단일 로그인 및 종속 포털 인증을 위한 ASDM과의 Active Directory 통합 구성(온박스 관리)

목차

소개

이 문서에서는 ASDM(Adaptive Security Device Manager)을 사용하여 Firepower Module에서 종속 포털 인증(액티브 인증) 및 Single-Sign-On(패시브 인증)의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA(Adaptive Security Appliance) 방화벽 및 ASDM에 대한 지식
- FirePOWER 모듈 지식

- LDAP(Light Weight Directory Service)
- Firepower UserAgent

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 5.4.1 이상을 실행하는 ASA FirePOWER 모듈(ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)
- 소프트웨어 버전 6.0.0 이상을 실행하는 ASA FirePOWER 모듈(ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Captive Portal Authentication(종속 포털 인증) 또는 Active Authentication(활성 인증)은 로그인 페이지를 표시하고 호스트가 인터넷 액세스를 얻으려면 사용자 자격 증명이 필요합니다.

Single-Sign-On 또는 Passive Authentication은 사용자 자격 증명을 여러 번 입력하지 않고도 네트워크 리소스 및 인터넷 액세스를 위한 사용자에게 원활한 인증을 제공합니다.Single-Sign-On 인증은 Firepower 사용자 에이전트 또는 NTLM 브라우저 인증을 통해 수행할 수 있습니다.

> **참고**:종속 포털 인증, ASA는 라우팅 모드여야 합니다.

> **참고:**captive portal 명령은 ASA 버전 9.5(2) 이상에서 사용할 수 있습니다.

구성

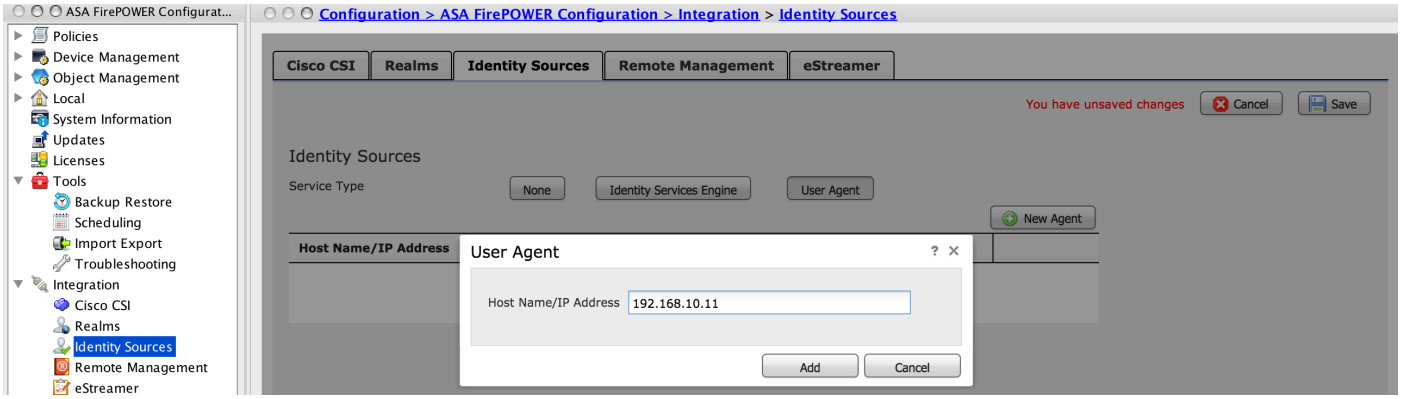
1단계. Single-Sign-On용 Firepower User Agent를 구성합니다.

이 문서에서는 Windows 시스템에서 Firepower User Agent를 구성하는 방법에 대해 설명합니다.

Sourcefire User Agent 설치 및 제거

2단계. ASDM(Firepower Module)을 User Agent와 통합합니다.

ASDM에 로그인하고 Configuration(컨피그레이션) > **ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Integration(통합) > Identity Sources(ID 소스)로 이동하고 User Agent** 옵션을 클릭합니다.User **Agent** 옵션을 클릭하고 User Agent 시스템의 IP 주소를 구성한 후,이미지에 표시된 대로 Add(추가)를 클릭합니다.



