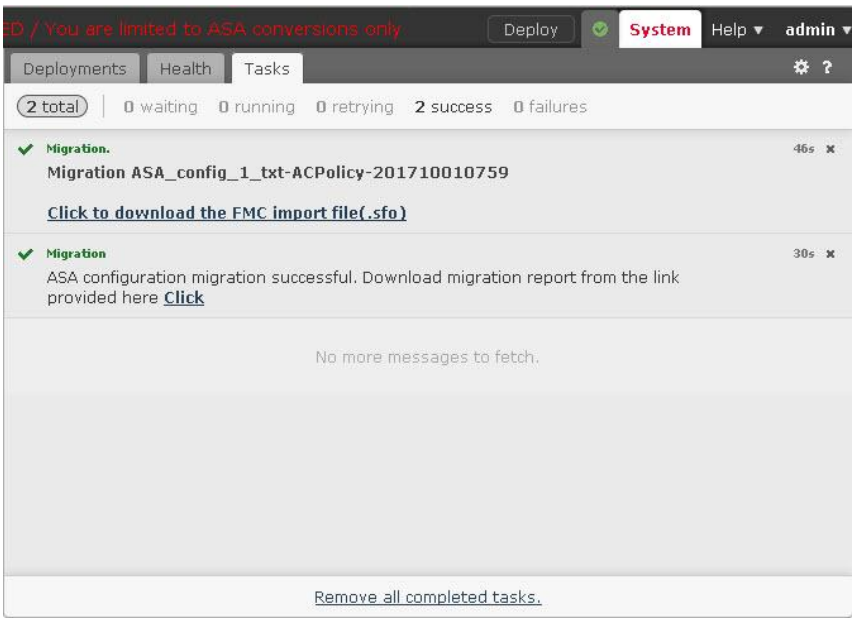
1. Jump 의 파일 폴더에서 **ASA_config_1.txt** 파일을 엽니다.
   a. 중첩된 네트워크 및 서비스 오브젝트가 있음을 관찰합니다.
   b. 이러한 오브젝트를 참조하는 액세스 리스트와 액세스 그룹이 있는지 확인하십시오. 액세스 그룹이 없으면 오브젝트는 정책 구성에 영향을 주지 않으므로 마이그레이션되지 않습니다.

2. Migrator UI 에서 **System > Tools > Import/Export** 로 이동합니다.
   a. **Upload Package** 를 클릭합니다.
   b. **Browse** 를 클릭하여 **Files** 폴더에 있는 **ASA_config_1.txt** 파일을 선택하십시오.
   c. **Upload** 를 클릭합니다.

3. 다음 페이지에서 아래와 같이 설정을 변경하지 않고 **OK** 를 클릭하십시오.



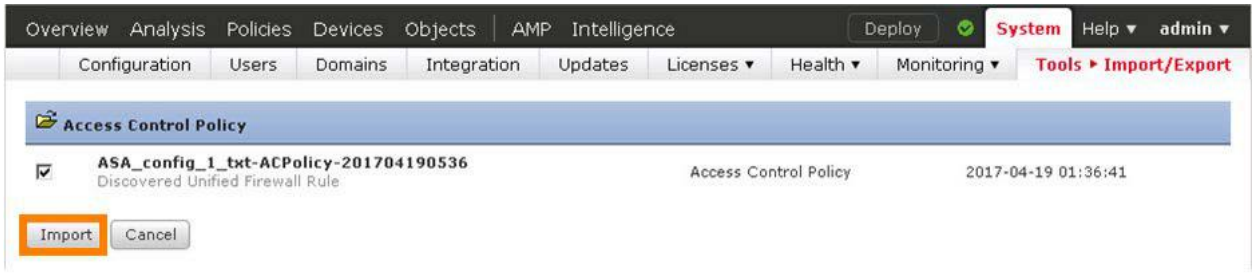
4. **Upload** 페이지로 돌아갈 때까지 기다리십시오
    a. **Deploy** 버튼 오른쪽에 있는 아이콘을 클릭하십시오
    b. **Task** 탭을 클릭하고 작업이 완료될 때까지 기다립니다.



    a. **Click to download the FMC import file(.sfo)** 텍스트를 클릭하고 SFO 파일을 저장하십시오.
    b. **Click** 텍스트를 클릭하고 기본값 **Open with Google Chrome** 를 선택하여 마이그레이션 보고서를 엽니다. 컨버전 보고서 내용에 오류가 없는지 확인하십시오. Chrome 을 종료합니다.

5. (프로덕션 환경의) FMC UI 에서 **System > Tools > Import/Export** 로 이동합니다.
    a. **Upload Package** 를 클릭합니다.
    b. **Browse** 를 클릭하고 **Downloads** 폴더에서 SFO 파일을 선택하십시오. 파일명은 **ExportForMigration-<some UUID>.sfo** 입니다. **Open** 을 클릭합니다.
    c. **Upload** 를 클릭.

6. 다음 페이지에서 **Import** 를 클릭하십시오.



7. 불러오기가 완료될 때까지 기다리십시오.

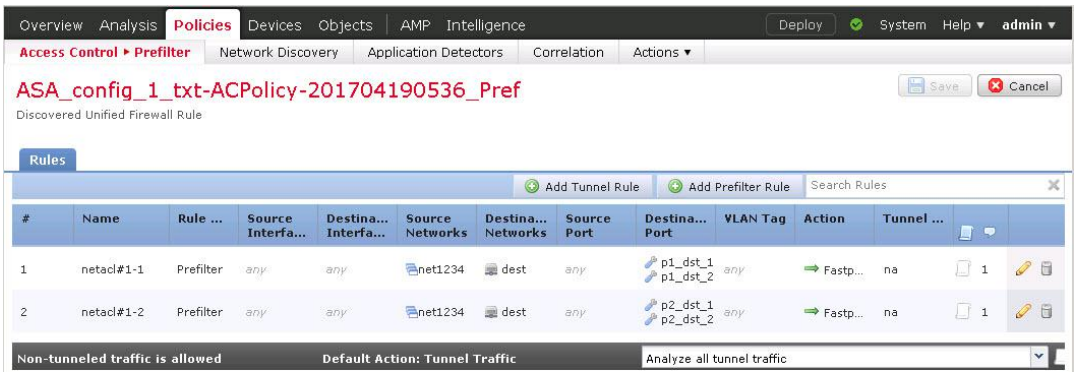
8. **Objects > Object Management** 으로 이동합니다.
    a. **Network** 오브젝트 페이지가 선택됩니다. 생성된 오브젝트에 주목합니다.
        - 4 개의 네트워크 오브젝트 **net1**, **net2**, **net3**, **net4**
        - 3 개의 네트워크 그룹 **net12** 및 **net34**
        - 하나의 중첩 네트워크 그룹 **net1234**

노트: 이것은 정확히 ASA 구성에 있었던 네트워크 및 네트워크 그룹 오브젝트 입니다.

    b. 왼쪽 창에서 **Port** 를 선택하십시오. 생성된 오브젝트에 주목합니다.
        - 4 개의 포트 오브젝트 **p1_dst_1**, **p1_dst_2**, **p2_dst_1**, **p2_dst_2**
        - 제로 포트 그룹

노트: ASA 포트 그룹 p1 및 p2 가 병합되었으며 p12 는 없습니다.

9. **Policies > Access Control > Prefilter** 로 이동합니다
    a. 새로운 사전 필터 정책이 있습니다. 룰을 검사 할 수 있도록 편집하십시오.
    b. 이 단일 ACE 는 ASA 구성이며 2 개의 개별적인 사전 필터 룰입니다.



10. **Policies > Access Control > Access Control** 로 이동합니다.
    a. 새 액세스 컨트롤 정책이 있습니다. 내용을 확인할 수 있도록 편집합니다.
    b. 룰이 없고 기본 동작은 차단으로 설정되어 있습니다.
    c. 사전 필터 정책은 전 단계에서 검사된 사전 필터 정책으로 설정됩니다.

NAT 및 미지원 기능의 마이그레이션 그리고 오브젝트 재사용 알아보기.

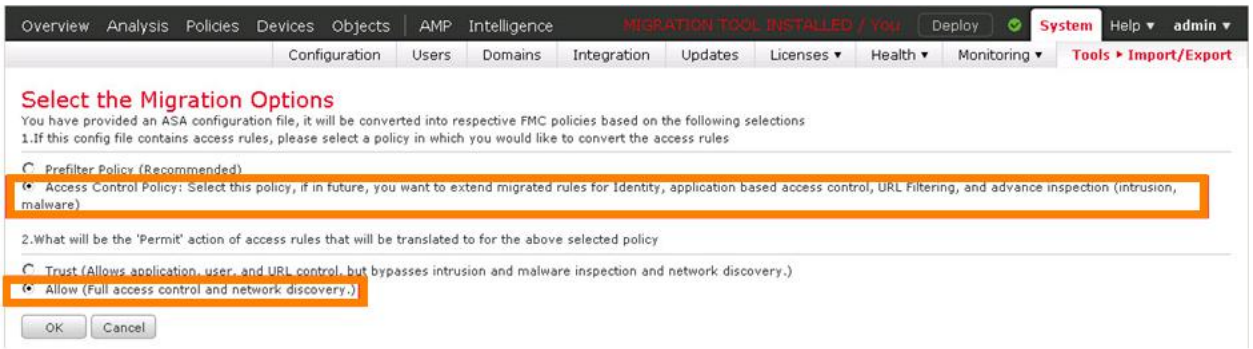
이 작업에는 세 가지 내용을 다루고 있으며 이들은 서로간에 직접 관련은 없습니다. 다만 이해를 돕기위해 포함되어 있습니다.

- NAT 정책의 마이그레이션.
- 오브젝트 재사용을 이해.
- 타임 기반의 ACL 을 마이그레이션하고 지원되지 않는 기능이 어떻게 처리되는지 보기.

1. Jump 의 **Files** 폴더에서 **ASA_config_2.txt** 파일을 엽니다.
    a. ASA 구성의 두 네트워크 오브젝트가 FMC 에 이미 있는 것을 확인하십시오.
        - 동일한 이름의 기존 오브젝트와 다른 정의를 가진 네트워크 오브젝트 **net1**
        - 동일한 이름을 가진 기존 오브젝트와 동일한 정의를 갖는 네트워크 오브젝트 **net2**
    b. Static NAT 규칙이 있음을 확인하십시오.
    c. 타임 기반 ACL 이 있음을 확인하십시오. 이 기능은 현재 지원되지 않습니다.

2. Migrator UI (FMC 아님)에서 **System > Tools > Import/Export** 로 이동합니다.
    a. **Upload Package** 를 클릭하십시오.
    b. **Browse** 를 클릭하고 **Files** 폴더에서 **ASA_config_2.txt** 파일을 선택하십시오. **Open** 을 클릭하십시오.
    c. **Upload** 를 클릭.

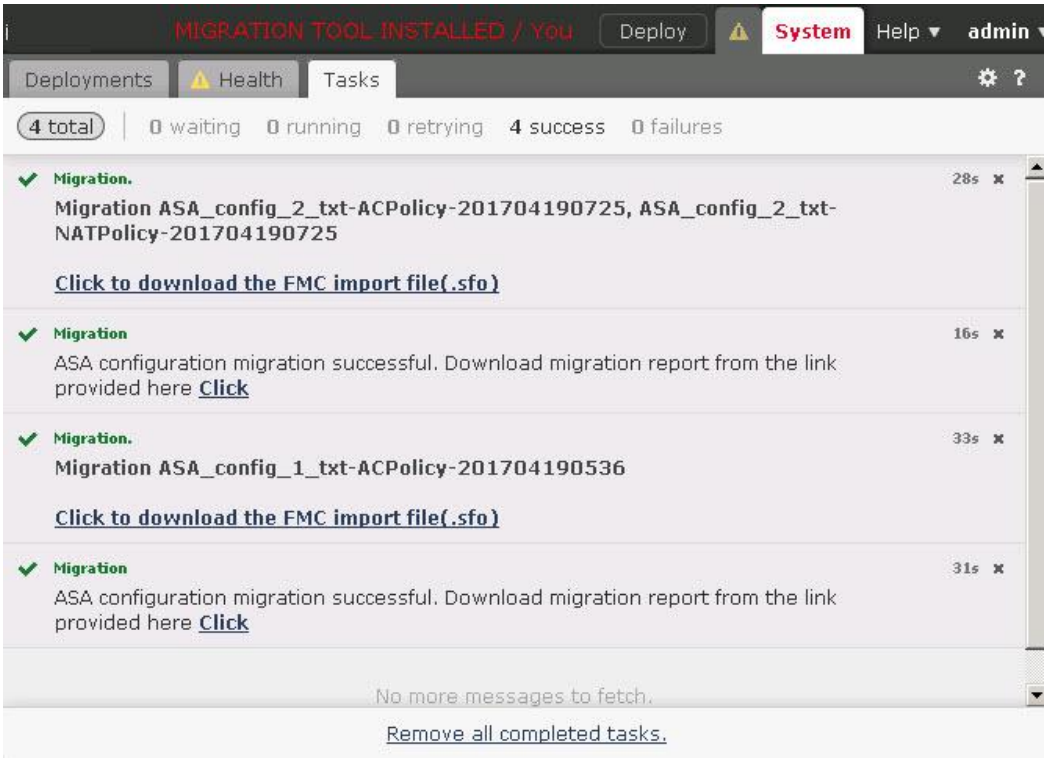
3. 다음 페이지에서 다음과 같이 **Access Control Policy** 과 **Allow** 를 선택하십시오. **OK** 을 클릭.



4. 업로드 페이지로 돌아갑니다.

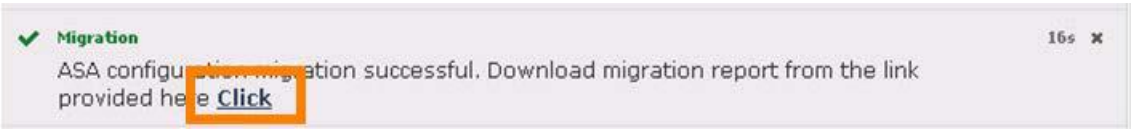
    a. **Deploy** 버튼 오른쪽에 있는 아이콘을 클릭하십시오.

    b. **Task** 탭을 클릭하고 작업이 종료될 때까지 기다립니다.



    c. **Click to download the FMC import file(.sfo)** 을 클릭하고 SFO 파일을 저장하십시오

    d. **Click 을** 클릭하고 기본값으로 **Open with Google Chrome** 을 선택하면 마이그레이션 보고서가 새 탭에 열립니다. 이 마이그레이션 보고서는 타입 기반 ACL 이 지원되지 않는다고 경고합니다. Chrome 을 종료합니다.



5. FMC UI(프로덕션) 에서 **System > Tools > Import/Export** 으로 이동합이다.

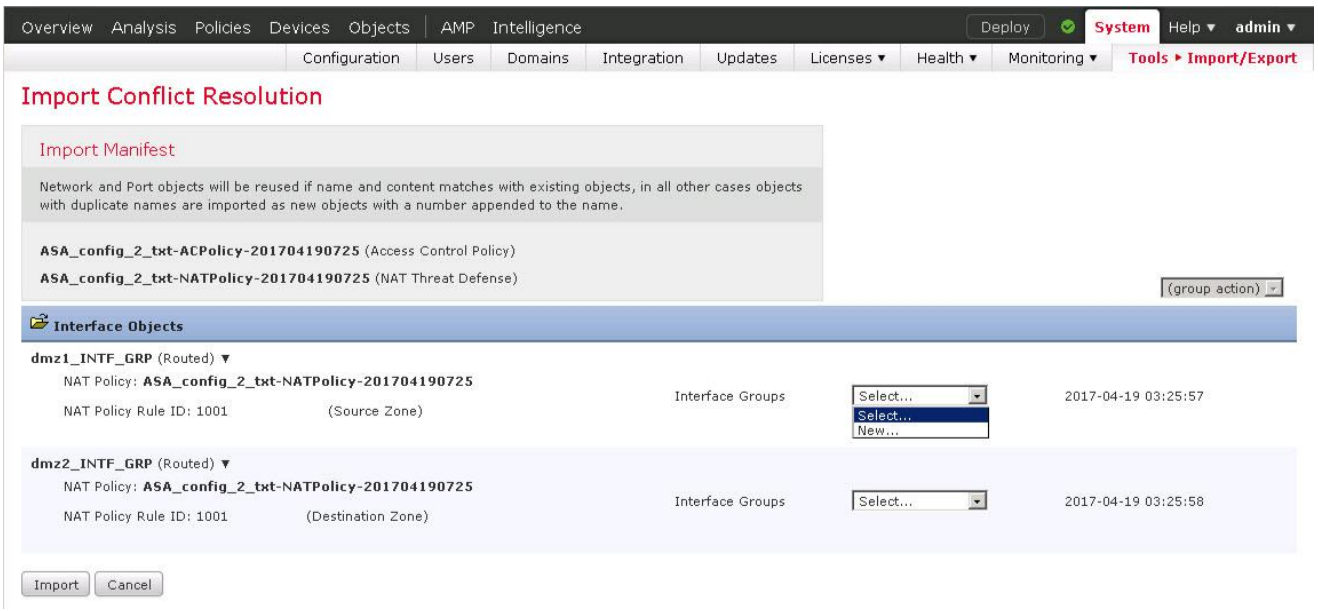
    a. **Upload Package** 버튼을 클릭하십시오.

    b. **Browse** 를 클릭하고 다운로드 폴더에서 SFO 를 선택하십시오. **ExportForMigration-<some UUID>.sfo** 라는 형식의 파일입니다. 가장 최근에 생성 된 SFO 파일을 선택하십시오.

    c. **Upload** 를 클릭.

6. 다음 페이지에서 **Import** 를 클릭.

7. 다음 페이지에서 아래의 하위 단계를 수행하십시오. 아래 그림을 참조합니다.



    a. 오브젝트 충돌 해결에 대한 내용 확인

    b. 이 페이지에서 드롭 다운 목록을 이용해 두 개의 인터페이스 그룹을 만듭니다. 마이그레이션된 NAT 룰을 참조하는 인터페이스는 인터페이스 그룹에 있어야 합니다. Security zone 은 허용되지 않습니다. **IF1** 과 **IF2** 라고 지정 할 수 있습니다.

    c. **Import** 를 클릭하십시오.

8. **Objects > Object Management** 로 이동하십시오. **Network** 오브젝트 페이지가 선택됩니다.

    a. **net1_1** 오브젝트가 만들어 졌는지 확인하십시오. 이는 마이그레이션 된 두 ASA 구성에서 **net1** 의 정의가 서로 달랐기 때문입니다. 따라서 오브젝트의 이름이 바뀌었습니다.

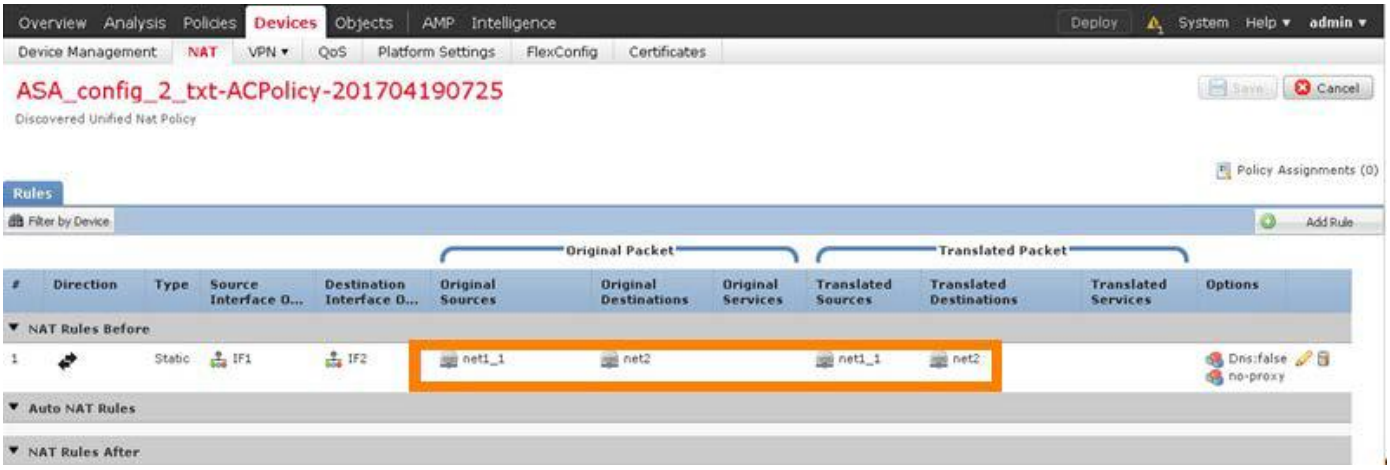
    b. **net2_1** 오브젝트가 생성되지 않았음을 확인하십시오. 이것은 마이그레이션 된 두 ASA 구성에서 **net2** 의 정의가 동일했기 때문입니다. 따라서 오브젝트가 재사용됩니다.

노트: 이 내용은 Firepower 6.2.1 릴리스에서 변경되었습니다. Firepower 6.2 에서는 두 오브젝트의 이름이 바뀝니다.

9. **Devices > NAT** 로 이동합니다.

    a. 새로운 NAT 정책이 나타납니다. 내용을 확인할 수 있도록 편집하십시오.

    b. 이 정책에서 오브젝트 **net1_1** 및 **net2** 가 참조됩니다.



10. **Policies > Access Control > Access Control** 로 이동합니다

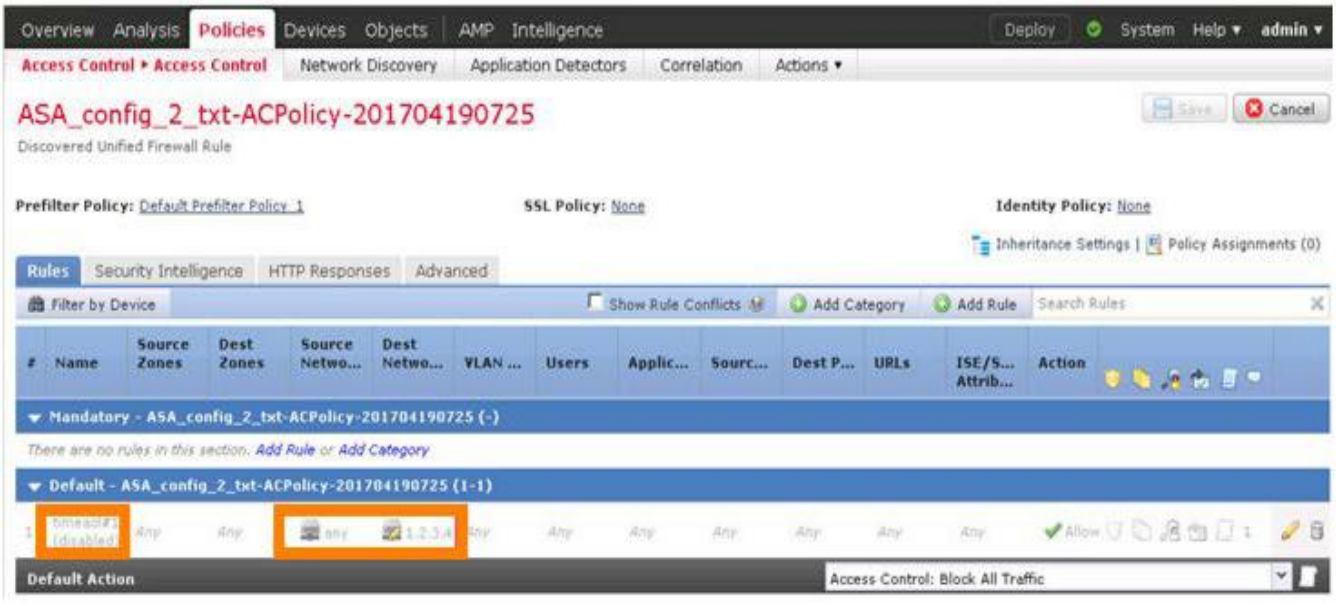
    a. 새 액세스 컨트롤 정책이 있습니다. 룰의 내용을 확인할 수 있도록 편집하십시오.

    b. 원래 ASA 구성의 ACL 은 다음과 같습니다:

    access-list timeacl extended permit ip any host 1.2.3.4 time-range office_hours

    이 내용은 동일한 출발지 및 목적지 정보를 사용해 액세스 컨트롤 정책의 규칙으로 변환되었음을 보여줍니다. 그러나 타임 범위에 대한 속성은 이 규칙에 포함되어 있지 않습니다.

c. 룰이 비활성화되어 있습니다. 원하는 경우 룰을 활성화할 수 있습니다.



노트: 마이그레이션 도구에 네트워크 및 타임 기반의 조건을 모두 포함하는 형태로 ACL 이 제공되었습니다. 다만 타임 기반의 ACL 은 현시점에서 지원되지 않으므로 마이그레이션 룰에는 네트워크 조건만 포함될 수 있습니다. 이런 부분으로 인해 규칙은 일단 비활성화 상태가 되고 수동으로 활성화 시켜야 합니다.

시나리오 10. NAT 및 라우팅

이 시나리오는 다음 작업으로 구성됩니다.

- 랩 실습에 필요한 오브젝트 생성
- Static NAT 구성
- wwwin 로의 외부 액세스 허용을 위한 액세스 컨트롤 정책의 수정
- BGP 구성
- 변경 사항 배포 및 구성 테스트
- 공인 웹 서버 만들기
- BGP 구성

첫 번째로 네트워크 오브젝트와 액세스 컨트롤 목록을 작성합니다. 또한 Static NAT 및 동적 라우팅을 구성합니다.

스텝

랩 실습에 필요한 오브젝트 만들기

1. **Objects > Object Management** 로 이동합니다. **Network** 오브젝트 페이지가 선택됩니다.
    a. **Add Network > Add Object**.를 클릭하십시오.
    b. **Name** 에 **wwwin** 을 입력하십시오.
    c. **Network** 에 **198.19.10.202** 를 입력하십시오
    d. **Save** 를 클릭하십시오
    e. **Add Network > Add Object** 를 클릭하십시오
    f. **Name** 에 **wwwout** 를 입력하십시오
    g. **Network** 에 **198.18.128.202** 를 입력하십시오
    h. **Save** 를 클릭하십시오
    i. **Add Network > Add Object** 를 클릭하십시오
    j. **Name** 에 **203.14.10.0** 를 입력하십시오
    k. **Network** 에 **203.14.10.0/24** 를 입력하십시오.
    l. **Save** 를 클릭하십시오.

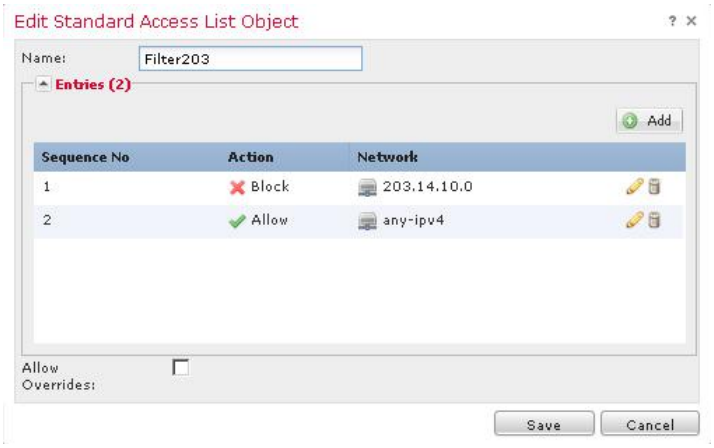
2. 왼쪽 창에서 **Access List > Standard** 을 선택하십시오.

    a. **Add Standard Access List** 를 클릭하십시오.

    b. **Name** 에 **Filter203** 를 입력하십시오

    c. 아래 그림과 같이 2 개의 액세스 컨트롤 항목을 추가하십시오. 두 번째 항목은 매우 중요합니다. 왜냐하면 목록 끝 부분에 암묵적으로 모두 거부가 적용되기 때문입니다.

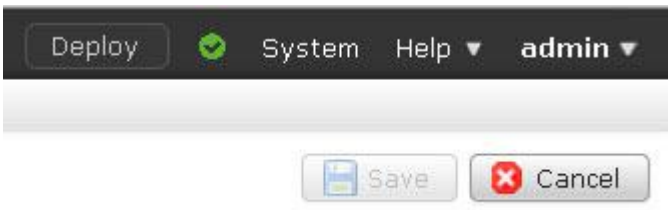
    d. **Save** 를 입력하십시오.



Static NAT 구성

1. **Devices > NAT** 로 이동합니다

2. 연필 모양의 아이콘을 클릭하여 **Default PAT** 정책을 편집합니다. 오른쪽 상단 **Save** 버튼이 회색으로 표시되는지 확인합니다. 그렇지 않은 경우 다른 곳으로 이동했다가 다시 돌아와서 편집 해보십시오. 이는 알려진 버그입니다.



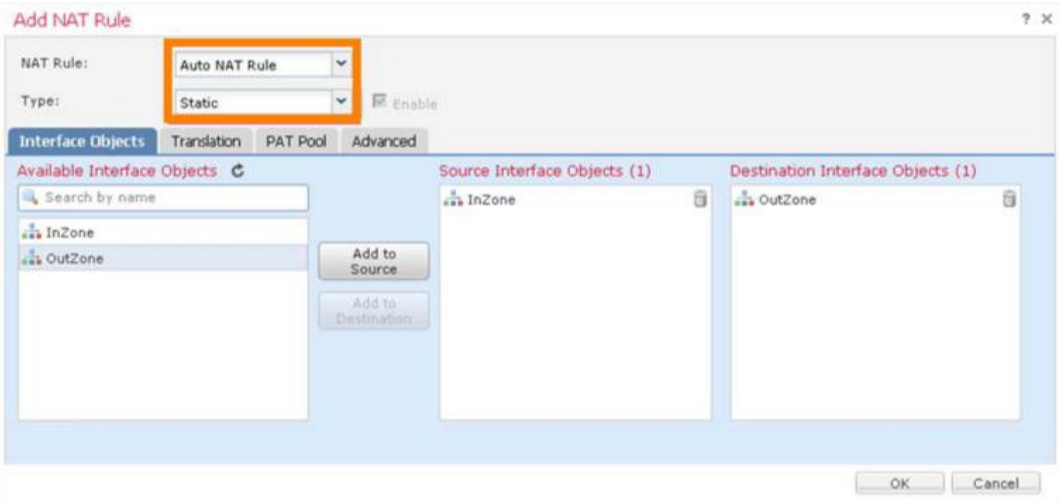
3. **Add Rule** 를 입력하십시오

    a. **Type** 드롭 다운 목록에서 **Auto NAT Rule** 을 선택하십시오

    b. 인터페이스 오브젝트 탭에 있습니다. **InZone** 을 선택하고 **Add to Source** 를 클릭하십시오.

    마이그레이션 시나리오를 수행 한 경우는 두 개의 인터페이스 그룹을 선택할 수 있습니다. 이는 무시하셔도 됩니다.

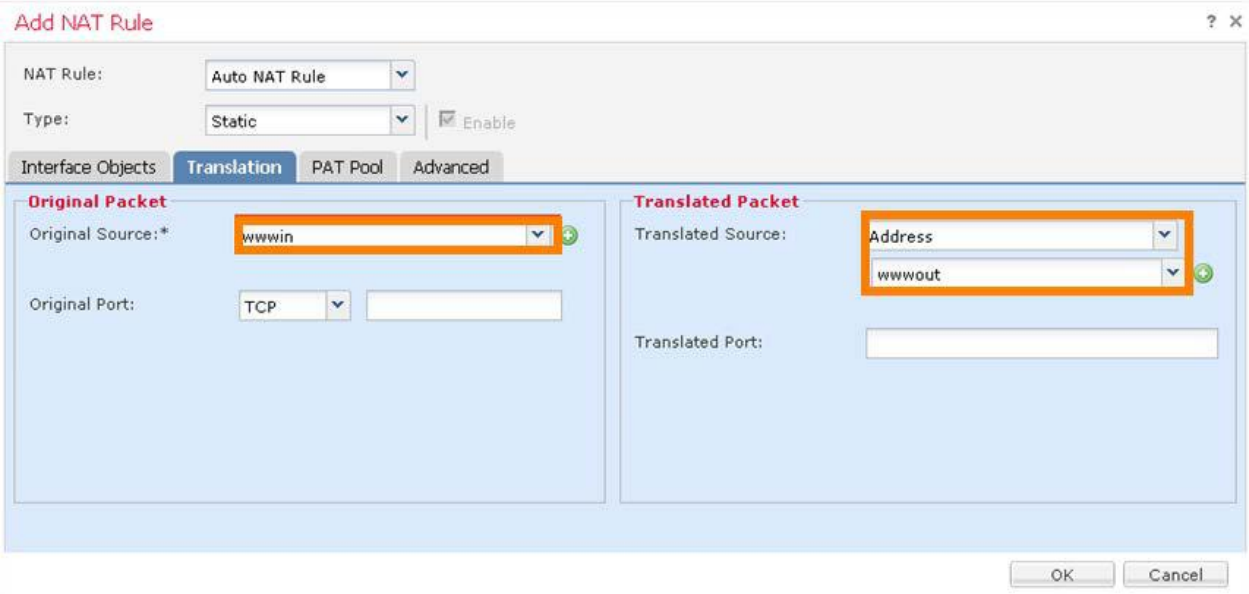
    c. **OutZone** 을 선택하고 **Add to Destination** 를 클릭합니다.



d. **Translation** 탭을 선택하십시오.

e. **Original Source** 드롭 다운 목록에서 **wwwin** 을 선택하십시오.

f. **Translated Source** 드롭 다운 목록에서 **wwwout** 및 **Address** 를 선택하십시오.



g. NAT 룰을 저장하기 위해 **OK** 를 클릭하십시오.

4. NAT 정책을 저장하기 위해 **Save** 를 클릭합니다.

액세스 컨트롤 정책을 수정하여 외부 wwwin 에 대한 액세스 허용

1. **Policies > Access Control > Access Control** 로 이동합니다. **NGFW Access Control Policy** 를 편집합니다.

2. Add Rule 를 클릭합니다.

    a. Name 에 **Web Server Access** 를 입력하십시오.
    b. 삽입 드롭 다운 목록에서 **into Default** 를 선택하십시오.
    c. **Zones** 탭이 미리 선택되어져 있어야합니다. **InZone** 을 선택하고 **Add to Destination**. **Zones** 를 클릭하십시오.
    d. **OutZone** 을 선택하고 **Add to Source** 를 클릭하십시오.
    e. **Networks** 탭을 선택하십시오.
    f. **wwwin** 을 선택하고 **Add to Destination** 을 클릭하십시오.

노트: NAT 된 주소 대신 실제 웹 서버의 IP 를 사용합니다.

    g. **Ports** 탭을 선택하십시오.
    h. **HTTP** 과 **HTTPS** 를 선택하고 **Add to Destination** 을 클릭하십시오
    i. **Inspection** 탭을 선택하십시오.
    j. **Intrusion Policy** 드롭 다운 목록에서 **Demo Intrusion Policy** 를 선택하십시오.
    k. **File Policy** 드롭 다운 목록에서 **Demo File Policy** 를 선택하십시오.
    l. **Add** 를 클릭하여 룰을 추가하십시오.

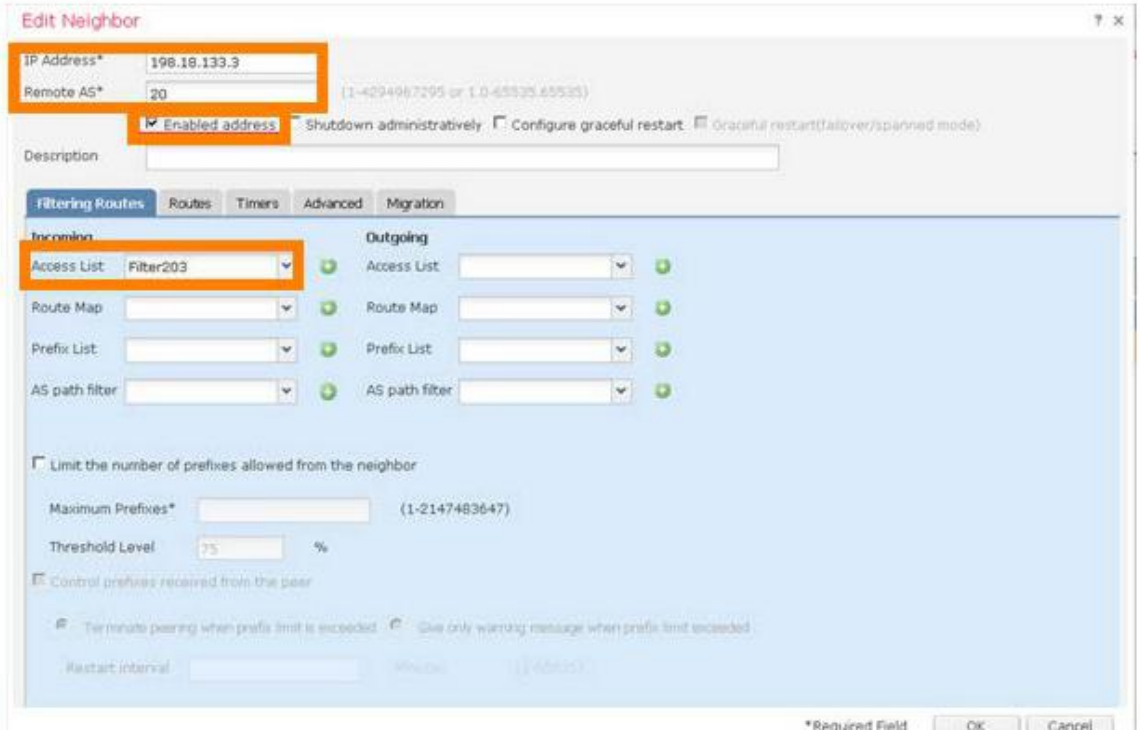
3. **Save** 를 클릭하여 액세스 컨트롤 정책 변경 사항을 저장합니다.

BGP 구성

1. **Devices > Device Management** 로 이동합니다.

2. **NGFW** 디바이스 설정을 수정하기 위해 연필 모양 아이콘을 클릭합니다.

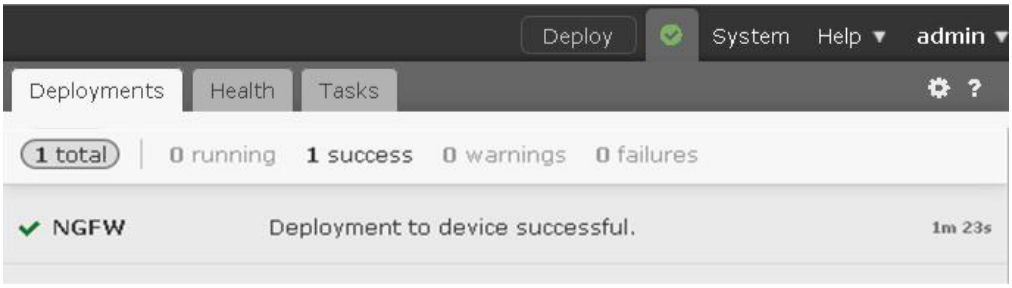
3. **Routing** 탭을 선택하십시오.
    a. **BGP** 를 선택하고 **Enable BGP** 체크 박스에 체크합니다.
    b. **AS Number** 번호를 **10** 으로 설정하십시오
    c. 왼쪽 창에서 **BGP** 를 확장하여 **IPv4** 를 선택하십시오.
    d. **Enable IPv4** 체크 박스를 체크합니다.
    e. **Neighbor** 탭을 클릭하고 **Add** 를 클릭하십시오.
        i. **IP Address** 에 **198.18.133.3** 을 입력하십시오.
        ii. **Remote AS** 로 **20** 을 입력하십시오
        iii. **Enable address** 확인란을 체크합니다.
        iv. 들어오는 접속 리스트 드롭 다운 목록에서 **Filter203** 을 선택하십시오.
        v. **OK** 을 클릭하여 네이버를 추가하십시오.



f. **Save** 를 클릭하여 BGP 구성을 저장하십시오.