변경 사항을 저장하려면 **Save** 버튼을 클릭합니다.

3단계. Firepower를 Active Directory와 통합합니다.

3.1단계 영역을 생성합니다.

ASDM에 로그인하고 Configuration(컨피그레이션) > **ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Integration(통합) > Realms(영역)**로 이동합니다.Add a **New Realm**을 클릭합니다.

이름 및 설명: 영역을 고유하게 식별하는 이름/설명을 지정합니다.

유형: AD

AD 기본 도메인: Active Directory의 도메인 이름(NETBIOS 이름).

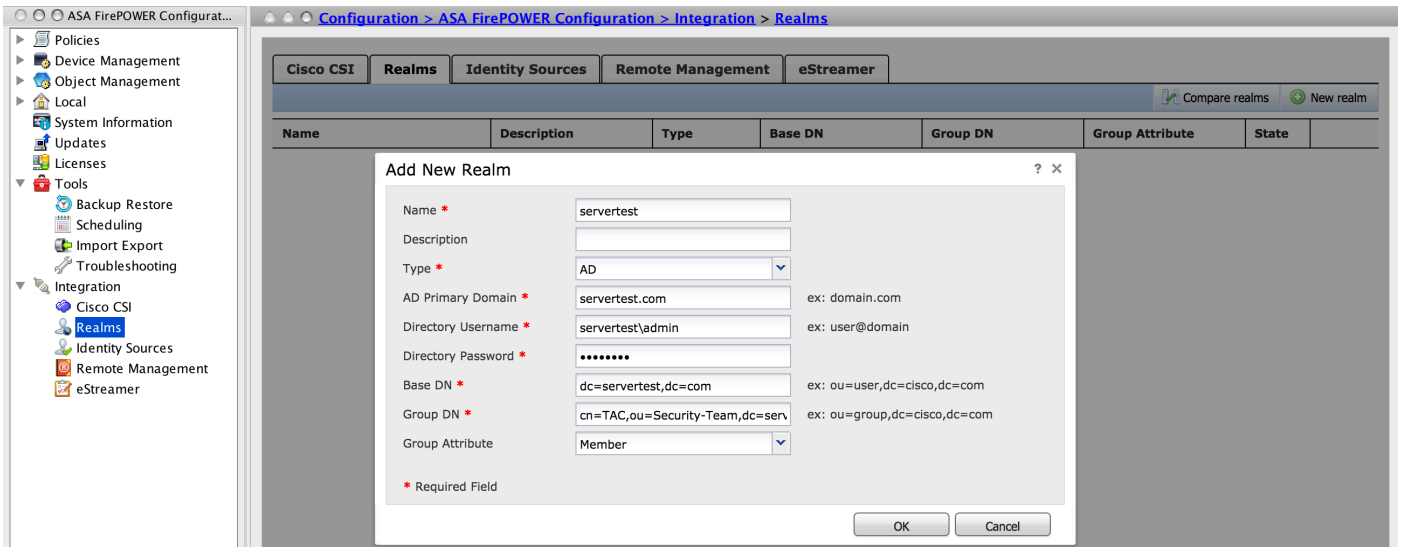
Directory Username(디렉토리 사용자 이름): <*username*>을 지정합니다.

디렉터리 암호: <*password*>를 지정합니다.

Base DN: 시스템이 LDAP 데이터베이스에서 검색을 시작할 도메인 또는 특정 OU DN입니다.

그룹 DN:그룹 DN을 지정합니다.

그룹 특성:드롭다운 목록에서 Member 옵션을 지정합니다.



OK(확인)를 클릭하여 컨피그레이션을 저장합니다.

이 문서에서는 기본 DN 및 그룹 DN 값을 파악하는 데 도움이 될 수 있습니다.

[Active Directory LDAP 개체 특성 식별]

3.2단계 디렉토리 서버 IP 주소/호스트 이름을 추가합니다.