변경 사항 적용 및 구성 테스트

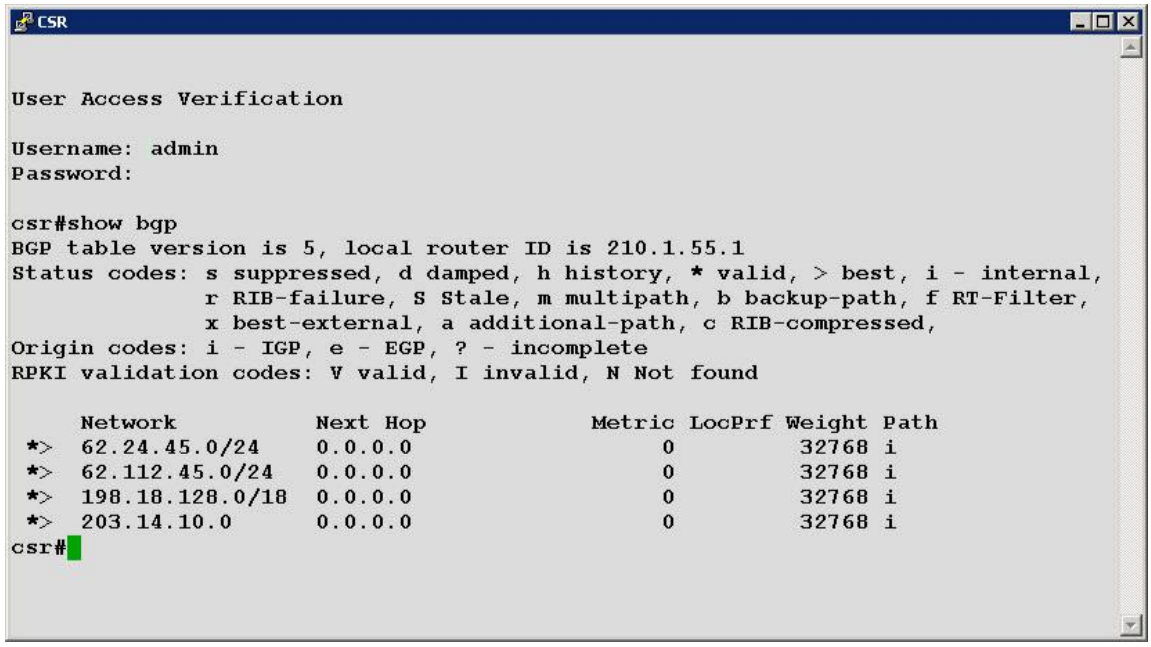
1. 변경 사항을 적용하고 구성 완료까지 기다립니다.



2. Jump 데스크탑에서 PuTTY 를 여십시오. 사전에 구성된 **Outside Linux Server** 이라는 세션을 더블 클릭하십시오. 계정은 **root**, 패스워드는 **C1sco12345** 입니다.
   a. **curl wwwout** 을 입력하십시오. 이것은 성공해야합니다.
   b. **ssh wwwout** 을 입력하십시오. 이것은 실패해야합니다.

3. Jump 데스크탑에서 PuTTY 를 여십시오. 사전에 구성된 **CSR** 이라는 세션을 더블 클릭하십시오. 계정은 **admin**, 패스워드는 **C1sco12345 입니다.**

4. CSR CLI 에서 **show bgp** 명령을 실행하고 4 개의 경로가 나타나는지 확인합니다.



5. NGFW CLI 에서 다음을 수행하십시오.

   a. **show route** 를 실행합니다. BGP 가 학습한 유일한 경로가 62.24.45.0/24 및 62.112.24.0/24 인지 확인합니다. 203.14.10.0/24 가 BGP 에서 성공적으로 필터링되었습니다. 만약 FlexConfig 시나리오를 수행하였다면 이 경로는 외부 EIGRP 경로로 표시됩니다.

   b. **show bgp** 및 **show bgp rib-failure** 를 실행합니다. 198.18.128.0/18 경로는 더 나은 경로(직접 연결됨)가 있기 때문에 경로 테이블에 따로 반영되지 않았음을 보여줍니다.

노트: FMC 에서 아래 명령을 실행할 수도 있습니다.

1. **Device > Device Management** 로 이동합니다.

2. **NGFW** 장치를 편집하고 **Devices** 탭을 선택합니다.

3. **Health** 섹션에서 **Status** 오른쪽에 있는 아이콘을 클릭하십시오.

4. **Advanced Troubleshooting** 을 클릭합니다

4. **Threat Defense CLI** 탭을 선택하십시오.

여기에서 여러 종류의 NGFW CLI 명령어를 실행할 수 있습니다.

6. Inside Linux 서버 세션에서 **ping 62.24.45.1** 을 실행합니다. 이는 성공해야합니다.

시나리오 11. Site-to-Site VPN

이 시나리오 연습은 다음 작업으로 구성됩니다.

- 실습에 필요한 오브젝트 만들기
- site-to-site VPN 구성
- NAT exemption 생성
- 액세스 컨트롤 정책을 수정하고 변경 사항을 적용.
- 변경 사항 적용 및 구성 테스트

이 연습의 목적은 NGFW 과 ASA 사이에 site-to-site VPN 터널을 구성하는 것입니다.

스텝

이 실습에 필요한 오브젝트 만들기

1. **Objects > Object Management** 으로 이동합니다. **Network** 오브젝트 페이지가 선택됩니다.
    a. **Add Network > Add Object** 를 클릭하십시오.
    b. **Name** 에 **MainOfficeNetwork** 를 입력하십시오.
    c. **Network** 에 **198.19.10.0/24** 를 입력하십시오
    d. **Save** 를 클릭하십시오
    e. **Add Network > Add Object** 를 클릭하십시오
    f. **Name** 에 **BranchOfficeNetwork** 를 입력하십시오
    g. **Network** 에 **198.19.11.0/24** 를 입력하십시오
    h. **Save** 를 클릭.

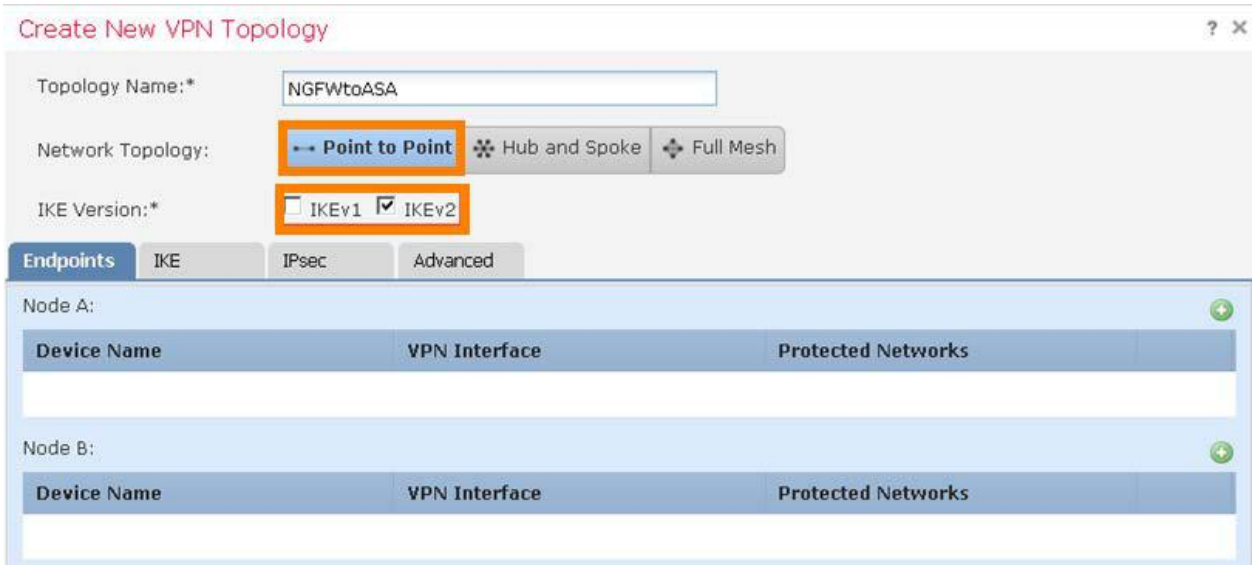
Site-to-Site VPN 구성

1. **Devices > VPN> Site To Site** 로 이동합니다. **Add VPN > Firepower Threat Defense Device** 를 클릭하십시오.

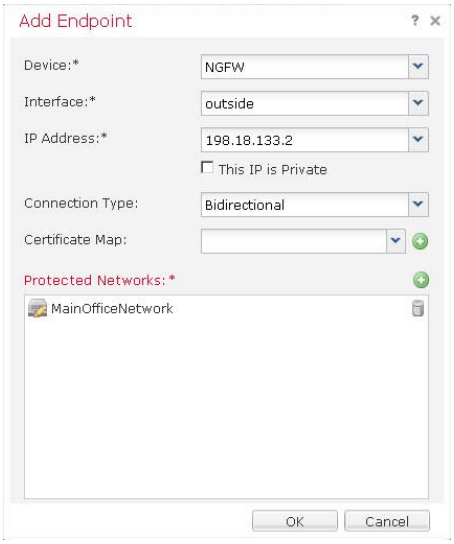
노트: 다른 VPN 옵션인 Firepower Device 는 Firepower 장치간 보안 터널을 구성하기 위한 것입니다.

2. **Name** 에 **NGFWtoASA** 를 입력하십시오.

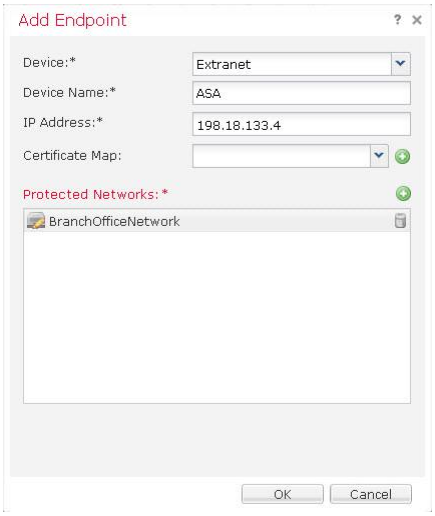
3. 네트워크 토폴로지가 Point to Point 로 선택되어 있는지 확인합니다. IKE 버전의 경우 IKEv1 가 아닌 IKEv2 가 선택되어 있는지 확인합니다.



4. **Node A** 오른쪽에 있는 녹색의 + 기호를 클릭하십시오. 아래 그림과 같이 입력 한 다음 **OK** 를 클릭합니다.



5. **Node B** 오른쪽에 있는 녹색의 + 기호를 클릭하십시오. 아래 그림과 같이 입력 한 다음 **OK** 를 클릭합니다.



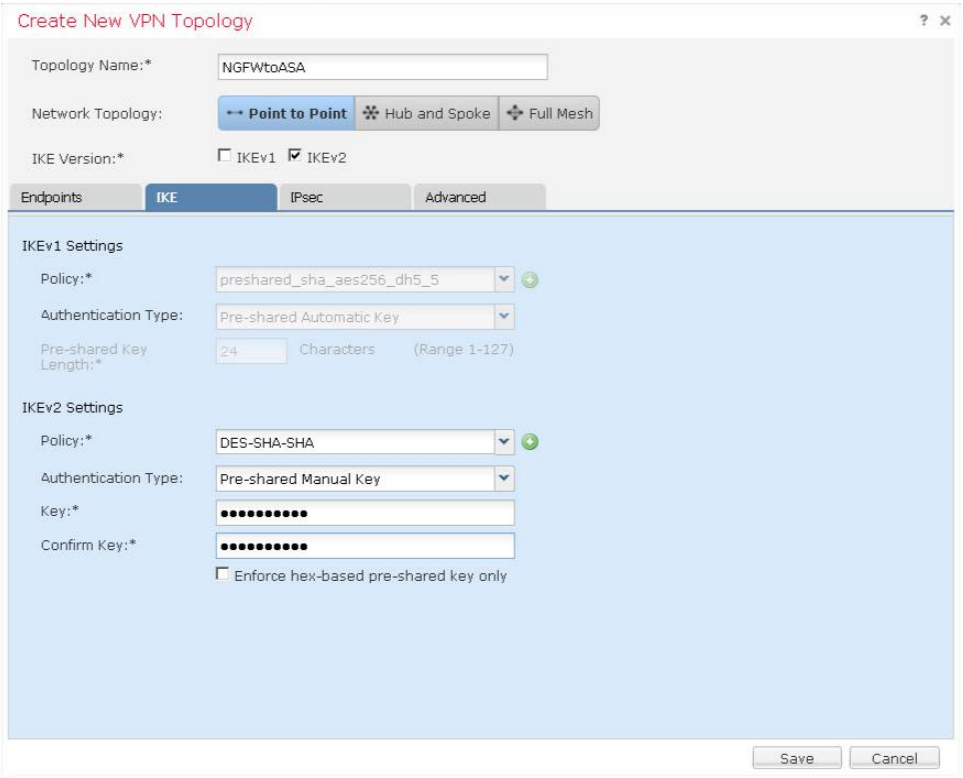
6. **IKE** 탭을 선택하십시오.

   a. **IKEv2** 설정에서 Policy 에 **DES-SHA-SHA** 를 선택합니다.

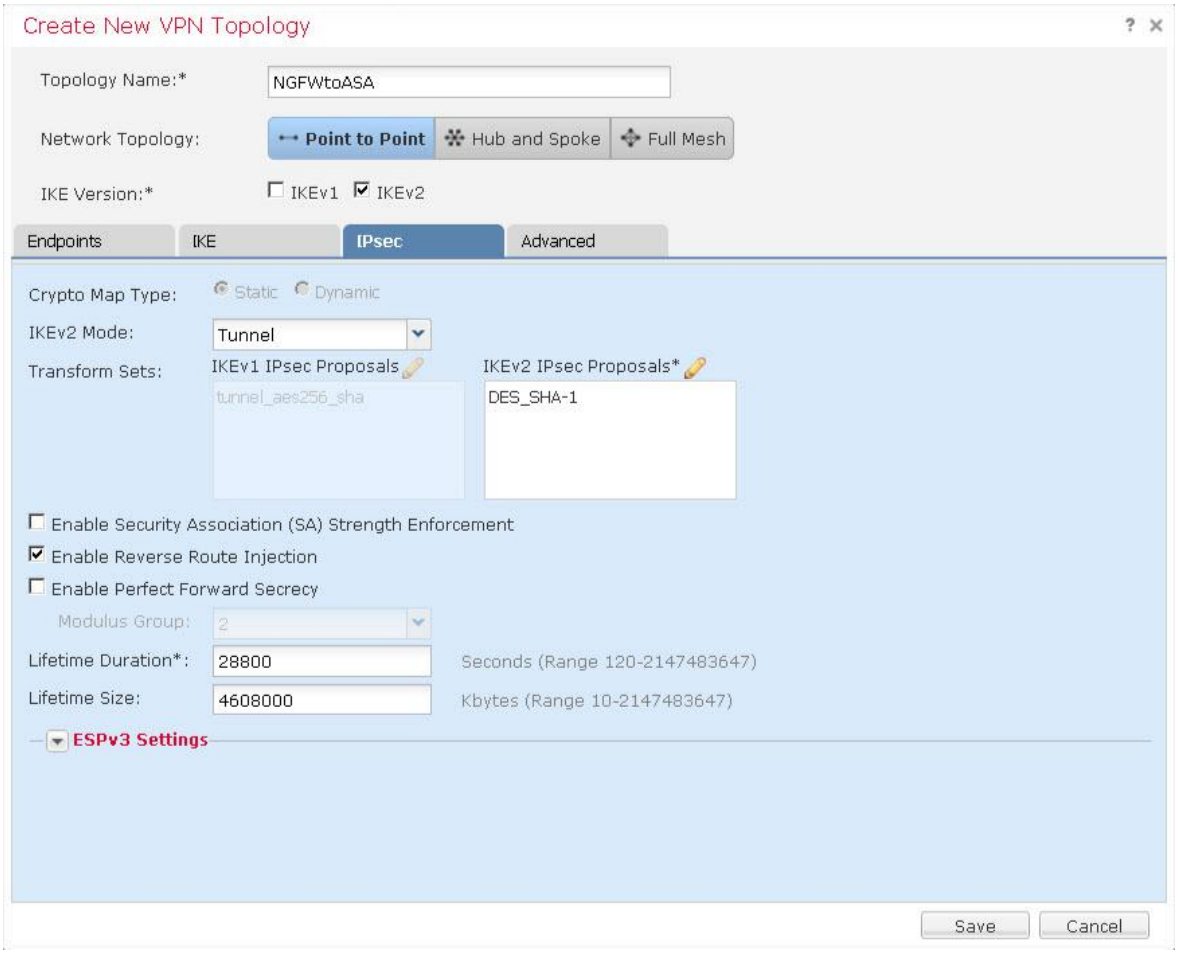
   b. IKEv2 Settings 에서 **Authentication Type** 에 **Pre-shared Manual Key** 를 선택합니다.

노트: FMC 가 양쪽 엔드 포인트를 관리하는 경우에만 자동 설정을 사용할 수 있습니다. 이 경우에는 FMC 가 임의의 공유 키를 생성 할 수 있습니다.

   c. **IKEv2** 설정에서 **Key** 에 **C1sco12345** 를 입력합니다.



7. **IPsec** 탭을 선택하고 **IKEv2 IPsec Proposal** 을 **DES_SHA-1** 로 변경합니다.



8. **Save** 를 클릭하여 VPN 설정을 저장합니다.

NAT exemption 생성

1. **Devices > NAT** 로 이동합니다.

2. **Default PAT** 정책을 편집하기 위해 연필 모양의 아이콘을 클릭합니다.

3. **Add Rule** 을 클릭합니다.
    a. 선택된 **NAT Rule** 드롭 다운 목록에서 **In Category** 및 **NAT Rules Before** 를 그대로 둡니다.
    b. 인터페이스 오브젝트 탭에 있습니다
        i. **InZone** 을 선택하고 **Add to Source** 를 클릭하십시오
        ii. **OutZone** 을 선택하고 **Add to Destination** 를 클릭하십시오.

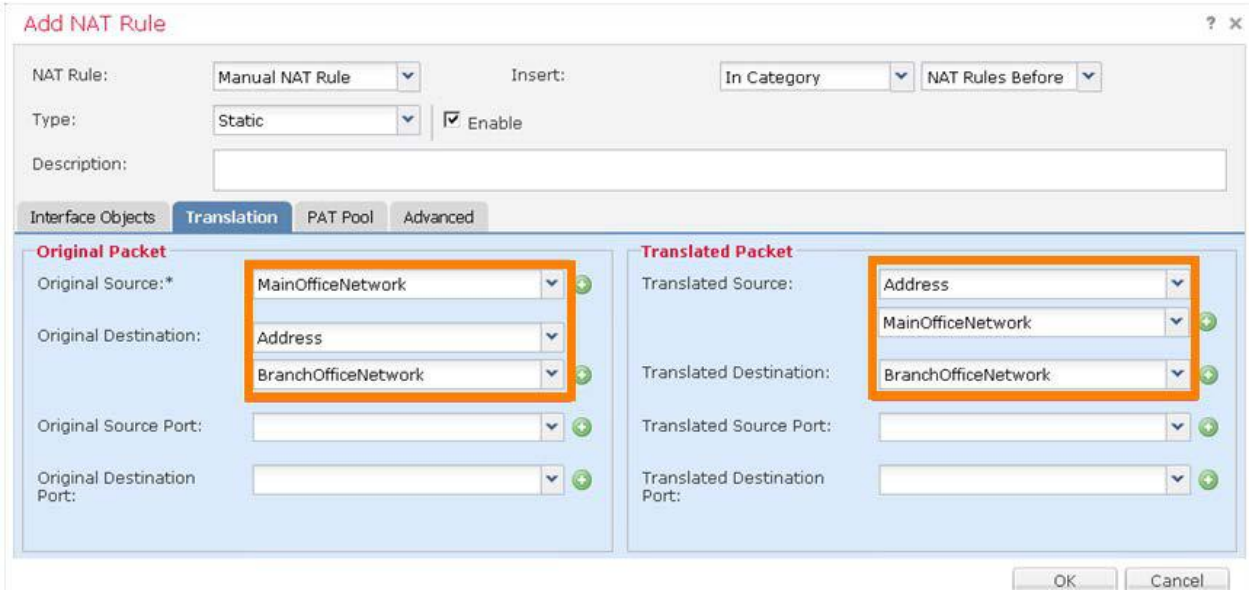
c. Translation 탭을 선택하십시오

i. **Original Source** 드롭 다운 목록에서 **MainOfficeNetwork** 를 선택하십시오

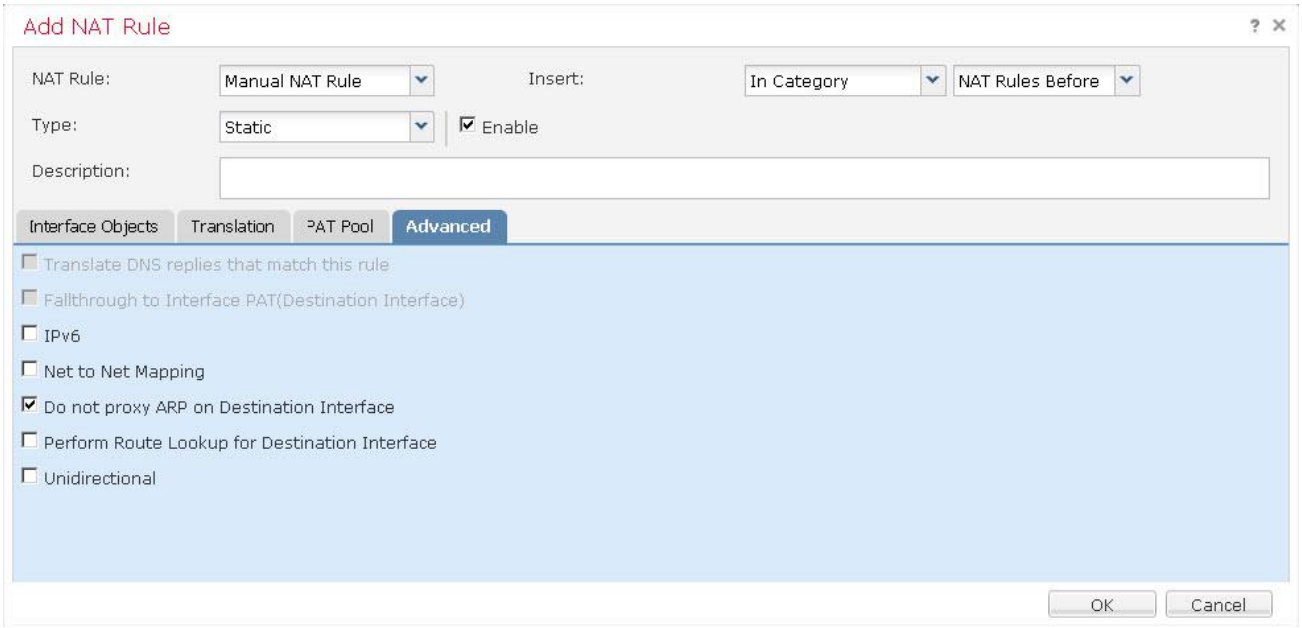
ii. **Translated Source** 드롭 다운 목록에서 **MainOfficeNetwork** 를 선택하십시오

iii. **Original Destination** 드롭 다운 목록에서 **BranchOfficeNetwork** 를 선택합니다.

iv. **Translated Destination** 드롭 다운 목록에서 **BranchOfficeNetwork** 를 선택하십시오



d. Advanced 탭을 선택하고 **Do not proxy ARP on Destination Interface** 를 체크합니다.



e. **OK** 를 클릭하여 NAT 룰을 저장합니다.