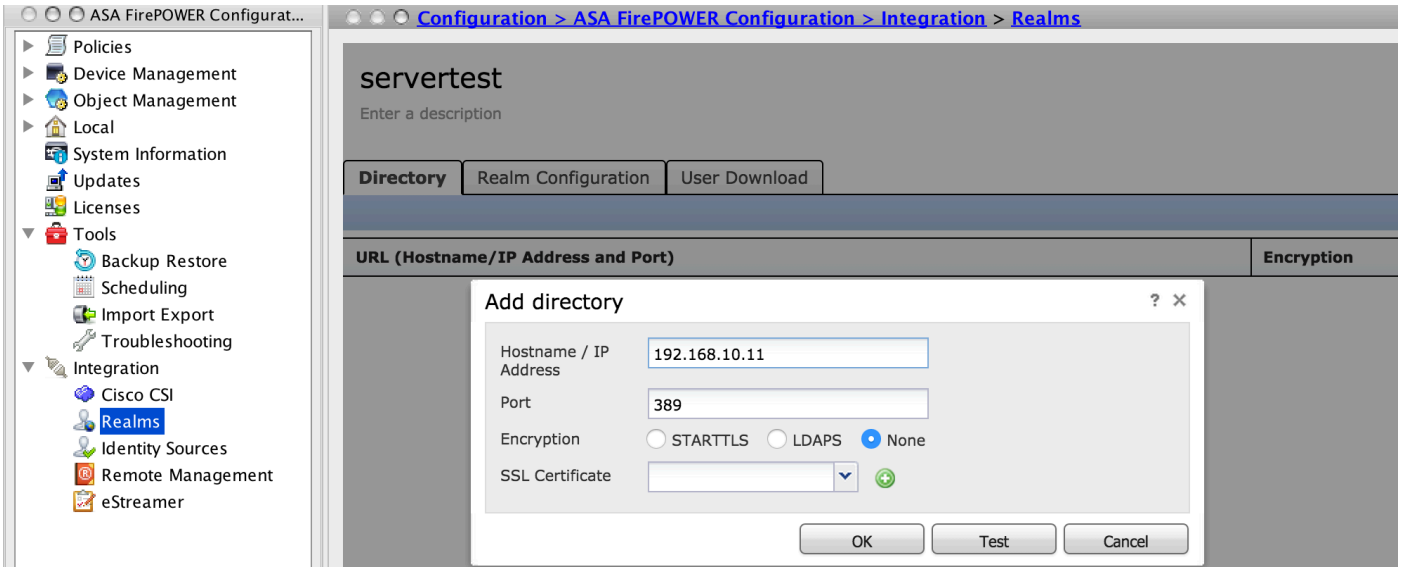
AD 서버 IP/호스트 이름을 지정하려면 Add **directory**를 클릭합니다.

Hostname/IP Address: AD 서버의 IP 주소/호스트 이름을 구성합니다.

포트: Active Directory LDAP 포트 번호를 지정합니다(기본값 389).

암호화/SSL 인증서: (선택 사항) FMC 및 AD 서버 간의 연결을 암호화하려면 다음 문서를 참조하십시오.

[SSL/T를 통한 Microsoft AD 인증을 위한 FireSIGHT System의 인증 객체 확인...]



클릭 **테스트** AD 서버와의 FMC 연결을 확인하기 위해이제 **OK(확인)**를 클릭하여 컨피그레이션을 저장합니다.

3단계 영역 컨피그레이션을 수정합니다.

AD 서버의 통합 컨피그레이션을 수정하고 확인하려면 Realm Configuration(영역 컨피그레이션)으로 **이동합니다**.

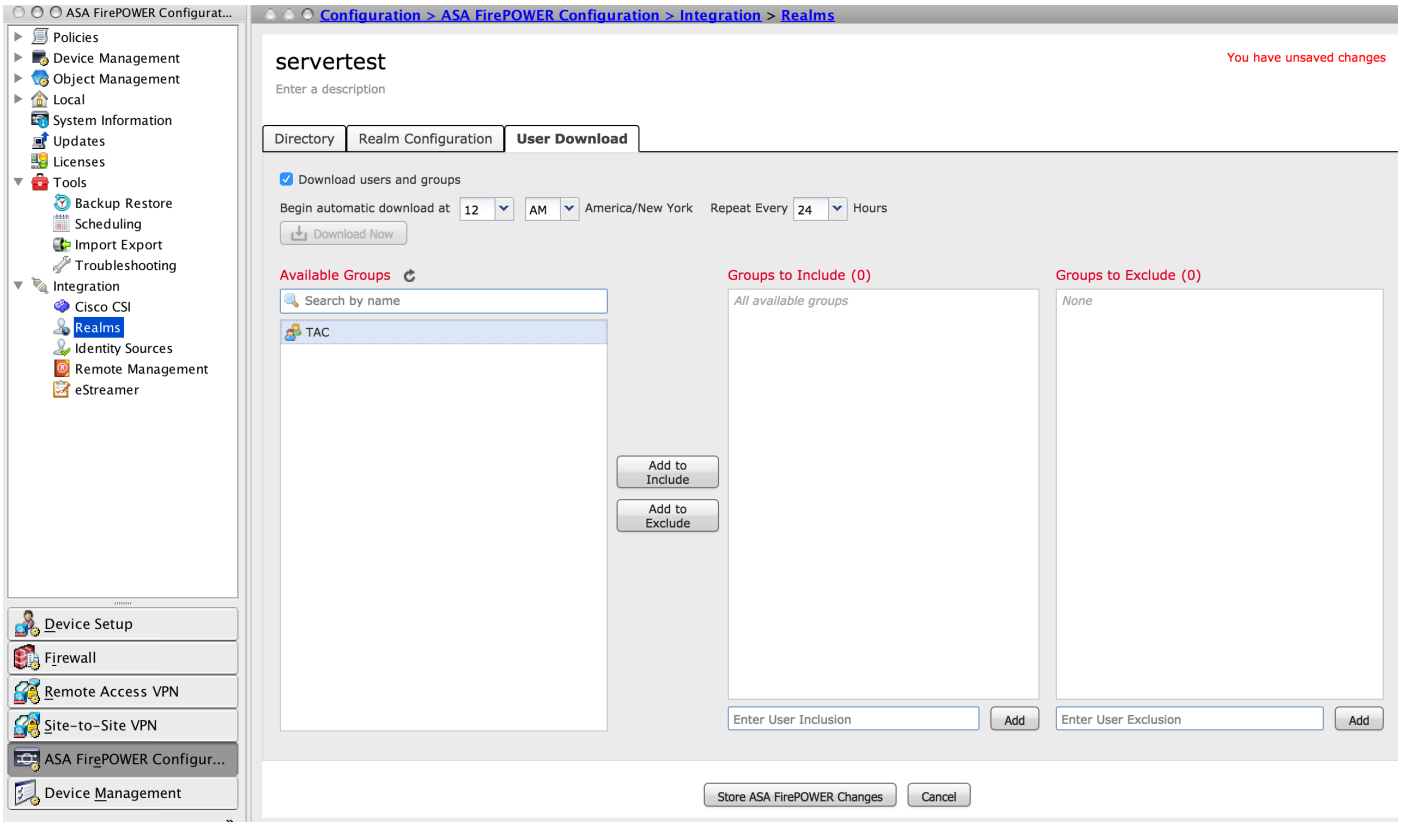
3.4단계 사용자 데이터베이스 다운로드

User **Download(사용자 다운로드)**로 이동하여 AD 서버에서 사용자 데이터베이스를 가져옵니다.

Download users and groups(**사용자 및 그룹 다운로드)를 다운로드하고** Firepower 모듈이 AD 서버에 연결하여 사용자 데이터베이스를 다운로드하는 빈도에 대한 시간 간격을 정의하려면 이 확인란을 활성화합니다.