4. **Save** 를 클릭하여 NAT 정책을 저장합니다.

액세스 컨트롤 정책을 수정하고 변경 사항의 적용

이제 지사와 본사간의 트래픽 허용을 위한 룰을 생성합니다.

1. **Policies > Access Control > Access Control** 로 이동하십시오. NGFW 액세스 컨트롤 정책을 편집합니다.

2. **Add Rule** 을 클릭합니다
    a. 룰은 **VPN Access** 로 합니다.
    b. **Insert** 드롭 다운 목록에서 **into Default** 를 선택하십시오. 이는 액세스 컨트롤 정책의 마지막 룰입니다.
    c. 액션은 **Allow** 로 둡니다.
    d. **Zones** 탭이 이미 선택되어져 있어야합니다.
    e. **OutZone** 을 선택하고 **Add to Source** 를 클릭하십시오.
    f. **InZone** 을 선택하고 **Add to Destination** 을 클릭하십시오.
    g. **Networks** 탭을 선택하고 **BranchOfficeNetwork** 를 선택한 다음 **Add to Source** 를 클릭합니다
    h. **Networks** 탭을 선택하고 **MainOfficeNetwork** 를 선택한 다음 **Add to Destination** 을 클릭합니다
    i. **Inspection** 탭을 선택하십시오.
        i. **Intrusion Policy** 드롭 다운 목록에서 **Demo Intrusion Policy** 를 선택하십시오
        ii. **File Policy** 드롭 다운 목록에서 **Demo File Policy** 를 선택하십시오
    j. **Add** 를 클릭하여 이 룰을 액세스 컨트롤 정책에 추가하십시오.

3. **Save** 를 클릭하여 액세스 컨트롤 정책을 저장하십시오.

변경 사항의 적용 및 구성 테스트

1. 변경 사항을 적용하고 적용이 완료될 때까지 기다립니다.

2. NGFW CLI 에서 **show crypto ipsec sa** 를 입력합니다. IPSec 을 위한 Security association 은 없어야 합니다.

3. Inside Linux 서버 CLI 에서 **ping branch** 를 입력하십시오. 몇 초 뒤 ping 이 성공해야합니다.

4. NGFW CLI 에서 **show crypto ipsec sa** 를 입력합니다. 이제 IPSec 의 Security association 이 있어야 합니다.

5. Jump 데스크탑에서 PuTTY 를 여십시오. 미리 만들어진 **Branch Linux Server** 를 더블 클릭하십시오.
    a. 계정은 **root**, 패스워드는 **C1sco12345** 로 로그인합니다..
    b. **curl inside** 을 입력하십시오. 이것은 성공해야합니다.

시나리오 12. Web Proxy 통합

이 시나리오 연습은 다음 작업으로 구성됩니다.

- WSA 설정을 수정
- XFF 타입 헤더 사용을 구성
- 액세스 컨트롤 정책 적용
- 변경 사항 적용 및 구성 테스트

NGFW 는 XFF 타입의 헤더를 사용하여 프록시 서버 대신 실제 클라이언트에 대해 정책을 시행할 수 있습니다. 이 섹션은 여러분이 True-Client-IP 기능을 익힐 수 있도록 하는 것 입니다. 이 기능을 이용하여 NGFW 은 웹 프록시를 통과해 엔드 포인트에게 정책을 시행 할 수 있도록 합니다.

구성한 규칙이 다소 인위적이지만 이를 이용하여 테스트를 손쉽게 진행할 수 있습니다.

스텝

WSA 구성을 수정

1. Jump 데스크탑에서 PuTTY 를 여십시오. **WSA** 라는 사전에 구성된 세션을 더블 클릭합니다. 계정은 **admin**, 패스워드는 **C1sco12345** 로 로그인하십시오.

2. WSA CLI 에서 다음 명령을 수행하십시오

```
wsa.dcloud.local> setgateway
Warning: setting an incorrect default gateway may cause the current connection to be
interrupted when the changes are committed.
Set the default gateway for:
1. IPv4
2. IPv6
[1]> 1

Enter new default gateway:
[198.19.10.11]> 198.19.10.1

wsa.dcloud.local> commit

Please enter some comments describing your changes:
[]> Changing gateway

Changes committed: Mon Oct 02 00:01:11 2017 GMT
wsa.dcloud.local>
```

3. WSA 가 X-Forwarded-For 헤더를 생성하도록 구성되었는지 확인합니다. 이는 원래 기본값이 아닙니다.
    a. Firefox 브라우저에서 새 탭을 엽니다
    b. **WSA 북마크**를 클릭하십시오. 계정명은 **admin**, 패스워드는 **C1sco12345** 로 로그인하십시오. (이 자격 증명은 미리 입력되어 있습니다)
    c. WSA UI 에서 Security Services > Web Proxy 로 이동합니다.
    d. **Advanced Settings** 에서 **Generate Headers** 의 경우 **X_Forwarded-For** 헤더가 전송되고 있는지 확인합니다.

XFF 타입의 헤더 사용을 구성

1. FMC 탭에서 **Policies > Access Control > Access Control** 로 이동합니다. NGFW 액세스 컨트롤 정책을 편집합니다.
2. **Add Rule** 를 클릭하십시오.
    a. **룰명을 Test XFF Feature** 로 합니다.
    b. 액션을 **Block with reset** 로 설정하십시오.
    c. 삽입 드롭 다운 목록에서 **into Mandatory** 를 선택하십시오.
    d. **Zones** 탭에서 **InZone** 을 선택하고 **Add to Source** 를 클릭합니다.
    e. **Zones** 탭에서 **OutZone** 을 선택하고 **Add to Destination** 을 클릭합니다.
    f. **Networks** 탭을 선택하십시오.
        i. **Source Networks** 영역에서 **Source** 하위 탭을 선택하십시오. 페이지 하단에 **198.19.10.101** 을 입력하고 **Add** 를 클릭하십시오. 이것은 WSA 프록시 서버의 IP 주소입니다.
        ii. **Source Networks** 영역에서 **Original Client** 하위 탭을 선택합니다. 페이지 하단에 **198.19.10.201** 을 입력하고 **Add** 를 클릭하십시오.
        iii. **Destination Networks** 부분의 페이지 하단에 **198.18.133.201** 을 입력하고 **Add** 를 클릭하십시오.
    g. **Loggig** 탭을 선택하십시오. **Log at Beginning of Connection** 에 체크합니다.
    h. **Add** 를 눌러 정책에 룰을 추가합니다.
    i. **Save** 를 클릭하여 정책 변경 사항을 저장하십시오.

변경 사항을 적용 및 구성 테스트

1. 변경 사항을 적용하고 완료되기까지 기다립니다.

2. Inside Linux 서버의 PuTTY 세션으로 돌아갑니다. 다음 명령을 실행하여 구성을 테스트합니다.

   a. 단일 라인 명령을 실행합니다:
   `wget --bind-address=198.19.10.201 -e use_proxy=yes -e http_proxy=198.19.10.101 198.18.133.201`

   403 (forbidden) 응답 코드를 받아야합니다.

   b. 단일 라인 명령을 실행합니다:
   `wget --bind-address=198.19.10.200 -e use_proxy=yes -e http_proxy=198.19.10.101 198.18.133.201`

   성공해야합니다.

노트: WSA 에 파일이 캐싱되었기 때문에 2a 단계를 반복하면 파일이 다운로드됩니다. 프로덕션 환경에서 이를 막기 위해서는 클라이언트와 WSA 사이에 NGFW 를 구성해야합니다. 테스트를 위해 WSA CLI 에서 **diagnostic**, **PROXY**, **CACHE** 를 입력하여 WSA Proxy 캐시를 지울 수 있습니다.

---

3. FMC 에서 **Analysis > Connections > Event**s 로 이동합니다.

   a. **Table View of Connection Event**s 를 클릭하십시오.

   b. **Original Client IP** 열(Column)은 기본값으로 표시되지 않습니다. 이것을 추가 합니다.

   c. **Original Client IP** 추가하려면 다음 단계를 수행하십시오.

      i. 사용되지 않는 열(Column)의 맨 위에 있는 **X** 를 클릭하십시오.

      ii. 열(Column) 선택기를 아래로 스크롤하여 **Disabled Columns** 로 변경하십시오.

      iii. **Original Client IP 에** 체크합니다.

      iv. 열(Column) 선택기를 맨 아래로 스크롤하여 **Apply** 을 클릭하십시오.

   d. WSA IP (198.19.10.101)와 클라이언트 IP (198.19.10.201)가 모두 표시되는지 확인합니다.

시나리오 13. 사전 필터(Prefilter) 정책

이 시나리오 연습은 다음 작업으로 구성됩니다.

- 터널링된 트래픽에 대한 NGFW 기본 동작 확인
- 터널 zone 을 생성
- 사전 필터 정책을 생성
- 액세스 컨트롤 정책을 수정
- 변경 사항 적용 및 구성 테스트

사전 필터 정책에는 2 가지 유형의 룰 (사전 필터 및 터널)이 있습니다. 사전 필터 룰이 일반적으로 사용되며 이 룰을 통해 Lina 의 데이터 플레인에서 어떤 트래픽을 드롭해야 하는지, Snort 를 우회해야 하는지, 어떤 트래픽을 Snort 로 보내야 하는지를 지정합니다. 이는 성능 향상에 도움이 될 수 있습니다. 이 시나리오 뒷 부분에서 사전 필터 룰도 다루긴 하지만 일단 이 시나리오는 기본적으로 터널 룰에 초점을 맞추고 있습니다.

암호화 되지 않은 일반 텍스트 터널의 경우 액세스 컨트롤 정책은 **터널링되는** 트래픽에 적용됩니다. 사전 필터 정책은 **터널링** 프로토콜에 대한 컨트롤 기능을 제공합니다. 지원되는 터널링 프로토콜은 다음과 같습니다.

- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo

사전 필터 정책은 터널 태그를 통해 액세스 컨트롤 정책과 통신합니다. 사전 필터 정책은 특정 터널에 터널링 태그를 할당합니다. 그러면 액세스 컨트롤 정책은 특정 터널을 통과하는 터널링 트래픽에만 적용되는 규칙을 포함시킬 수 있습니다.

이 시나리오에서는 CentOS 서버의 내부와 외부 사이에 GRE 터널을 생성합니다.

그 다음 GRE 터널을 통과하는 ICMP 를 차단하도록 NGFW 을 구성합니다.

노트: 이 시나리오를 진행하기 위해선 시나리오 10 이 필요합니다. 왜냐하면 198.19.10.202 를 198.18.128.202 로 변환하는 Static NAT 을 가정하기 때문입니다. 터널 인터페이스 구성을 확인하기 위해 서버의 내부 및 외부에서 **/etc/sysconfig/network-scripts/ifcfg-tun0** 을 검사 할 수 있습니다.

스텝

터널링 트래픽에 대한 NGFW 기본 동작 확인

이 작업에서는 액세스 컨트롤 정책 룰이 터널링 된 트래픽을 적용되는지 확인합니다.

1. 아직 Inside Linux 서버의 SSH 세션이 열려 있어야합니다.

2. Outside Linux 서버에 대한 SSH 세션이 없는 경우는 Jump 데스크탑에서 PuTTY 를 실행하고 사전에 정의된 **Outside Linux Server** 세션을 더블 클릭하십시오. 계정명은 **root**, 패스워드는 **C1sco12345** 입니다.

3. Inside Linux 서버와 Outside Linux 서버 사이에 GRE 터널을 만듭니다.
    a. Outside Linux Server CLI 에서 type **ifup tun0** 을 입력하십시오.
    b. Inside Linux Server CLI 에서 type **ifup tun0** 을 입력하십시오.
    c. Inside Linux Server 에서 다음 명령어를 이용하여 터널을 통해 ping 이 동작 하는지 확인하십시오

    ping 10.3.0.2

4. IPS 기능을 테스트합니다.
    a. Inside Linux 서버의 CLI 에서 다음 명령을 실행하십시오.

    ftp 10.3.0.2
    b. 계정명은 **guest**, 패스워드는 **C1sco12345** 로 로그인합니다.
    c. **cd ~root** 를 입력하십시오. 다음 메시지가 표시됩니다.

    421 Service not available, remote server has closed connection
    d. FTP 를 종료하려면 **quit** 를 입력하십시오.

5. FMC 에서 **Analysis > Intrusions > Events** 로 이동합니다.
    a. 이벤트 테이블을 자세히 보려면 왼쪽의 화살표를 클릭하십시오
    b. 소스 및 대상 IP 는 각각 10.3.0.1 및 10.3.0.2 입니다.

6. Inside Linux 서버 CLI 에서 다음 명령을 실행하여 파일 및 멀웨어 차단 기능을 테스트합니다.

노트: 아래의 Wget 명령어는 Jumps 데스크탑에 있는 Strings to cut and paste.txt 파일에서 복사 붙여넣기 할 수 있습니다.

    a. 컨트롤 테스트로 WGET 을 사용하여 차단되지 않은 파일을
    다운로드하십시오. 아래 명령은 성공해야 합니다.
    wget -t 1 10.3.0.2/files/ProjectX.pdf
    b. 그런 다음 WGET 을 사용하여 유형별로 차단된 파일을
    다운로드하십시오.
    wget -t 1 10.3.0.2/files/test3.avi

    일부 파일이 다운로드 됩니다. NGFW 가 첫 번째 데이터 블록을 보고 파일 유형을 감지 할 수 있기 때문입니다.
    c. 마지막으로 WGET 을 사용하여 악성 코드를
    다운로드하십시오.
    wget -t 1 10.3.0.2/files/Zombies.pdf

    파일의 약 99 %가 다운로드됩니다. 이것은 NGFW 가 SHA 값을 계산하기 위해 전체 파일을 필요로하기 때문입니다.
    NGFW 는 해시가 계산되어 룩업될 때까지 마지막 데이터 블록을 홀드합니다.

7. FMC 에서 **Analysis > Files > File Events** 로 이동합니다.
    a. **Table View of File Events** 를 클릭하십시오.
    b. 송수신 IP 는 각각 **10.3.0.2** 와 **10.3.0.1** 입니다.

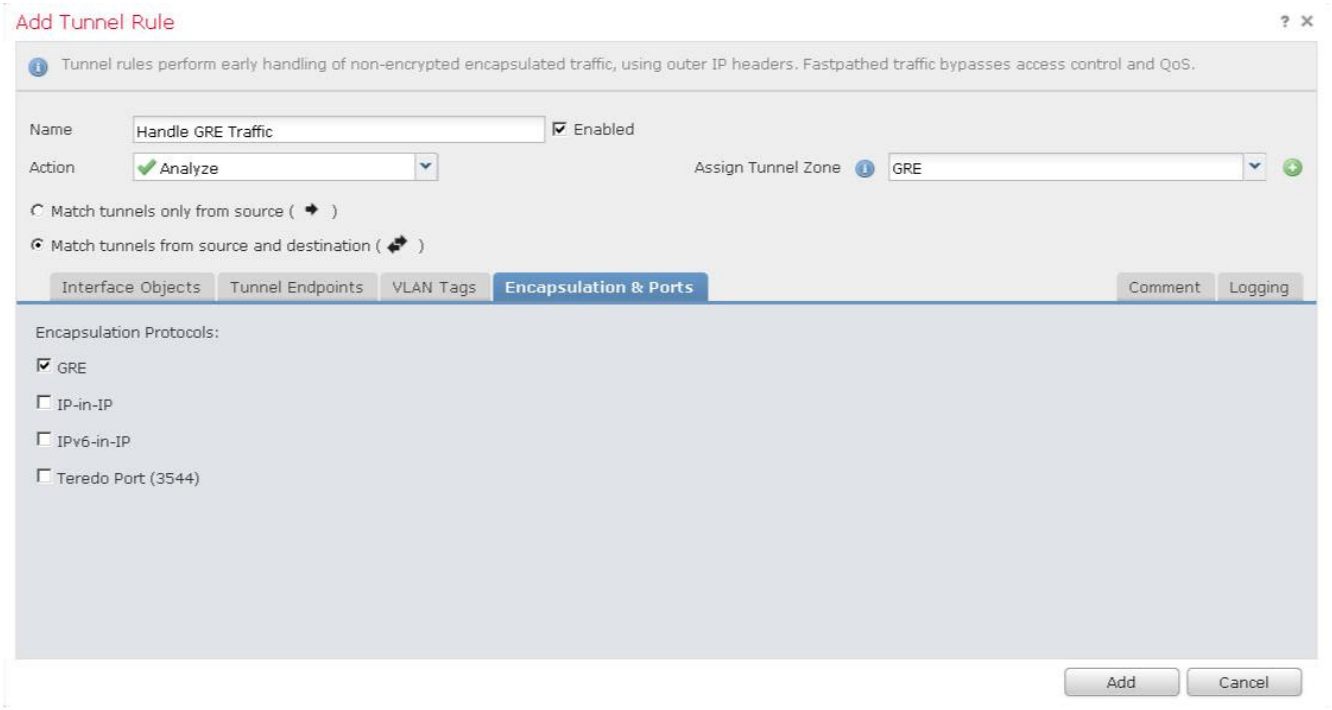
터널 Zone 만들기

1. **Objects > Object Management** 로 이동합니다.
    a. 왼쪽 창에서 **Tunnel Zone** 을 선택하십시오.
    b. **Add Tunnel Zone** 을 클릭하십시오.
    c. **Name** 에 **`GRE`** 를 입력하십시오.
    d. **Save** 를 클릭하십시오.

사전 필터 정책 만들기

1. **Policies > Access Control > Prefilter** 로 이동합니다.
2. **New Policy** 를 클릭하십시오. **`NGFW Prefilter Policy`** 이름을 입력한 다음 **Save** 를 클릭하십시오.
3. 정책 편집창이 열릴 때까지 잠시 기다립니다.
4. **Add Tunnel Rule** 을 클릭하십시오.
    a. **Name** 에 **`Handle GRE Traffic`** 을 입력하십시오.
    b. **Assign Tunnel Zone** 드롭 다운 목록에서 **GRE** 를 선택하십시오.

    Encapsulation & Ports 탭을 선택하고 **GRE** 체크 박스를 체크하십시오.



노트: 세 가지 동작이 있습니다.
• 분석 – 트래픽이 Snort 에 전달되고 액세스 정책 규칙이 적용됩니다.
• 차단 – 트래픽이 차단되었습니다.
• Fastpath – 트래픽이 허용되며 추가 검사는 건너 뜁니다.
이 정책에 대한 사전 필터 룰을 작성할 수 있습니다. 이를 통해 레이어 2 ~ 4 정보를 기반으로 트래픽을 분석, 차단 또는 신속히 처리 할 수 있습니다.

d. **Add** 를 클릭하여 규칙을 추가하십시오.

5. 목적지가 198.18.133.202 인 모든 트래픽에 대해 Snort 를 우회하는 규칙을 추가합니다. 이는 신뢰되는 주소입니다. **Add Prefilter Rule** 를 클릭하십시오.
   a. **Name** 에 **Example of Fastpath** 를 입력하십시오.
   b. **Action** 드롭 다운 목록에서 **Fastpath** 를 선택하십시오.
   c. **Networks** 탭을 선택하십시오
   d. **Destination Network**s 열의 맨 아래에 198.18.133.202 를 입력하십시오.
   e. **Add** 를 클릭하여 대상 네트워크를 추가합니다.