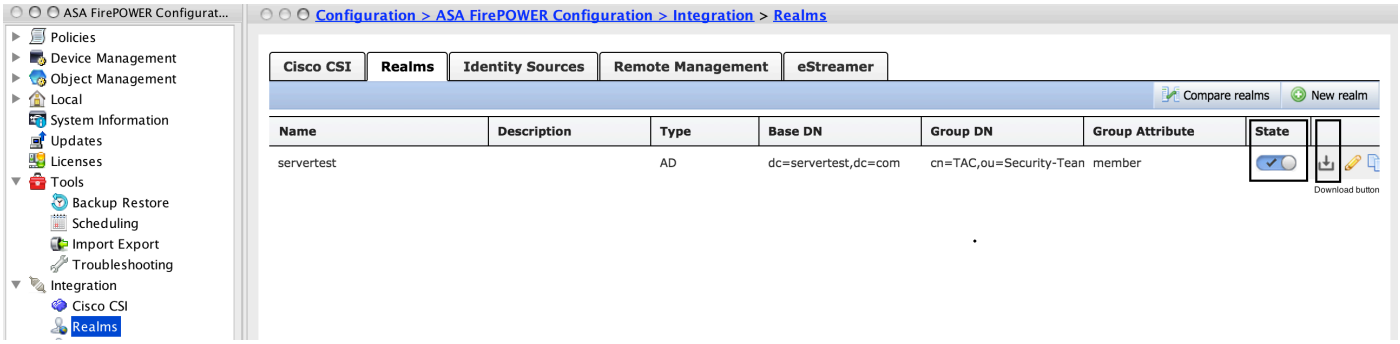
그룹을 선택하고 인증을 구성할 **Include** 옵션에 추가합니다.기본적으로 그룹을 포함하도록 선택하

지 않으면 모든 그룹이 선택됩니다.



Store **ASA Firepower Changes(ASA Firepower 변경 사항 저장)**를 클릭하여 영역 컨피그레이션을 저장합니다.

영역 상태를 활성화하고 다운로드 버튼을 클릭하여 이미지에 표시된 대로 사용자 및 그룹을 다운로드합니다.



4단계. ID 정책을 구성합니다.

ID 정책은 사용자 인증을 수행합니다.사용자가 인증하지 않으면 네트워크 리소스에 대한 액세스가 거부됩니다.이는 조직의 네트워크 및 리소스에 RBAC(Role-Based Access Control)를 적용합니다.

4.1단계 종속 포털(활성 인증)

Active Authentication(활성 인증)은 모든 연결을 허용할 사용자 ID를 식별하기 위해 브라우저에서 사용자 이름과 비밀번호를 요청합니다.브라우저는 인증 페이지를 제공하여 사용자를 인증하거나 NTLM 인증을 사용하여 자동으로 인증합니다. NTLM은 웹 브라우저를 사용하여 인증 정보를 보내고 받습니다.Active Authentication은 다양한 유형을 사용하여 사용자의 ID를 확인합니다.인증 유형은 다음과 같습니다.

1. **HTTP Basic: 이 방식에서는 브라우저가 사용자 자격 증명을 묻는 메시지를 표시합니다.**
2. **NTLM: NTLM은 windows 워크스테이션 자격 증명을 사용하고 웹 브라우저를 사용하여 Active Directory와 협상합니다.브라우저에서 NTLM 인증을 활성화해야 합니다.사용자 인증은 프롬프트를 표시하지 않고 투명하게 이루어집니다.사용자에게 단일 로그인 환경을 제공합니다.**
3. **HTTP 협상:**이 유형에서는 시스템이 NTLM을 사용하여 인증하려고 시도하며, 실패하면 센서가 HTTP 기본 인증 유형을 대체 방법으로 사용하고 사용자 자격 증명을 위한 대화 상자를 표시합니다.
4. **HTTP Response 페이지: HTTP 기본 유형과 유사하지만, 사용자 정의할 수 있는 HTML 형식으로 인증을 채우라는 메시지가 표시됩니다.**

각 브라우저에는 NTLM 인증을 활성화하는 특정 방법이 있으므로 NTLM 인증을 활성화하기 위해 브라우저 지침을 따를 수 있습니다.

라우티드 센서와 자격 증명을 안전하게 공유하려면 ID 정책에 자체 서명 서버 인증서 또는 공개적으로 서명된 서버 인증서를 설치해야 합니다.