6. **Add** 클릭하여 사전 필터 룰을 추가하십시오.

7. **Save** 을 클릭하여 정책을 저장하십시오.

액세스 컨트롤 정책의 수정

1. **Policies > Access Control > Access Control** 로 이동합니다. NGFW 의 액세스 컨트롤 정책을 편집하십시오.

2. 정책 룰 위의 문자열 **Prefilter Policy** 오른쪽에 있는 **Default Prefilter Policy** 링크를 누릅니다. NGFW 사전 필터 정책을 선택한 다음 **OK** 를 클릭하십시오.

3. **Rules** 탭을 선택하십시오.

4. **Add Rule** 를 클릭하십시오.
   a. **Block ICMP Over GRE** 규칙을 호출하십시오.
   b. **Insert** 드롭 다운 목록에서 **into Mandatory** 를 선택하십시오.
   c. 동작을 **Block with reset** 로 설정하십시오.
   d. **Available Zones** 열에서 **GRE** 를 선택하고 **Add to Source** 를 클릭하십시오
   e. **Applications** 열에서 **ICMP** 를 선택하고 **Add to Rule** 을 클릭하십시오
   f. **Logging** 탭을 선택하십시오. **Log at Beginning of Connection** 체크박스를 선택하십시오.
   g. **Add** 를 클릭하여 정책에 규칙을 추가하십시오.

5. **Add Rule** 를 클릭하십시오.
   a. **Allow GRE Traffic** 이라고 이름을 정합니다.
   b. Insert 드롭 다운 목록에서 **into Default** 를 선택하십시오. 이는 액세스 컨트롤 정책의 마지막 룰로 동작합니다.
   c. **Available Zones** 열에서 **GRE** 를 선택하고 **Add to Source** 를 클릭하십시오.
   d. **Inspection** 탭을 선택하십시오

i. **Intrusion Policy** 드롭 다운 목록에서 **Demo Intrusion Policy** 를 선택하십시오.
ii. **File Policy** 드롭 다운 목록에서 **Demo File Policy** 를 선택하십시오.

e. **Add** 를 클릭하여 룰을 정책에 추가하십시오.

6. **Save** 를 클릭하여 액세스 컨트롤 정책을 저장하십시오.

변경 사항 적용 및 구성 테스트

1. 변경 사항을 적용하십시오. 적용이 완료될 때까지 기다립니다.

2. Outside Linux 서버에서 **tcpdump -n -i tun0** 을 실행하여 터널 트래픽을 모니터링합니다**.**

3. Inside Linux 서버 CLI 에서 다음 명령을 실행하십시오.
   a. **wget 10.3.0.2**
      위 작업은 성공해야합니다.
   b. **ping 10.3.0.2**
      ping 이 차단되고 있음을 나타내는 아래 출력이 나타나야 합니다.
      From 10.3.0.2 icmp_seq=1 Packet filtered

4. Outside Linux 서버에서 `tcpdump` 명령의 출력을 확인하여 10.3.0.2 으로의 Ping 상태를 확인합니다.

5. 터널을 중지시킵니다.
   a. Outside Linux Server CLI 에 `ifdown tun0` 을 입력하십시오.
   b. Inside Linux Server CLI 에 `ifdown tun0` 을 입력하십시오.

6. 이제 사전 필터 룰을 테스트합니다.
   a. **wget -t 1 198.18.133.200/files/Zombies.pdf** 을 입력하십시오.
      차단돼야 합니다**.**
   b. **wget -t 1 198.18.133.202/files/Zombies.pdf** 을 입력하십시오.
      트래픽이 Snort 를 우회하기 허용돼야 합니다.

시나리오 14. Integrate Routing and Bridging (IRB)

이 시나리오의 연습은 다음 작업으로 구성됩니다.

- 실습에 필요한 오브젝트 만들기
- NGFW 인터페이스 구성을 수정
- NAT 정책의 수정
- 액세스 컨트롤 정책의 수정
- 구성 적용 및 테스트

랩에는 GigabitEthernet0 / 2 에 연결되는 별도의 VLAN 에 속한 Linux 서버가 있습니다. 이 서버의 FQDN 은 i**solated.dcloud.local** 이며 IP 주소는 198.19.10.220/24 입니다. 이 주소는 내부 네트워크와 동일한 서브넷에 있습니다.

이 시나리오의 목표는 NGFW 에서 브리지 그룹을 이용하여 이러한 VLAN 에 참여하는 것입니다. 이 VLAN 들 간의 트래픽은 검사됩니다.

노트: 이 연습에서 브리지 그룹에 속해있는 두 인터페이스는 동일한 Security Zone 에 속해있습니다. 그러나 이는 필수는 아닙니다. 브리지 그룹은 서로 다른 Security Zone 에 속한 인터페이스들을 포함할 수 있습니다. 이를 통해 동일 브리지 그룹에 속한 인터페이스 간의 트래픽을 보다 세부적으로 제어할 수 있습니다.

스텝

실습에 필요한 오브젝트 만들기

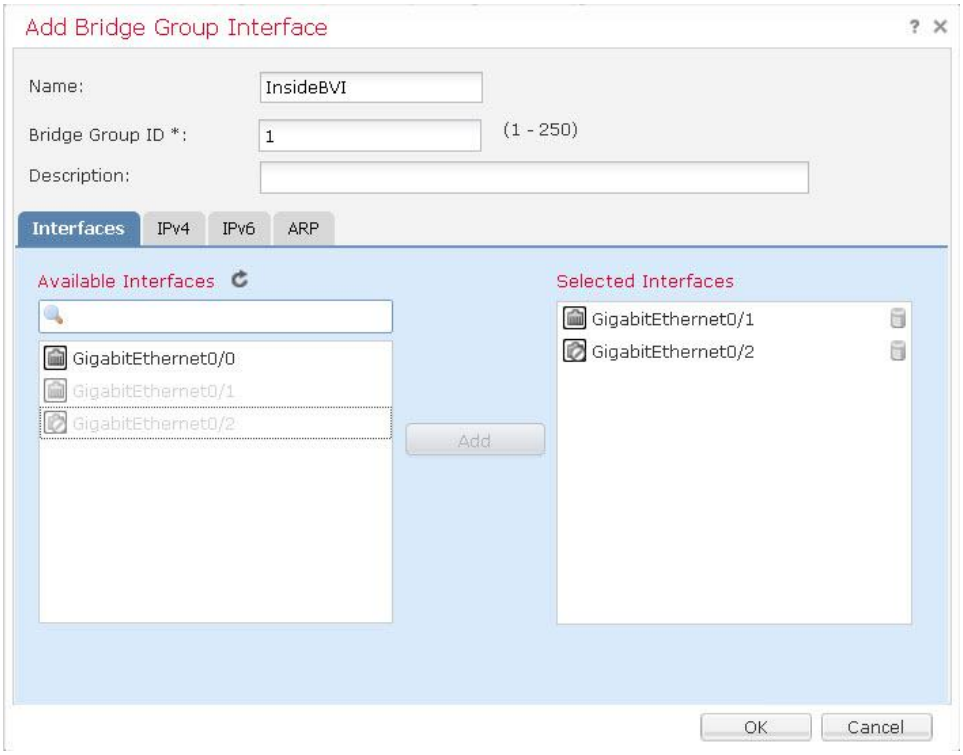
1. **Objects > Object Management** 로 이동합니다. 왼쪽 패널에서 **Interface** 를 선택하십시오.
2. **Add > Security Zone** 을 클릭합니다.
    a. Name 에 **BVIZone** 을 입력하십시오.
    b. **Interface Type** 드롭 다운 메뉴에서 **Switched** 를 선택하십시오
    c. **Save** 를 클릭하십시오.

NGFW 인터페이스 구성 수정

1. **Devices > Device Management** 로 이동합니다.
2. 연필 모양의 아이콘을 클릭하여 NGFW 장치 구성을 편집하고 **Interfaces** 탭을 선택하십시오.
3. 연필 모양의 아이콘을 클릭하여 **GigabitEthernet0/1** 인터페이스를 편집합니다.
4. **IPv4 address** 를 제거하고 **OK** 를 클릭하십시오. IP 는 삭제하여 다른 인터페이스에서 사용할 수 있도록 합니다.
5. **Add Interfaces** 를 선택하고 **Bridge Group Interface** 를 선택합니다.
    a. **Name** 에 **InsideBVI** 를 입력하십시오.

b. Bridge Group ID 에 **1** 을 입력하십시오.

c. **GigabitEthernet0/1** 및 **GigabitEthernet0/2** 를 선택하고 **Add** 를 클릭하십시오.



d. IPv4 탭을 선택하고 IP 주소 **198.19.10.1/24** 를 입력하십시오.

e. **OK** 를 클릭하십시오. 확인 메시지 창이 나타나면 메시지를 읽고 **Yes** 를 클릭하십시오.

6. 연필 모양의 아이콘을 클릭하여 **GigabitEthernet0/1** 인터페이스를 편집하십시오.

a. **Name** 에 **inside1** 를 입력하십시오

b. **Enabled** 체크박스가 체크되어 있는지 확인하십시오

c. **Security Zone** 드롭 다운 목록에서 **BVIZone** 을 선택하십시오.

d. **OK** 를 클릭합니다.

7. 연필 모양의 아이콘을 클릭하여 **GigabitEthernet0/2 interface** 를 편집하십시오.
    a. **Name** 에 **inside2** 를 입력하십시오.
    b. **Enabled** 체크 박스에 체크하십시오.
    c. **Security Zone** 드롭 다운 목록에서 **BVIZone** 을 선택하십시오.
    d. **OK** 를 클릭하십시오.
8. **Save** 를 클릭하여 구성을 저장합니다.

NAT 정책 수정

1. 시나리오 10 을 진행하였으며 Static NAT 룰이 BVI 인터페이스와 함께 작동하게 하려면 이 단계를 포함해야 합니다. 이는 오브젝트 NAT 가 둘 이상의 인터페이스에 대한 인터페이스 오브젝트를 허용하지 않기 때문입니다.
    a. **Objects > Object Management** 로 이동합니다. 왼쪽 패널에서 **Interface** 를 선택하십시오
    b. **Add > Interface Group** 을 클릭하십시오.
        i. **NAME** 에 **InGroup1** 을 입력하십시오
        ii. **Interface Type** 에 **Switched** 를 선택하십시오.
        iii. 인터페이스 **inside1** 선택하고 **Add** 를 클릭하십시오**.**
        iv. **Save** 를 클릭하십시오**.**
2. **Devices > NAT** 로 이동합니다.
3. **Default PAT** 정책을 편집하십시오. 오른쪽 상단에 **Save** 버튼이 회색으로 표시되는지 확인합니다. 그렇지 않은 경우에는 다른 곳으로 이동한 뒤 돌아와 다시 편집 해보십시오.

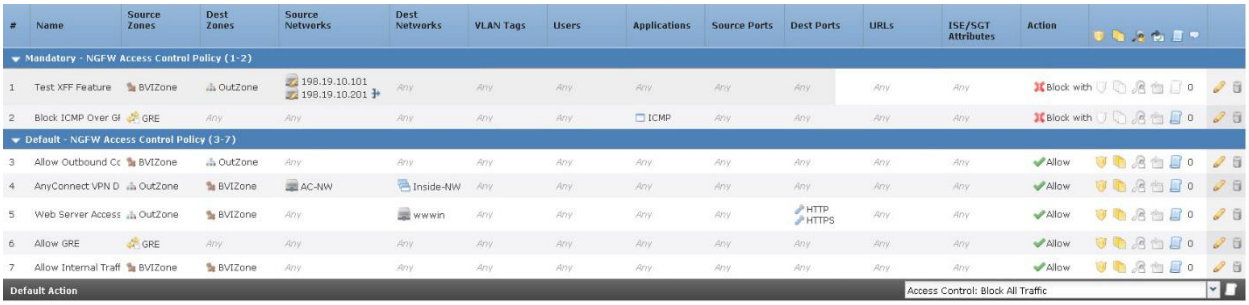
    a. 시나리오 10 에서 Static NAT 구성을 수행한 경우에는 auto NAT 룰에서 **InZone** 을 **InGroup1** 로 바꿉니다. auto NAT 는 둘 이상의 인터페이스가 포함된 Security Zone 을 허용하지 않으므로 **BVIZone** 을 사용할 수 없습니다. 해결 방법은 인터페이스 그룹을 만드는 것입니다.
    b. 모든 룰에서 **InZone** 을 **BVIZone** 으로 바꿉니다.
    c. NAT 정책은 다음과 같아야합니다. 여러분이 수행한 시나리오에 따라 룰이 많거나 적을 수 있습니다.

#	Direction	Type	Source Interface Obje...	Destination Interface Obje...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
1		Static	BVIZone	OutZone	Inside-NW	AC-NW		Inside-NW	AC-NW		Dns:false, no-proxy-arp
Auto NAT Rules											
#		Static	InGroup1	OutZone	wwwin			wwwout			Dns:false
NAT Rules After											
2		Dyna...	BVIZone	OutZone	any			Interface			Dns:false

    d. **Save** 를 클릭하여 NAT 정책을 저장하십시오

액세스 컨트롤 정책 수정

1. **Policies > Access Control > Access Control** 로 이동하고 액세스 컨트롤 정책을 편집하십시오.
2. NGFW 장치 구성을 편집을 위해 **연필 모양 아이콘**을 클릭하여 **Interfaces tab** 을 선택하십시오.
    a. 모든 룰에서 **InZone** 을 **BVIZone** 으로 바꿉니다.
    b. **BVIZone** 의 인터페이스 간의 트래픽을 허용(하지만 검사)하기 위해 액세스 컨트롤 룰을 추가하십시오.
        i. **Name** 에 **Allow Internal Traffic** 를 입력하십시오.
        ii. **Insert** 드롭 다운 목록에서 *into* **Default rule** 를 선택하십시오.
        iii. **Zones** 탭은 이미 선택되어져 있어야합니다.
        iv. **BVIZone** 을 선택하고 소스에 **Add to Source** 를 클릭하십시오.
        v. **BVIZone** 을 선택하고 **Add to Destination** 을 클릭하십시오.
        vi. **Inspection** 탭을 선택하십시오.
        vii. Intrusion Policy 드롭 다운 목록에서 **Demo Intrusion Policy** 를 선택하십시오.
        viii. File Policy 드롭 다운 목록에서 **Demo File Policy** 를 선택하십시오.
        ix. **Add** 를 클릭하여 룰을 추가하십시오.
    c. 액세스 컨트롤 정책은 다음 그림과 같아야합니다. 앞서 수행한 시나리오에 따라 규칙이 더 많거나 적을 수 있습니다.



    d. **Save** 를 클릭하여 변경 사항을 저장하십시오.

구성 적용 및 테스트

1. 구성 변경 사항을 적용하고 적용이 완료될 때까지 기다립니다.
2. Inside Linux 서버 CLI 에서 **ping isolated** 를 입력하여 연결성을 테스트하십시오. 성공해야합니다.
3. Inside Linux 서버 CLI 에서 IPS 기능을 테스트하십시오.
    a. Inside Linux 서버 CLI 에서 다음 명령을 실행하십시오.
    ftp isolated
    b. 계정은 **guest**, 패스워드는 **C1sco12345** 로 로크인하십시오.
    c. **cd ~root** 를 입력하십시오. 다음 메시지가 표시됩니다.
    421 Service not available, remote server has closed connection

4. Inside Linux 서버 CLI 에서 파일 및 멀웨어 차단 기능을 테스트합니다.

   a. 제어 테스트로 WGET 을 사용하여 차단되지 않은 파일을 다운로드하십시오.

      wget -t 1 isolated/files/ProjectX.pdf

      위 작업은 성공해야합니다.

   b. 그런 다음 WGET 을 사용하여 유형별로 차단 된 파일을 다운로드합니다**.**

      wget -t 1 isolated/files/test3.avi

      약간의 파일만 다운로드됩니다. 이는 NGFW 이 첫 번째 데이터 블록을 보고 파일 유형을 감지 할 수 있기 때문입니다. *Demo File Policy* 가 AVI 파일을 차단하도록 구성되었습니다.

   c. 마지막으로 WGET 을 사용하여 악성 코드를 다운로드하십시오.

      wget -t 1 isolated/files/Zombies.pdf

노트: 파일의 약 99 %가 다운로드됩니다. 이것은 NGFW 가 SHA 를 계산하기 위해 전체 파일을 필요로하기 때문입니다. NGFW 는 해시값이 계산되고 Lookup 될 때까지 마지막 데이터 블록을 홀드합니다. *데모 파일 정책*은 PDF 파일에서 탐지된 멀웨어를 차단하도록 구성되었습니다.

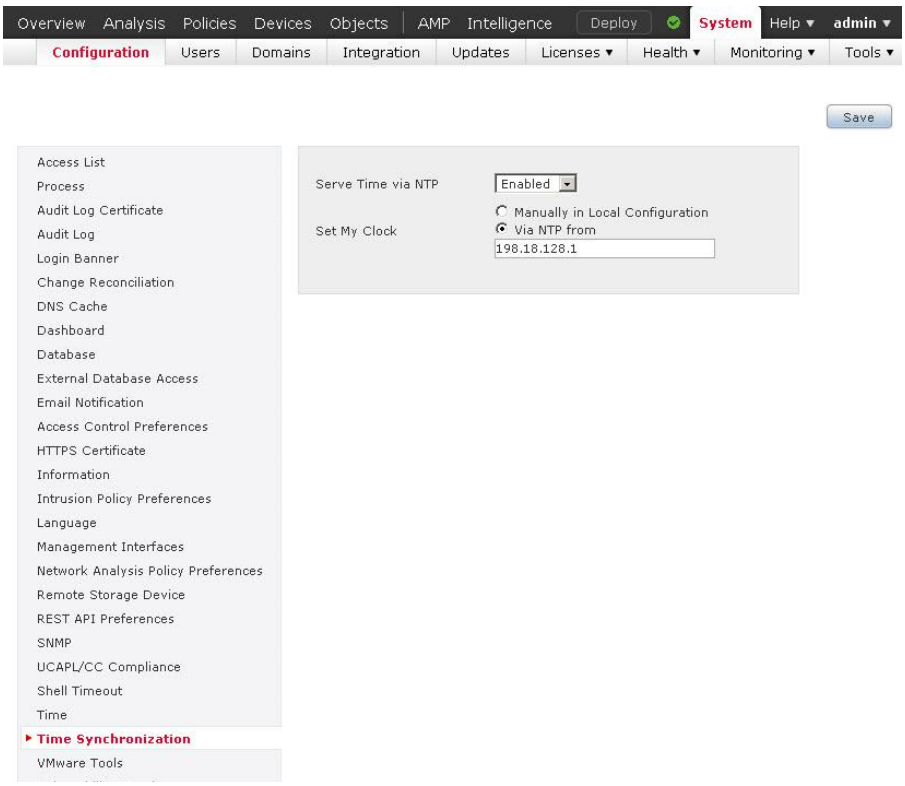
부록 A. FMC 사전 구성

초기 설치 후, 신속한 랩 진행을 위해 FMC 에서 몇 가지 구성 단계가 수행되었습니다. 이 구성 단계는이 부록에서 자세히 설명합니다.

- 구성 A1,1 : NTP 설정
- 구성 A1,2 : 데모 파일 정책
- 구성 A1,3 : 데모 침입 정책
- 구성 A1, 4 : 데모 SSL 정책
- 구성 A1,5 : 사용자 지정 검색 목록
- 구성 A1,6 : resetapiuser 추가.
- 구성 A1,7 : 서버 인증서 설치

구성 A1,1 : NTP 설정

1. FMC 에서 NTP 설정을 구성하십시오.
    a. FMC 에서 **System > Configuration** 으로 이동하십시오.
    b. 왼쪽 창에서 **Time Synchronization** 을 선택하십시오.
    c. 기본 NTP 서버를 **198.18.128.1** 로 바꿉니다.
    d. Save 를 클릭하십시오.

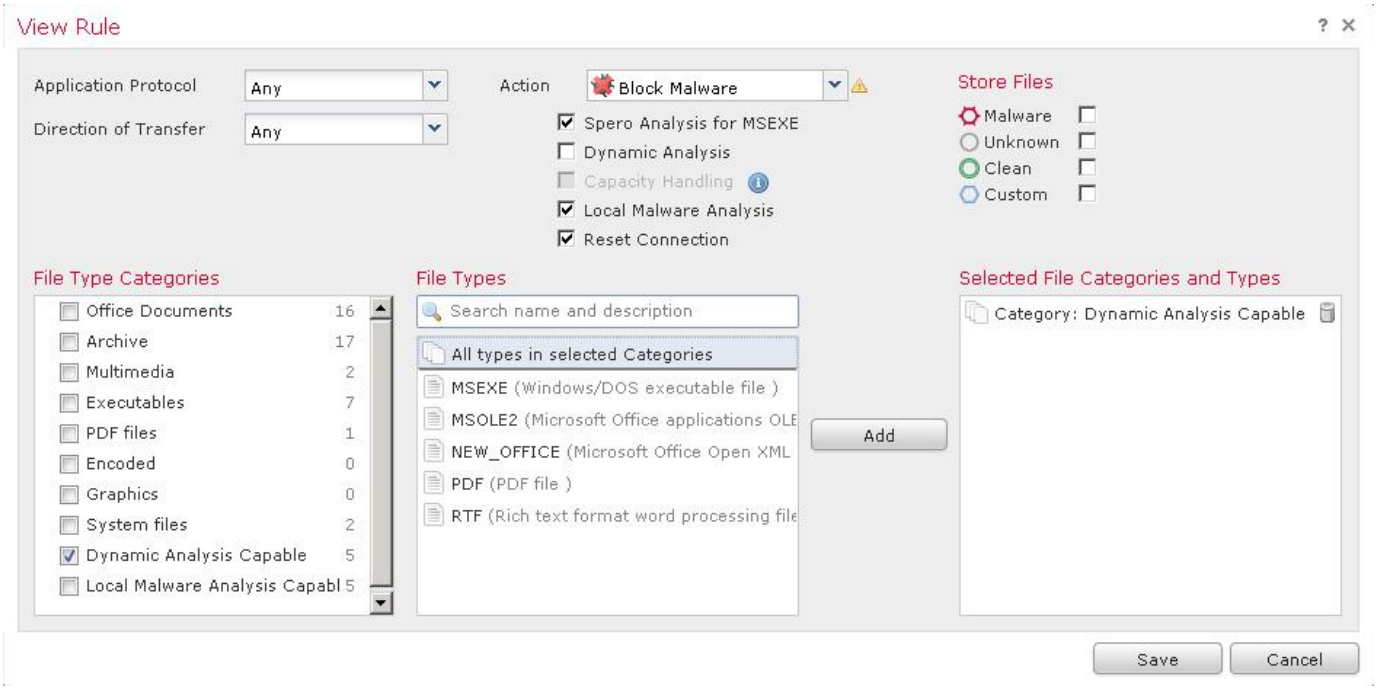


구성 A1,2 : 데모 파일 정책

1. **Policies > Access Control > Malware & File** 로 이동하십시오.

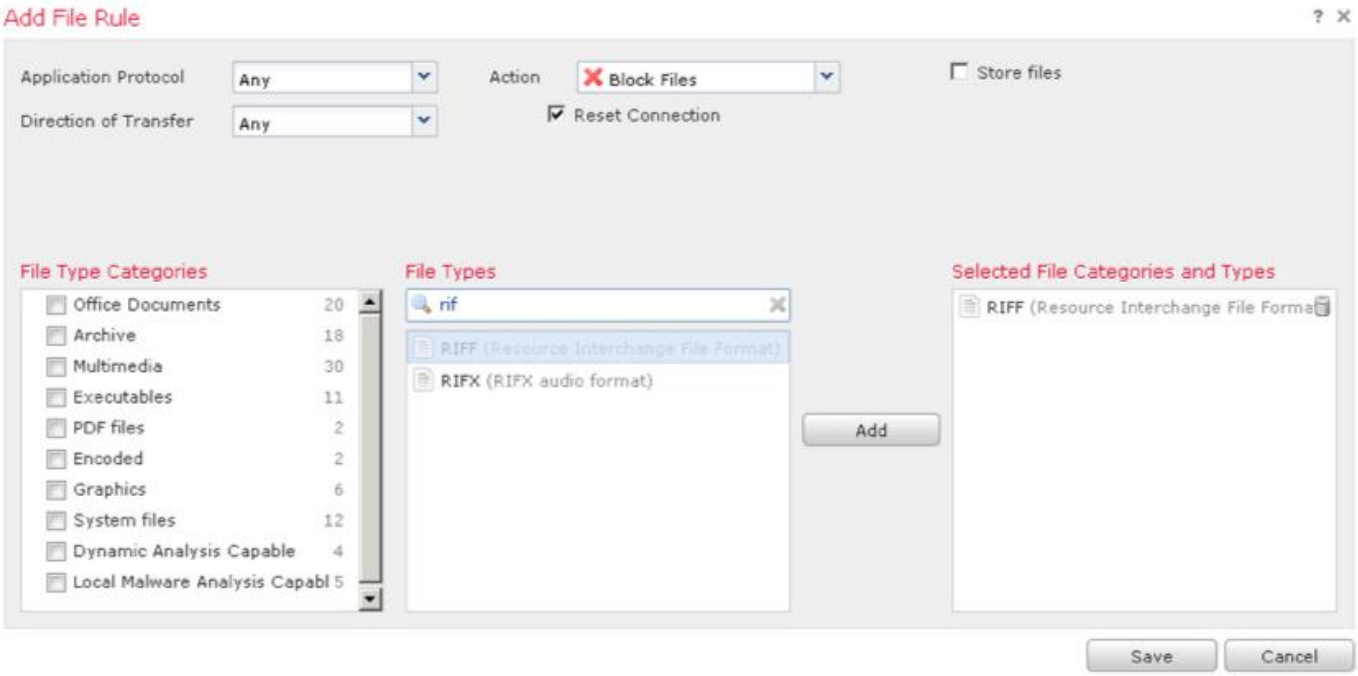
2. **New File Policy** 를 클릭하십시오. **Demo File Policy** 이름을 입력하십시오. **Save** 를 클릭하십시오.

3. **Add File Rule** 를 클릭하십시오. 이 룰은 MSEXE, MSOLE2, NEW_OFFICE 및 PDF 파일에 있는 멀웨어를 차단합니다.
   a. **Action** 에 **Block Malware** 를 선택하십시오.
   b. Spero 및 **Local Malware Analysis** 체크 박스를 체크하십시오.
   c. **File Type Categories** 에서 *Dynamic Analysis Capable* 을 선택하십시오. 여러 파일 유형이 이 범주에 속합니다. **Add** 를 클릭하십시오
   d. 화면은 아래 그림과 같아야합니다.



   e. **Save** 를 클릭하십시오. 경고를 메시지가 나타나면 무시하고 **OK** 을 클릭하십시오

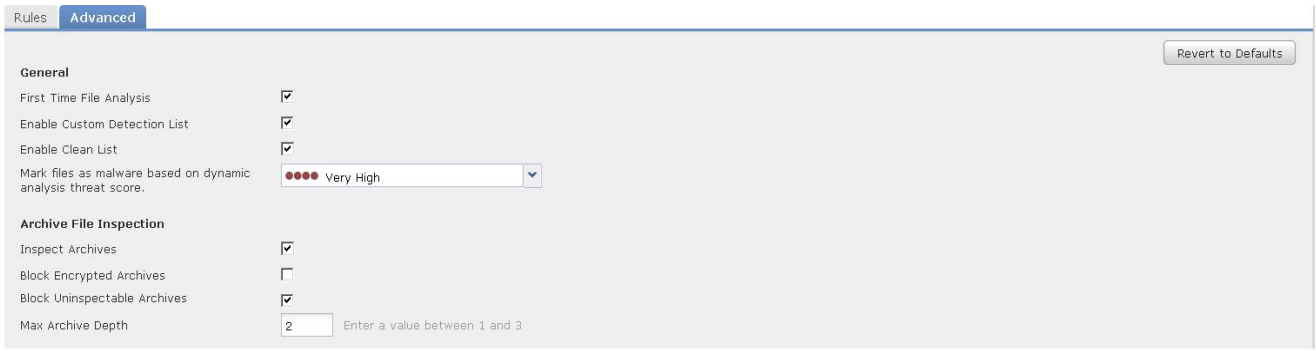
4. **Add File Rule** 를 클릭하십시오. 이 룰은 RIFF 파일을 차단합니다. AVI 파일은 RIFF 파일 유형이므로 AVI 파일을 사용하여 이 룰을 테스트합니다. 그러나 AVI 는 별도의 파일 유형으로 나열되지 않습니다.
   a. **Action** 에 **Block Files** 를 선택하십시오.
   b. **File Types** 에서 **rif** 를 검색 상자에 입력하십시오. 목록에서 **RIFF** 를 선택하십시오. **Add** 를 클릭하십시오.
   c. 다른 설정에는 기본값을 사용합니다. 화면은 아래 그림과 같아야합니다
   d. **Save** 를 클릭하십시오.



노트: 생성한 규칙 순서는 변경할 수 없습니다. 규칙의 순서는 중요하지 않습니다. 규칙의 동작에 따라 우선 순위가 결정됩니다. 액션 우선 순위는 다음과 같습니다.

1. 파일 차단
2. 악성 코드 차단
3. 멀웨어 클라우드 룩업
4. 파일 탐지

3. **Advanced** 탭을 선택하십시오. **Enable Custom Detection List** 가 선택되어 있는지 확인합니다. **Inspect Archives** 체크 박스를 체크하십시오.



노트: 손상된 아카이브 파일은 검사할 수 없습니다.

6. 오른쪽 위의 **Save** 버튼을 클릭하여 파일 정책을 저장하십시오.

구성 A1,3 : 데모 침입 정책

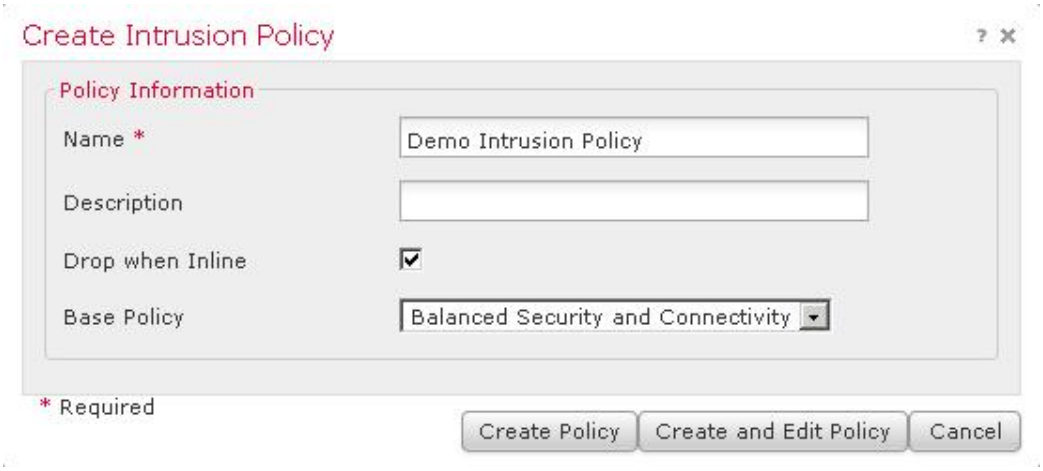
1. **Objects** > **Intrusion Rules** 로 이동하십시오. **Import Rules** 를 클릭하십시오.
    a. **Rule update or text rule file to upload and install** 을 선택하십시오.
    b. **Browse** 클릭하고 Jump 데스크탑의 **Files** 폴더에 있는 **Snort_Rules.txt** 파일을 엽니다.

노트: 이 파일에는 IPS 테스트에 유용한 두 가지의 간단한 Snort 룰이 포함되어 있습니다.
alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR"; sid: 1001001; rev:1;)
alert tcp any any -> any any (msg:"ProjectZ detected"; content:"ProjectZ"; sid: 1001002; rev:1;)
첫 번째 룰은 ProjectQ 문자열을 ProjectR 로 대체합니다. 두 번째 줄은 ProjectZ 문자열을 감지합니다. 규칙은 플로우의 어느 부분에 문자열이 있는지 지정하지 않기 때문에 프로덕션 환경에서 문제를 일으킬 수 있습니다.

    c. **Import** 를 클릭하십시오. 가져 오기 프로세스는 1 ~ 2 분이 소요됩니다. 작업이 완료되면 **Rule Update Import Log** 페이지가 나타납니다. 두 개의 룰을 성공적으로 가져 왔는지 확인하십시오.

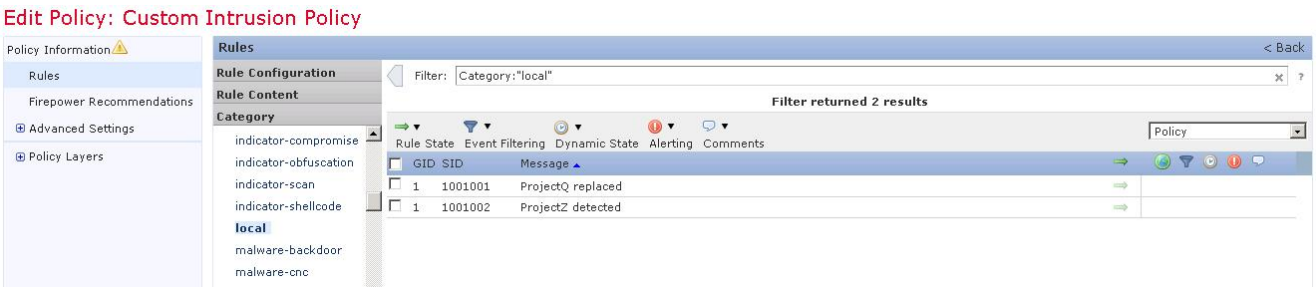
2. **Policies** > **Access Control** > **Intrusion** 로 이동하십시오.

3. **Create Policy** 를 클릭하십시오.
    a. 이름을 **Demo Intrusion Policy** 으로 설정하십시오.
    b. **Drop when Inline** 체크되었는지 확인하십시오.
    c. Balanced Security 및 Connectivity 를 **Base Policy** 로 선택하십시오.



    d. **Create and Edit Policy** 를 클릭하십시오.

4. 이 새로운 정책에 대한 규칙 상태를 수정합니다
    a. **Edit Policy** 페이지의 왼쪽에 있는 정책 정보 메뉴에서 **Rules** 를 클릭합니다.
    b. 룰의 카테고리 섹션에서 **local** 선택하십시오. 업로드된 2 개의 룰을 확인해야 합니다. 각 규칙의 오른쪽에있는 밝은 녹색 화살표는이 정책에 대한 규칙이 비활성화되었음을 나타냅니다.



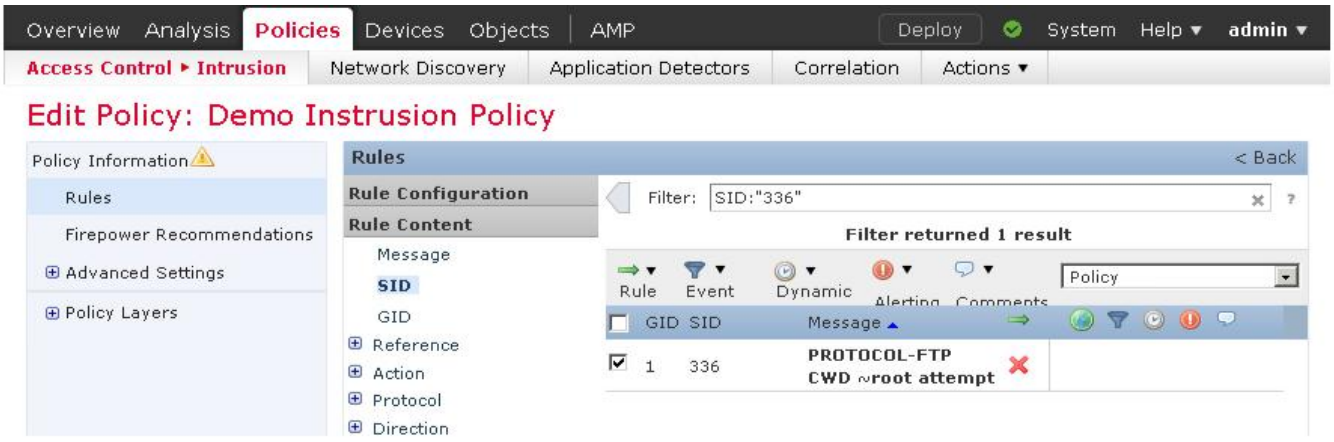
c. 첫 번째 룰 옆에 있는 체크박스를 체크하십시오. **Rule State** 드롭 다운 메뉴에서 **Generate Events** 를 선택하십시오. OK 를 클릭하십시오. 첫 번째 규칙 옆에 있는 체크박스의 체크를 취소하십시오.

d. 두 번째 룰 옆에 있는 체크박스를 체크하십시오. **Rule State** 드롭 다운 메뉴에서 **Drop and Generate Events** 를 선택하십시오. OK 를 클릭하십시오.

e. **Filter** 텍스트 필드의 오른쪽에있는 **X** 를 클릭하여 필터를 지웁니다.

f. **Rule Content** 섹션에서 **SID** 를 선택합니다. **Enter the SID** 필터 팝업에 **336** 을 입력하십시오. **OK** 를 클릭하십시오.

g. 룰 옆의 체크박스에 체크하십시오. **Rule State** 드롭 다운 메뉴에서 **Drop and Generate Events** 를 선택하십시오. **OK** 를 클릭하십시오.



노트: 이 룰은 21 포트를 통한 FTP 트래픽의 루트 홈 디렉토리에 대한 변경을 찾습니다. 외부 네트워크에서 들어오는 트래픽만 검색하지만 우리는 양방향을 검사하는 기본값 $ EXTERNAL_NET 을 사용하므로 룰이 양방향 트래픽에서 트리거될 수 있습니다. 이 룰을 수정하여 모든 방향에서 오는 FTP 트래픽을 검색하고 appid 속성을 사용해 모든 포트에서의 FTP 트래픽을 탐지할 수 있습니다.

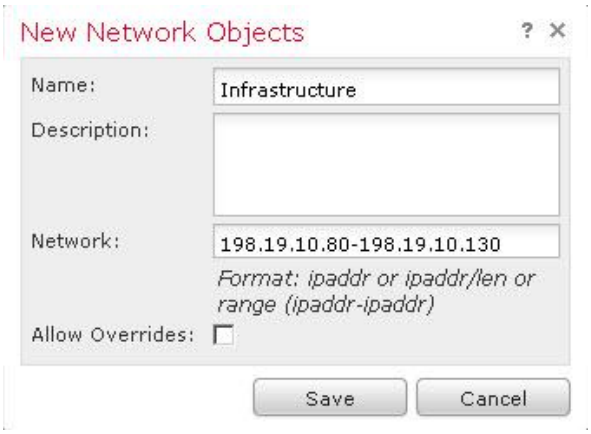
5. 왼쪽 상단의 메뉴에서 **Policy Information** 를 클릭합니다.

6. **Commit Changes** 를 클릭합니다. **OK** 를 클릭하십시오.

구성 A1, 4 : 데모 SSL 정책

1. **Objects > Object Management > PKI > Internal CAs** 로 이동합니다.
    a. **Import CA** 를 클릭합니다
    b. **Name** 에 **Verifraud** 를 입력하십시오.
    c. **Certificate Data or, choose a file** 텍스트 오른쪽에있는 **Browse** 선택하십시오
    d. Jump 데스크톱의 **Certificates** 폴더를 찾습니다.
    e. **Verifraud_CA.cer** 업로드합니다.
    a. *Key 또는, choose a file* 텍스트 오른쪽에있는 **Browse** 버튼을 클릭합니다.
    b. **Verifraud_CA.key** 업로드.
    c. **Save** 를 클릭합니다.

2. FMC 및 AMP Private Cloud 와 같은 디크립션 인프라 장치는 exempt 합니다. 이렇게 하려면 이러한 장치가 포함된 네트워크 오브젝트를 만듭니다.
    a. **Objects > Object Management > Networ**k 로 이동합니다.
    b. **Add Network > Add Object** 를 클릭십시오.
    c. **Name** 에 **Infrastructure** 를 입력하십시오.
    d. Network 에 **198.19.10.80-198.19.10.130** 을 입력하십시오.