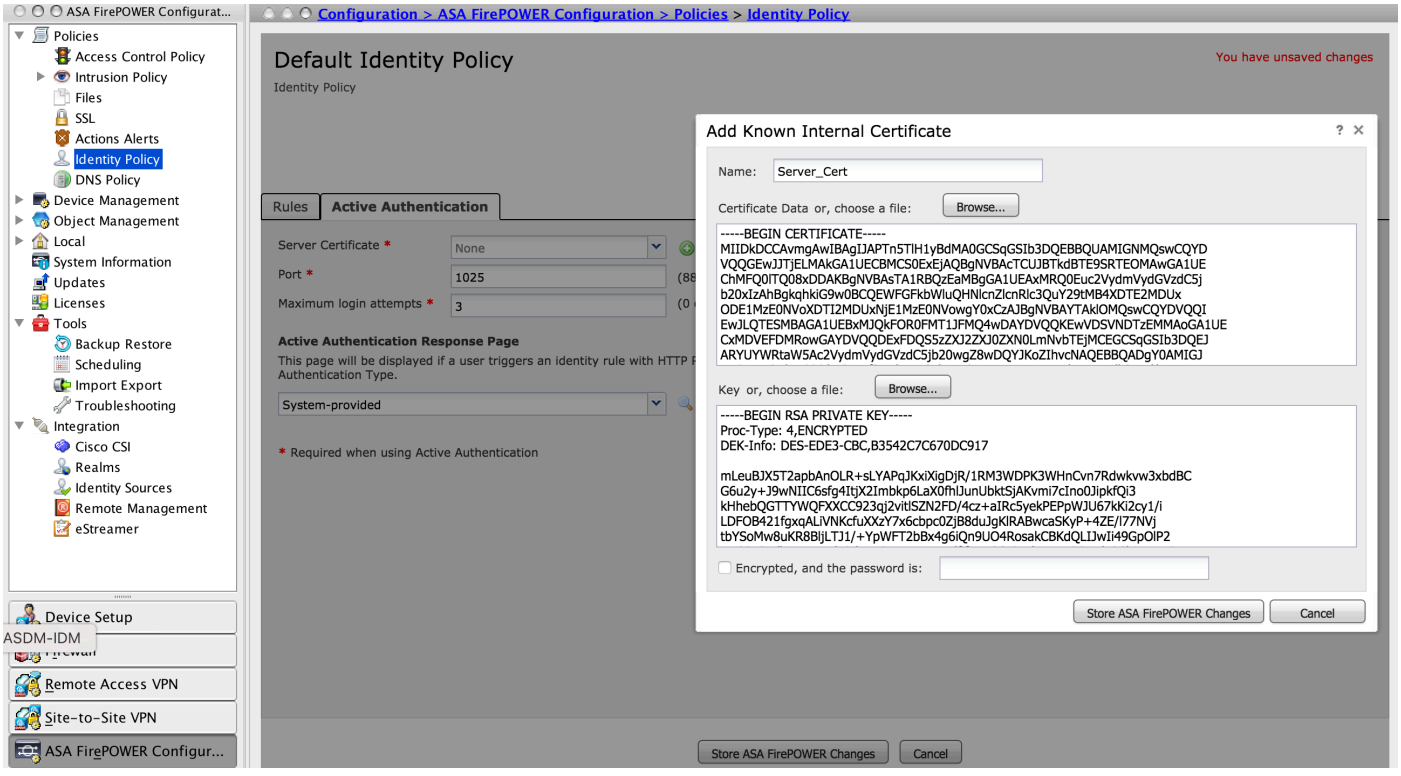
```
Generate a simple self-signed certificate using openSSL -

Step 1.    Generate the Private key
              openssl genrsa -des3 -out server.key 2048

Step 2.    Generate Certificate Signing Request (CSR)
              openssl req -new -key server.key -out server.csr

Step 3.    Generate the self-signed Certificate.
openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

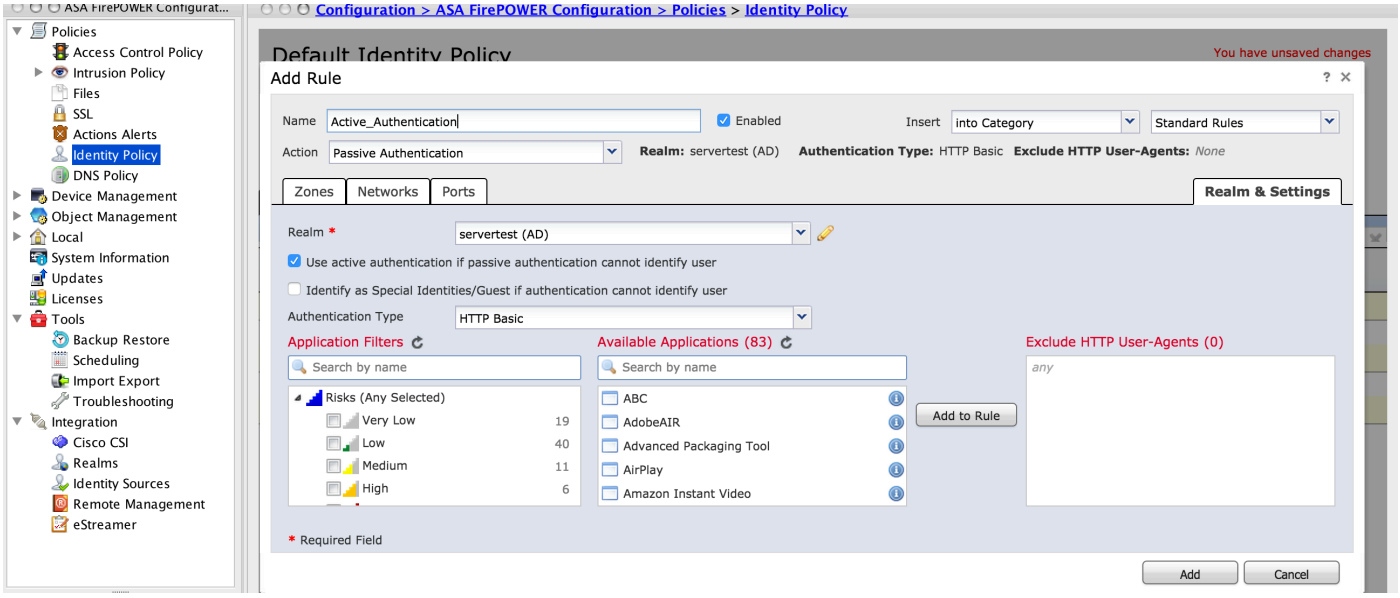
Configuration(컨피그레이션) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Policies(정책) > Identity Policy(ID 정책)로 이동합니다.**.이제 Active **Authentication** 탭으로 이동하고 **Server Certificate** 옵션에서 **아이콘(+)을 클릭합니다.** 다음 이미지에 표시된 것처럼 openSSL을 사용하여 이전 단계에서 생성한 인증서 및 개인 키를 업로드합니다.



이제 Add **rule(규칙 추가)**을 클릭하여 Rule(규칙)에 이름을 지정하고 작업을 Active

Authentication(**활성 인증**)으로 선택합니다.사용자 인증을 활성화할 소스/대상 영역, 소스/대상 네트워크를 정의합니다.

Realm **& Settings** 탭**으로** 이동합니다.이전 단계에서 구성한 드롭다운 목록에서 Realm을 선택하고 네트워크 환경에 가장 적합한 **Authentication Type**(인증 유형)을 드롭다운 목록에서 선택합니다.



4.2단계 종속 포털용 ASA 컨피그레이션

1단계. 검사를 위해 Sourcefire로 리디렉션될 흥미로운 트래픽을 정의합니다.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
ASA(config-cmap)# match access-list SFR_ACL
```