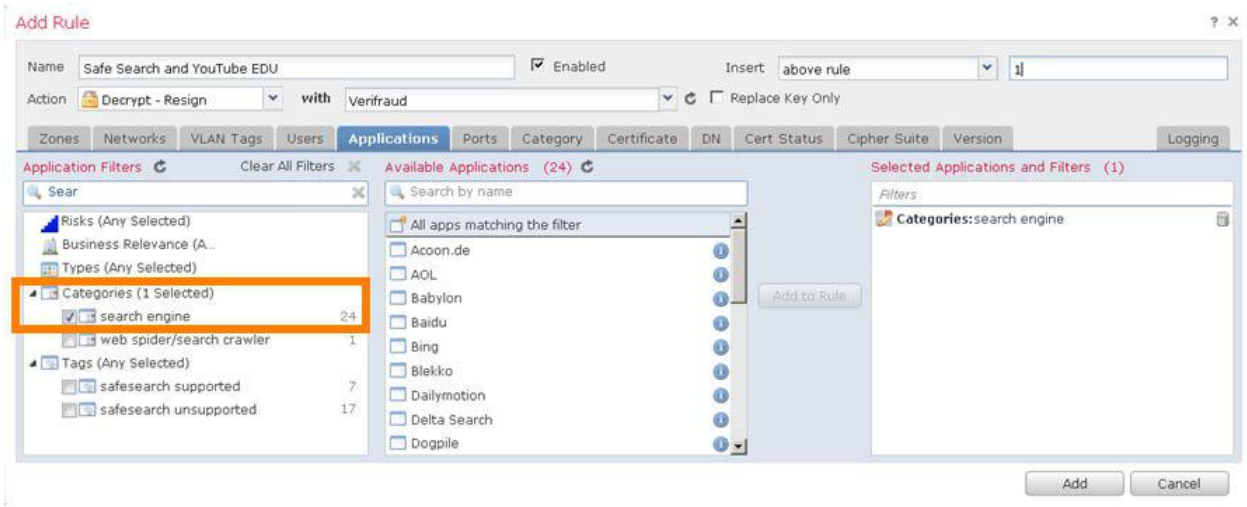
    e. **Save** 를 클릭하여 네트워크 오브젝트를 저장합니다.

3. **Policies > Access Control > SSL** 로 이동합니다.

4. **Add a new policy** 텍스트를 클릭하거나 **New Policy** 버튼을 클릭합니다.
    a. **Name** 에 **Demo SSL Policy** 를 입력하십시오.
    b. 기본 작업을 **Do not decrypt** 으로 그대로 둡니다.
    c. **Save** 를 클릭하십시오. 잠시 기다리면 정책 편집창이 열립니다.

5. **Add Rule** 을 클릭하십시오.
    a. **Name** 에 **Exempt Infrastructure** 를 입력하십시오.
    b. **Action** 을 **Do Not decrypt** 로 놔둡니다.
    c. **Networks** 탭의 **Networks** 에서 **Infrastructure** 선택하고 **Add to Source** 를 클릭합니다.
    d. **Add** 를 클릭하여 이 규칙을 SSL 정책에 추가합니다.

6. **Add Rule** 를 클릭하십시오.
    a. **Name** 에 **Decrypt Search Engines** 를 입력하십시오.
    b. **Action** 을 **Decrypt – Resign** 으로 설정합니다.
    c. **with** 오른쪽에 있는 드롭 다운 목록에서 **Verifraud** 를 선택하십시오.
    d. **Application Filters** 아래의 **Applications** 탭에서 **Sear** 를 검색합니다. **Categories** 아래에서 **Search Engine** 을 확인할 수 있습니다. 체크박스를 체크하고 **Add to Rule** 를 클릭하십시오.



    e. **Logging** 탭을 선택하고 **Log at End of Connection** 체크박스를 체크하십시오.
    f. **Add** 를 클릭하여이 규칙을 SSL 정책에 추가합니다.

7. **Add Rule** 를 클릭하십시오.
    a. Name 에 **Decrypt Other** 를 입력하십시오.
    b. **Action** 을 **Decrypt – Resign** 로 설정하십시오.
    c. **with** 의 오른쪽에 있는 드롭 다운 목록에서 Verifraud 를 선택하십시오.
    d. **Logging** 탭을 선택하고 **Log at End of Connection** 확인란을 선택하십시오.
    e. **Add** 를 클릭하여 이 룰을 SSL 정책에 추가합니다.

8. **Save** 를 클릭하여 SSL policy 를 저장하십시오.

노트: Replace Key 체크박스에 대해 설명합니다. 액션이 Decrypt – Resign 으로 설정 될 때마다 Firepower 가 공개키를 대체합니다. Replace Key 체크박스는 decrypt 액션이 자체 서명 서버 인증서에 어떻게 적용될지를 결정합니다.

• Replace Key 를 선택 취소하면 자체 서명 인증서는 다른 서버 인증서와 같이 취급됩니다. Firepower 가 키를 대체하고 인증서를 Resign 합니다. 일반적으로 엔드포인트은 Firepower 를 신뢰하도록 구성되기 때문에 Resigned 된 인증서를 신뢰합니다.

• Replace Key 를 선택하면 자체 서명 인증서는 다르게 취급됩니다. Firepower 가 키를 대체하고 새로운 자체 서명 인증서를 생성합니다. 엔드포인트의 브라우저는 인증서 경고를 표시합니다.

즉, Replace Key 체크박스를 선택하면 자체 서명 인증서의 신뢰성 부족으로 Resign 액션을 취하도록 합니다.

구성 A1,5 : 사용자 지정 검색 목록

Zombies.pdf 라는 파일이 안전한 파일로 인해 클라우드 룩업을 발생시키는 조회가 성공했다고 가정합니다. 때때로 실험실에는 클라우드 연결에 문제가 있습니다. 따라서 이것은 사용자 지정 검색 목록에 추가되어 맬웨어 이벤트를 트리거합니다.

1. **Objects > Object Management > File List** 로 이동합니다.

2. 연필 아이콘을 클릭하여 **Custom-Detection-List** 을 편집합니다

    a. **Add by** 드롭 다운 목록에서 **Calculate SHA** 를 선택합니다

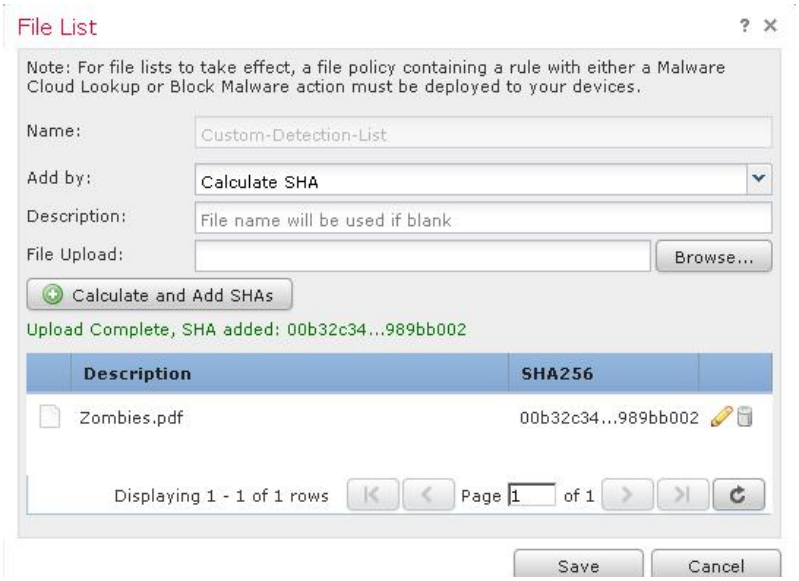
    b. **Browse** 를 클릭하십시오.

    c. Jump 데스크톱에서 Files 폴더를 찾습니다

    d. **Zombies.pdf** 를 선택하고 **OK** 를 클릭하십시오.

    e. **Calculate 및 Add SHAs** 를 클릭하십시오.

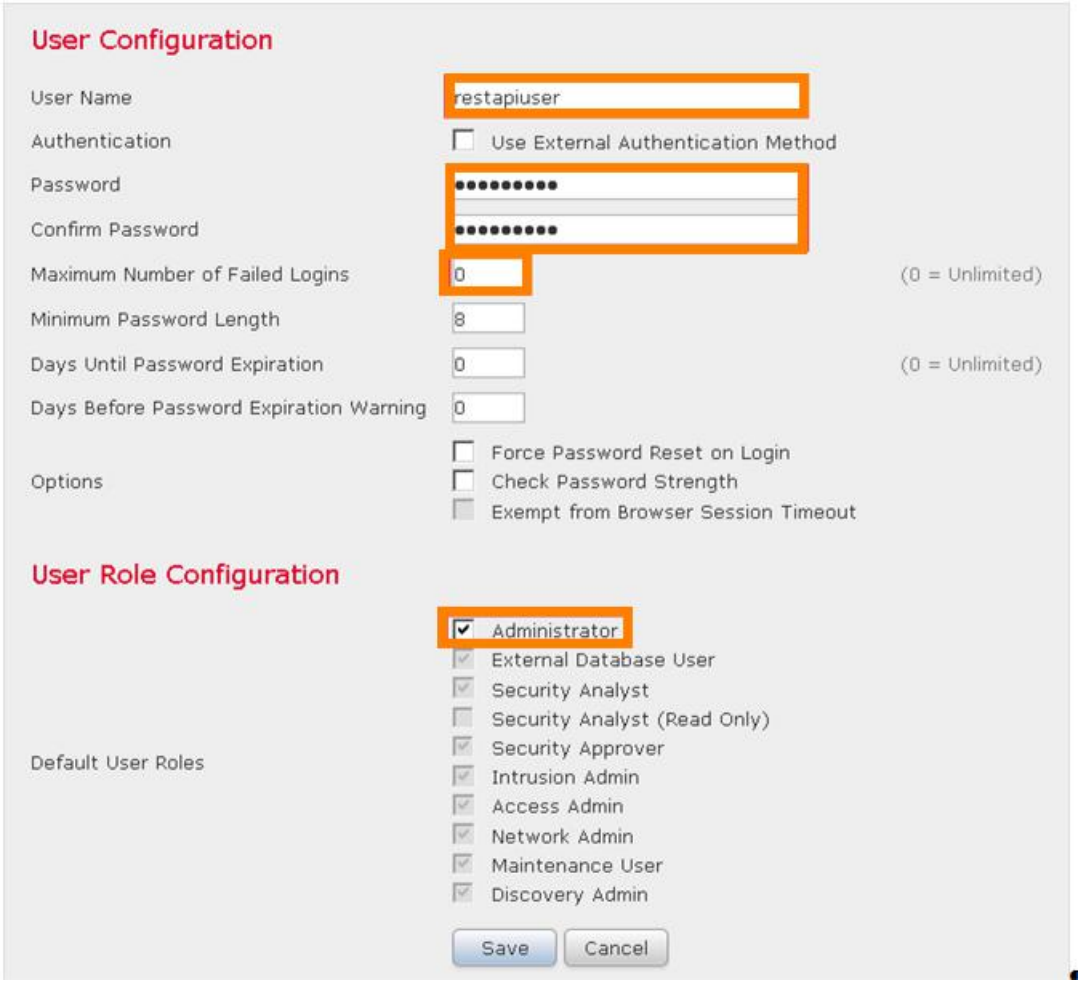
    f. Click **Save** 를 클릭하십시오.



구성 A1,6 : 추가 사용자 추가

별도로 API Explorer 를 사용하는 것이 편리합니다. 이렇게 하면 FMC 와 API Explorer 를 동시에 사용할 수 있습니다.

1. **System > Users** 로 이동한 다음 **Create User** 를 클릭하십시오.
    a. 이용자명에 **restapiuser 을** 입력하십시오.
    b. **패스워드**에 **C1sco12345** 를 입력하십시오. 패스워드를 확인하십시오.
    c. Failed Logins 의 최대 수를 **0** 으로 설정하십시오.
    d. **Administrator** 체크박스 확인하십시오.



구성 A1,7 : 서버 인증서 설치

기본값으로 FMC UI 는 자체 서명 인증서를 사용합니다. 이는 Jump 브라우저가 신뢰하는 pod AD 서버가 서명한 인증서로 대체됩니다.

1. **Objects > Object Management > PKI > Trusted CAs** 로 이동합니다.
    a. **Add Trusted CA** 를 클릭하십시오.
    b. **Name** 에 **dCloud** 를 입력하십시오.
    c. **Certificate Data or, choose a file** 텍스트 오른쪽에있는 **Browse** 버튼을 클릭.
    d. Jump 데스크톱의 **Certificates** 폴더를 찾습니다.
    e. **AD-ROOT-CA-CERT.cer** 을 업로드하십시오.
    f. **Save** 를 클릭합니다.
2. SSH 를 통해 FMC CLI 에 연결하십시오. **sudo -i** 를 입력하여 루트가 됩니다. Sudo 패스워드는 C1sco12345 입니다.
    a. **cd /etc/ssl** 를 입력한 다음 **cp server* /root** 를 입력하십시오.
    b. **cat > /etc/ssl/server.crt** 를 입력하십시오.
    c. 점프 데스크탑의 **Certificates** 폴더에서 Notepad++로 **fmc.cer** 파일을 편집하십시오.
    d. 모두 선택한 뒤 복사하여 FMC CLI 에 붙여 넣습니다.
    e. **Ctrl+D** 를 입력하십시오.
    f. **cat > /etc/ssl/server.key** 를 입력하십시오.
    g. 점프 데스크탑의 **Certificates** 폴더에서 Notepad++로 **fmc.key** 파일을 편집하십시오.
    h. 전체 선택하고 카피하여 FMC CLI 에 붙여 넣습니다.
    i. **Ctrl+D** 를 입력하십시오
    j. **pmtool restartbyid httpsd** 를 입력하십시오.

부록 B. REST API 스크립트

다음 스크립트들은 첫 번째 랩에서 사용한 두 개의 Python 스크립트입니다. 첫 번째 스크립트 **register_config.py** 만 실행하고, 실행한 뒤에 두 번째 스크립트인 **connect.py** 가 호출되어 컴파일된 **connect.pyc** 이 생성됩니다.

Python script register_config.py

```
#!/usr/bin/python
import json
import connect
import sys

host = "fmc.example.com"
username = "restapiuser"
password = "C1sco12345"
name="NGFW"

#connect to the FMC API
headers,uuid,server = connect.connect (host, username, password)

user_input = str(raw_input("Would you like to register the managed device? [y/n]"))
if user_input == "y":
 policy_name = str(raw_input("Enter name of new Access Control Policy to be create:"))
 access_policy = {
 "type": "AccessPolicy",
 "name": policy_name,
 "defaultAction": { "action": "BLOCK" }
 }
 post_response = connect.accesspolicyPOST(headers,uuid,server,access_policy)
 policy_id = post_response["id"]
 print "\n\nAccess Control Policy\n" + policy_name + "\ncreated\n\n"
 device_post = {
 "name": name,
 "hostName": "ngfw.example.com",
 "regKey": "C1sco12345",
 "type": "Device",
 "license_caps": [
 "BASE",
 "MALWARE",
 "URLFilter",
 "THREAT"
 ],
 "accessPolicy": {
 "id": policy_id,
 "type": "AccessPolicy"
 }
 }
 post_data = json.dumps(device_post)

 output = connect.devicePOST (headers, uuid, server, post_data)
# print "\n\nPost request is: \n" + json.dumps(output,indent=4) + "\n\n"

# GET ALL THE DEVICES AND THEIR corresponding interfaces

user_input = str(raw_input("In the FMC UI, confirm that the device discovery has completed and then
press 'y' to continue or 'n' to exit. [y/n]"))
headers,uuid,server = connect.connect (host, username, password)
```

```
if user_input == "n":
 quit()

devices = connect.deviceGET(headers,uuid,server)
for device in devices["items"]:
 if device["name"] == name:
 print "DEVICE FOUND, setting ID"
 device_id = device["id"]

# NOW THAT WE HAVE THE DEVICE ID WE NEED TO GET ALL THE INTERFACES

interfaces = connect.interfaceGET(headers,uuid,server,device_id)
# Interfaces i want to change
interface_1 = "GigabitEthernet0/0"
interface_2 = "GigabitEthernet0/1"

for interface in interfaces["items"]:
 if interface["name"] == interface_1:
 interface_1_id = interface["id"]
 print "interface 1 found"
 if interface["name"] == interface_2:
 interface_2_id = interface["id"]
 print "interface 2 found"

user_input = str(raw_input("Would you like to configure device interfaces? [y/n]"))

if user_input == "y":
 interface_put = {
 "type": "PhysicalInterface",
 "hardware": {
 "duplex": "AUTO",
 "speed": "AUTO"
 },
 "enabled": True,
 "MTU": 1500,
 "managementOnly": False,
 "ifname": "outside",
 "enableAntiSpoofing": False,
 "name": "GigabitEthernet0/0",
 "id": interface_1_id,
 "ipv4" : {
 "static": {
 "address":"198.18.133.2",
 "netmask":"18"
 }
 }
 }
 put_data = json.dumps(interface_put)
 connect.interfacePUT (headers, uuid, server, put_data,device_id,interface_1_id)
 interface_put = {
 "type": "PhysicalInterface",
 "hardware": {
 "duplex": "AUTO",
 "speed": "AUTO"
 },
 "enabled": True,
 "MTU": 1500,
 "managementOnly": False,
 "ifname": "inside",
```

```
 "enableAntiSpoofing": False,
 "name": "GigabitEthernet0/1",
 "id": interface_2_id,
 "ipv4" : {
 "static": {
 "address":"198.19.10.1",
 "netmask":"24"
 }
 }
 }
 put_data = json.dumps(interface_put)
 connect.interfacePUT (headers, uuid, server, put_data,device_id,interface_2_id)
```

Python script connect.py

```
#!/usr/bin/python
import json
import sys
import requests
#Surpress HTTPS insecure errors for cleaner output
from requests.packages.urllib3.exceptions import InsecureRequestWarning

requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

#define fuction to connect to the FMC API and generate authentication
token def connect (host, username, password):
 headers = {'Content-Type': 'application/json'}
 path = "/api/fmc_platform/v1/auth/generatetoken"
 server = "https://"+host
 url = server + path
 try:
 r = requests.post(url, headers=headers, auth=requests.auth.HTTPBasicAuth(username,password),
verify=False)
 auth_headers = r.headers
 token = auth_headers.get('X-auth-access-token', default=None)
 uuid = auth_headers.get('DOMAIN_UUID', default=None)
 if token == None:
 print("No Token found, I'll be back terminating....")
 sys.exit()
 except Exception as err:
 print ("Error in generating token --> "+ str(err))
 sys.exit()
 headers['X-auth-access-token'] = token

 return headers,uuid,server


def devicePOST (headers, uuid, server, post_data):
 api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords"
 url = server+api_path
 try:
 r = requests.post(url, data=post_data, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
```

```
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 201 or status_code == 202:
 print("Post was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response



def deviceGET (headers, uuid, server):
 api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords"
 url = server+api_path
 try:
 r = requests.get(url, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200:
 print("GET was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def interfaceGET (headers, uuid, server, device_id):
 api_path= "/api/fmc_config/v1/domain/" + uuid +
"/devices/devicerecords/"+device_id+"/physicalinterfaces"
 url = server+api_path
 try:
 r = requests.get(url, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200:
 print("GET was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def interfacePUT (headers, uuid, server, put_data,device_id, interface_id):
 api_path= "/api/fmc_config/v1/domain/" + uuid +
"/devices/devicerecords/"+device_id+"/physicalinterfaces/"+interface_id
```

```
 url = server+api_path
 try:
 r = requests.put(url, data=put_data, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200 :
 print("Put was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def accesspolicyPOST (headers, uuid, server, post_data):
    api_path= "/api/fmc_config/v1/domain/" + uuid + "/policy/accesspolicies"
    url = server+api_path
    try:
            r = requests.post(url, data=json.dumps(post_data), headers=headers, verify=False)
            status_code = r.status_code
            resp = r.text
            json_response = json.loads(resp)
            print("status code is: "+ str(status_code))
            if status_code == 201 or status_code == 202:
                    print("Post was sucessfull...")
            else:
                    r.raise_for_status()
                    print("error occured in POST -->"+resp)
    except requests.exceptions.HTTPError as err:
            print ("Error in connection --> "+str(err))
    finally:
            if r: r.close()
    return json_response
```

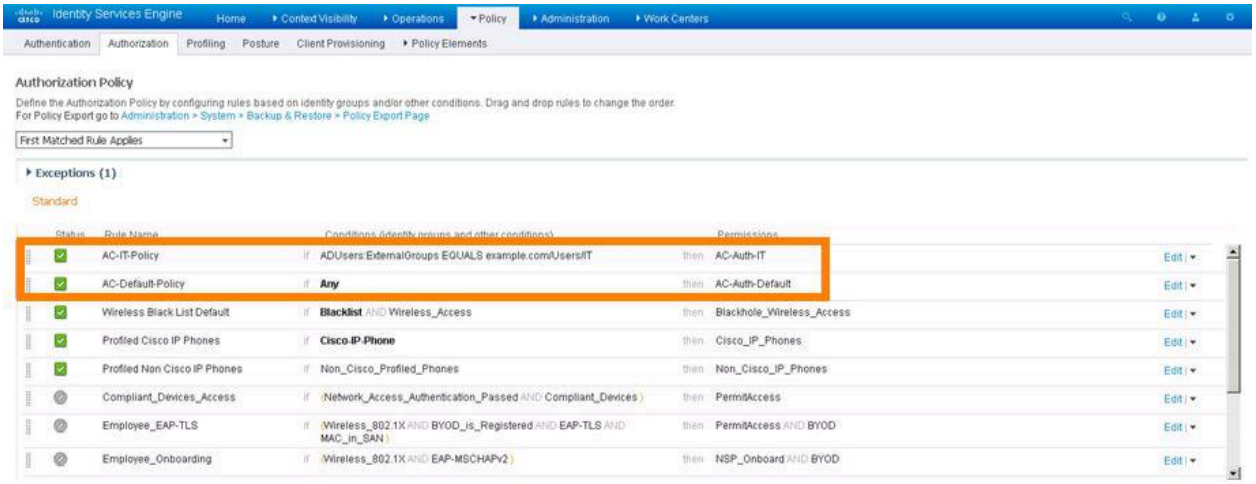
부록 C. ISE RA VPN 설정

ISE 는 모든 시나리오 내용을 지원하도록 사전에 구성되어 있습니다. 이 부록에서는 이 구성을 요약합니다. Firefox 북마크 툴바에 ISE 링크가 있으며 자격 증명은 미리 채워집니다. 자격 증명은 이용자명 **admin**, 패스워드는 **C1sco12345** 입니다.

노트: 이 부록은 ISE 튜토리얼이 아닙니다. 따라서 ISE 구성 방법에 대한 자세한 내용은 다루지 않습니다. 이 가이드의 실습을 위해 RA VPN 구성 요소를 구성하는데 필요한 세부 정보만 다루고 있습니다. 구성 내용에 대한 설명은 top-down 방식으로 되어 있으며 실제 이 구성을 만드는 경우에는 반대로 bottom-up 순서로 구성하는 것이 좋습니다.

권한 정책

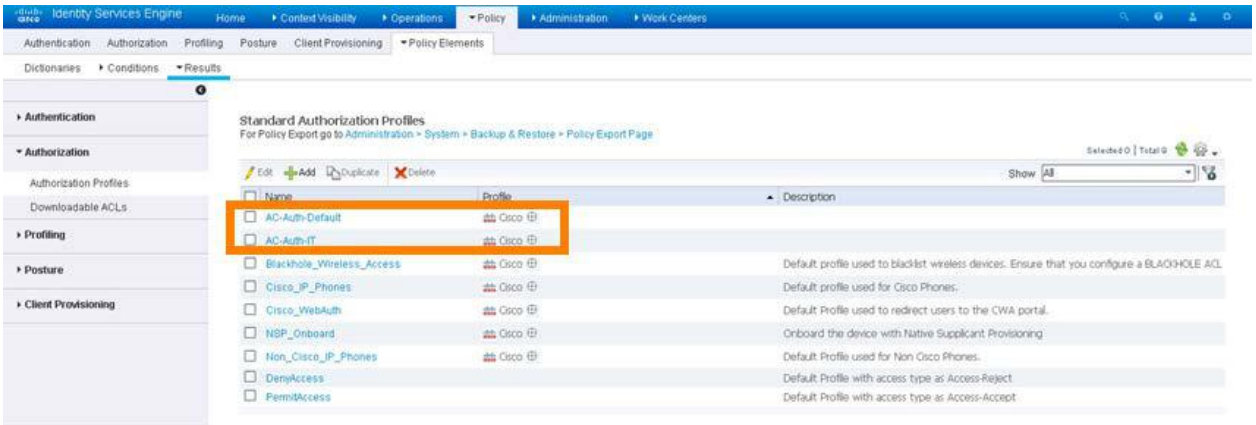
1. **Policy > Authorization** 로 이동합니다. 본 실습을 위해 두 가지 정책이 만들어졌습니다: **AC-IT-Policy** 및 **AC-Default-Policy**. 아래에 설명된 **AC-Auth-IT** 및 **AC-Auth-Default** 라는 두 가지 권한 프로파일을 참조합니다.



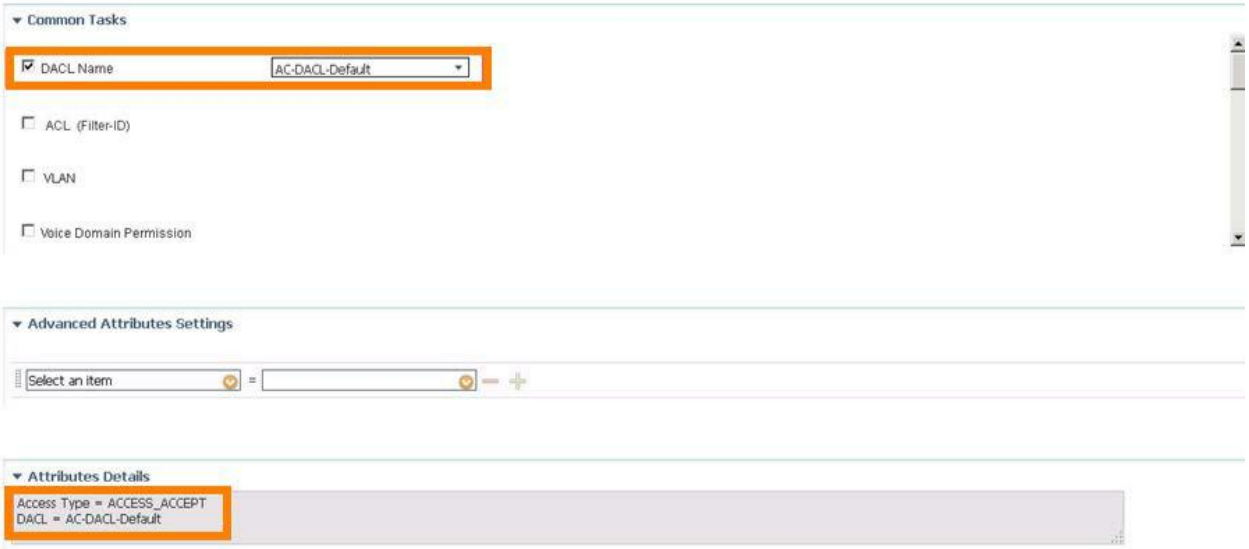
이 정책은 두 개의 권한 프로파일을 참조합니다: AC-Auth-IT 및 AC-Auth-Default.

권한 프로파일

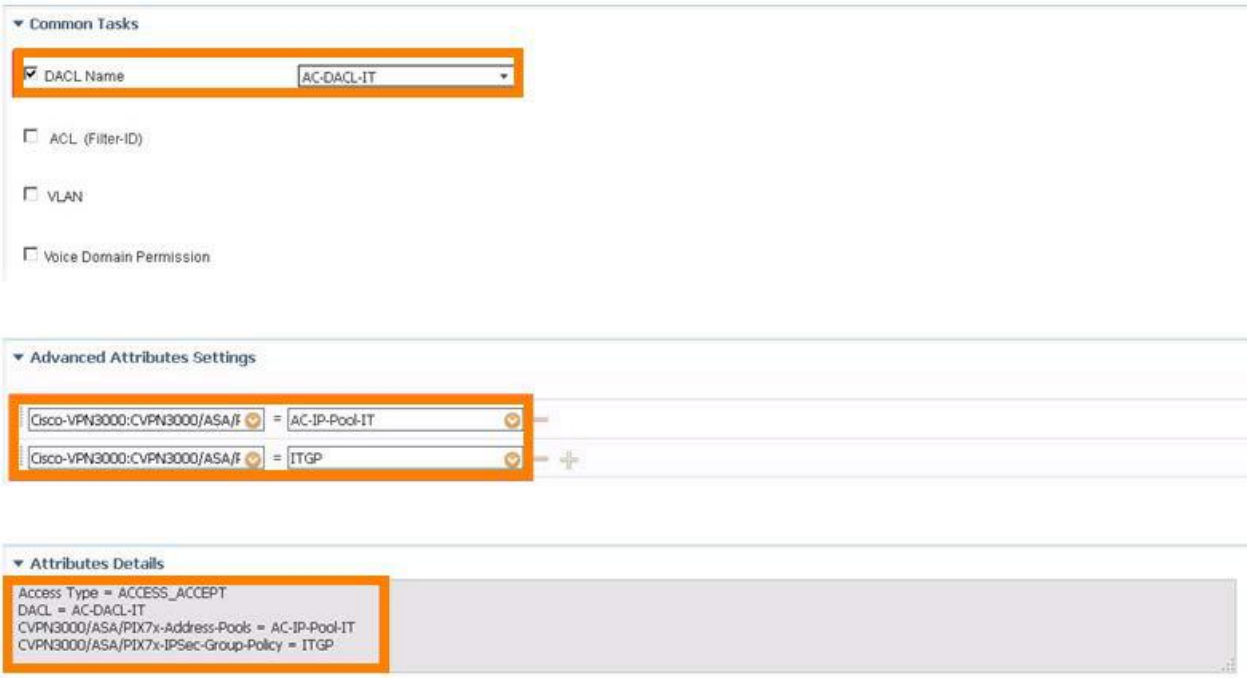
1. **Policy > Policy Elements > Results > Authorization > Authorization Profiles** 로 이동합니다. 처음 두 프로파일은 이 랩을 위해 작성되었습니다:. **AC-Auth-Default** 및 **AC-Auth-IT**.



2. **AC-Auth-Default** 을 드릴 다운하면 아래 설명된 **DACL AC-DACL-Default** 를 참조하는 것을 알 수 있습니다.

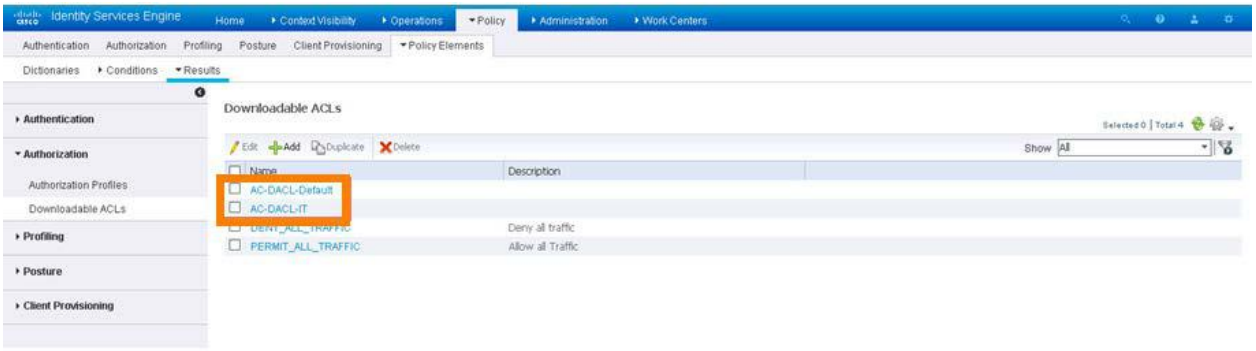


3. **AC-Auth-IT** 를 드릴 다운하면 아래 설명된 **DACL AC-DACL-IT** 를 참조하는 것을 알 수 있으며 또한 두 개의 고급 특성을 가지고 있습니다: 하나는 주소 Pool 용이고 다른 하나는 그룹 정책용입니다.

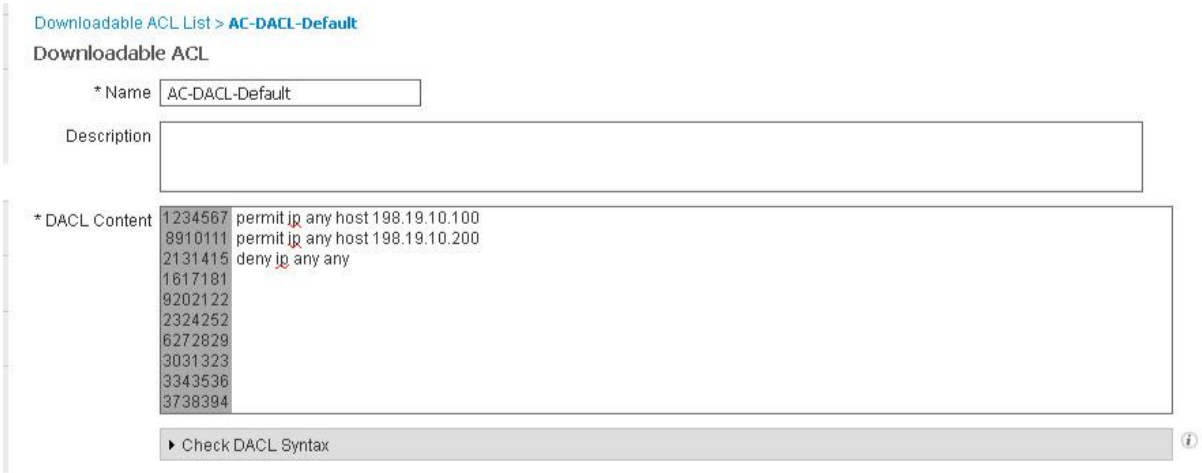


다운로드형 ACL

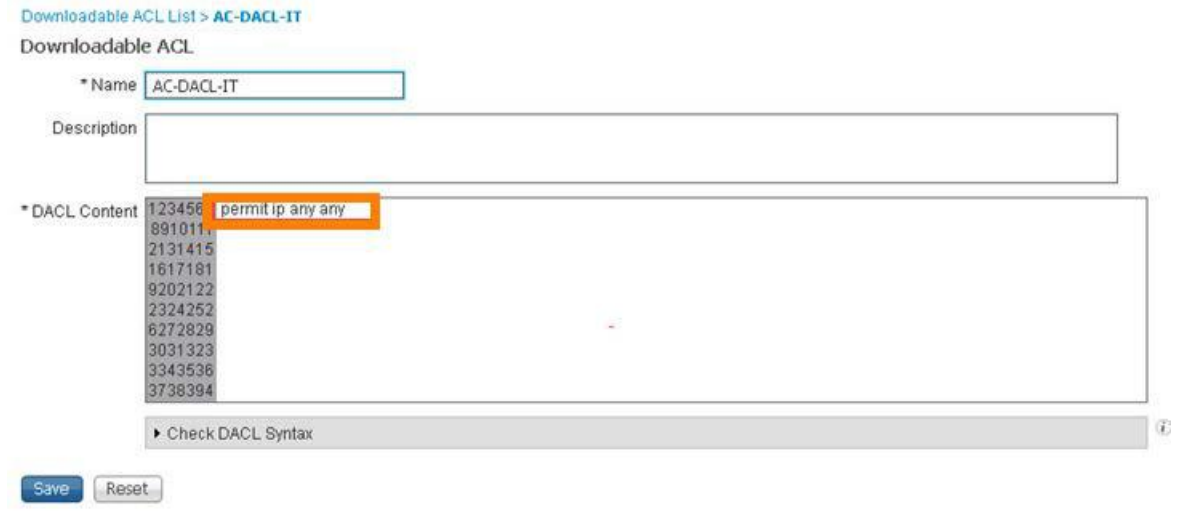
1. **Policy > Policy Elements > Authorization > Downloadable ACLs** 로 이동합니다. 먼저 두 개의 DACL 은 이 랩을 위해 만들어졌습니다: **AC-DACL-Default** 및 AC-DACL-IT.



2. **AC-DACL-Default** 을 드릴 다운하면 198.19.10.100 및 198.19.10.200 에 대한 액세스를 제한하고 있습니다.



3. **AC-DACL-IT 를** 드릴 다운하면 아무런 제한이 없음을 알 수 있습니다.



부록 D. Alien Vault 를 TAXII 피드로 사용

본 부록은 무료 TAXII 피드의 소스인 Hail a TAXII 의 대안을 제공합니다.
이 작업은 다음 작업으로 구성됩니다:

- Alien Vault 에서 계정 만들기
- API 토큰 얻기
- Alien Vault TAXII 피드로 CTID 구독

스텝

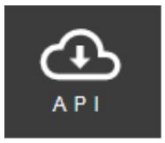
Alien Vault 계정 생성

1. https://otx.alienvault.com 로 이동합니다.
    a. 사용자 이름, 유효한 이메일 주소 및 암호를 입력하십시오.
    b. **SIGN UP** 을 클릭하십시오.

2. 위의 1a. 단계에서 사용한 이메일 계정에 로그인하고 확인 링크를 클릭하십시오.
    a. confirmation 링크를 클릭하십시오.
    b. **Confirm** 표시되면 **Confirm** 버튼을 클릭하십시오.
    c. **LOGIN** 을 클릭하여 Alien Vault 계정에 로그인하십시오.

API 토큰 얻기

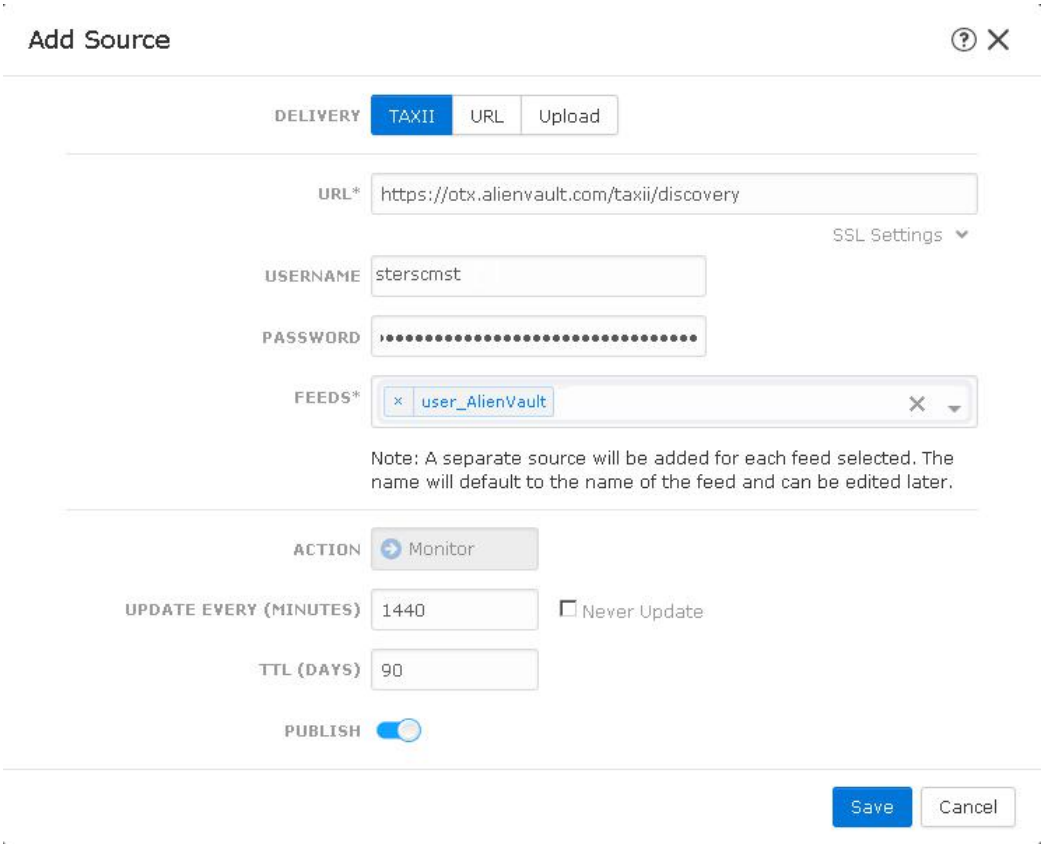
1. Alien Vault 계정에서 페이지의 중앙 상단에있는 API 링크를 클릭하십시오.



2. 페이지 오른쪽에서 API 토큰의 오른쪽에있는 Copy 버튼을 클릭하십시오. 이 파일을 저장할 수 있습니다.

Alien Vault TAXII 피드로 CTID 구독

1. **Intelligence > Sources > Sources** 로 이동합니다. 오른쪽 더하기 기호를 클릭하여 인텔리전스 소스를 추가하십시오.
    a. **DELIVERY 로 TAXII** 를 선택하십시오.
    b. **URL** 에 **https://otx.alienvault.com/taxii/discovery** 를 입력하십시오.
    c. **USERNAME** 에 여러분의 Alien Vault 로그인 계정을 입력하십시오.
    d. **PASSWORD** 에는 Alien Vault 계정에서 복사한 API 토큰을 붙여넣기 합니다.
    e. **FEEDS** 에 **user_AlienVault** 를 선택하십시오. **FEEDS** 드롭 다운 목록이 표시되기까지 몇 초 걸릴 수 있습니다.
    f. 화면이 아래의 그림과 같은지 확인합니다.



    g. *Save* 를 클릭하십시오

2. 이 Source 의 상태열이 Downloading 에서 Parsing 으로 바뀔 때까지 기다리십시오. Parsing 에서 Complete 로 바뀔 때까지 오래 걸리기 때문에 기다리지 마십시오.

3. **Intelligence > Sources > Indicators** 로 이동합니다. 여러 개의 URL indicators 가 추가되었는지 확인하십시오.

4. **Intelligence > Sources > Observables** 로 이동합니다. 여러 개의 URL observables 항목이 추가되었는지 확인하십시오.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**