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

2단계. 종속 포털을 활성화하려면 ASA에서 이 명령을 구성합니다.

```
ASA(config)# captive-portal interface inside port 1025
```

: .

: TCP 1025 ID Active Authentication .

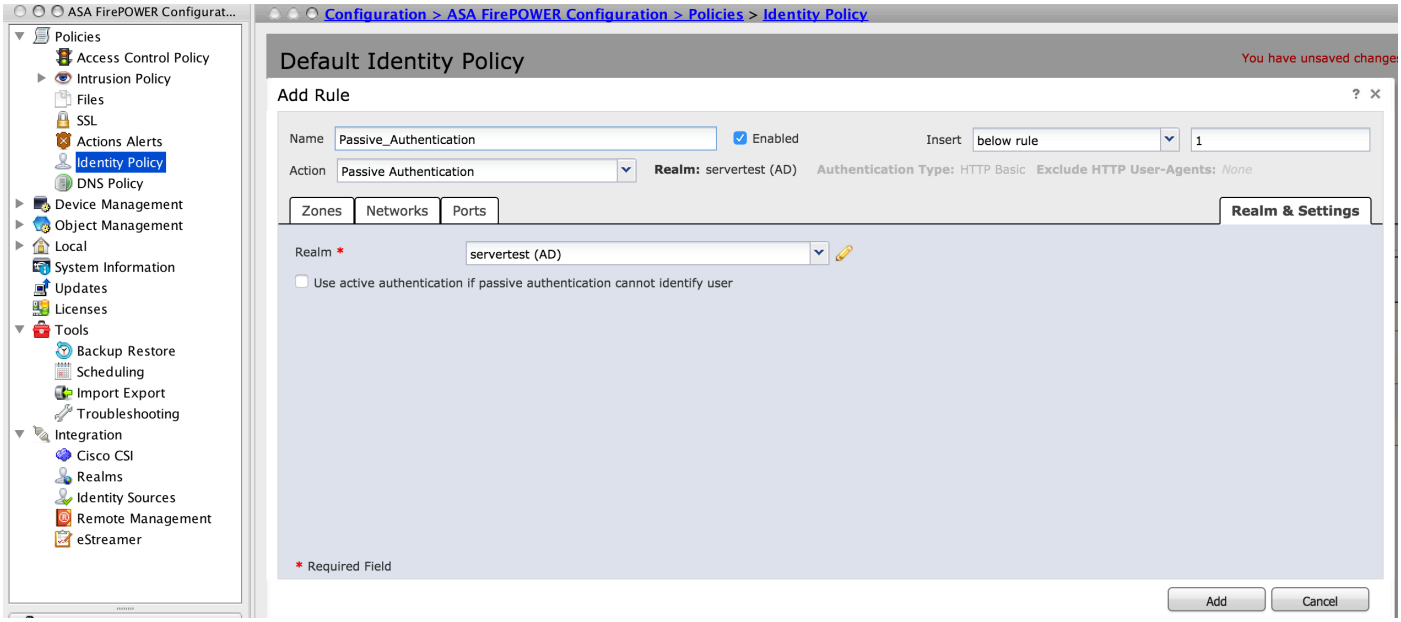
4.3단계 Single-Sign-On(수동 인증).

패시브 인증에서 도메인 사용자가 로그인하고 AD를 인증할 수 있는 경우 Firepower User Agent는 AD의 보안 로그에서 User-IP 매핑 세부사항을 폴링하고 이 정보를 Firepower Module과 공유합니다 .Firepower 모듈은 이러한 세부 정보를 사용하여 액세스 제어를 적용합니다.

패시브 인증 규칙을 구성하려면 Add **rule(규칙 추가)**을 클릭하여 규칙에 이름을 지정한 다음 Action as **Passive Authentication(패시브 인증으로 작업)**을 **선택합니다**.사용자 인증을 활성화할 소스/대상 영역, 소스/대상 네트워크를 정의합니다.

다음으로 이동 **영역 및 설정** 탭.다음을 선택합니다. **영역** 이전 단계에서 구성한 드롭다운 목록에서 선택합니다.

패시브 **인증**이 이미지에 표시된 것처럼 **사용자 ID를 식별할 수 없는 경우** 이에서 폴백 방법을 **액티브 인증으로** 선택할 수 있습니다.

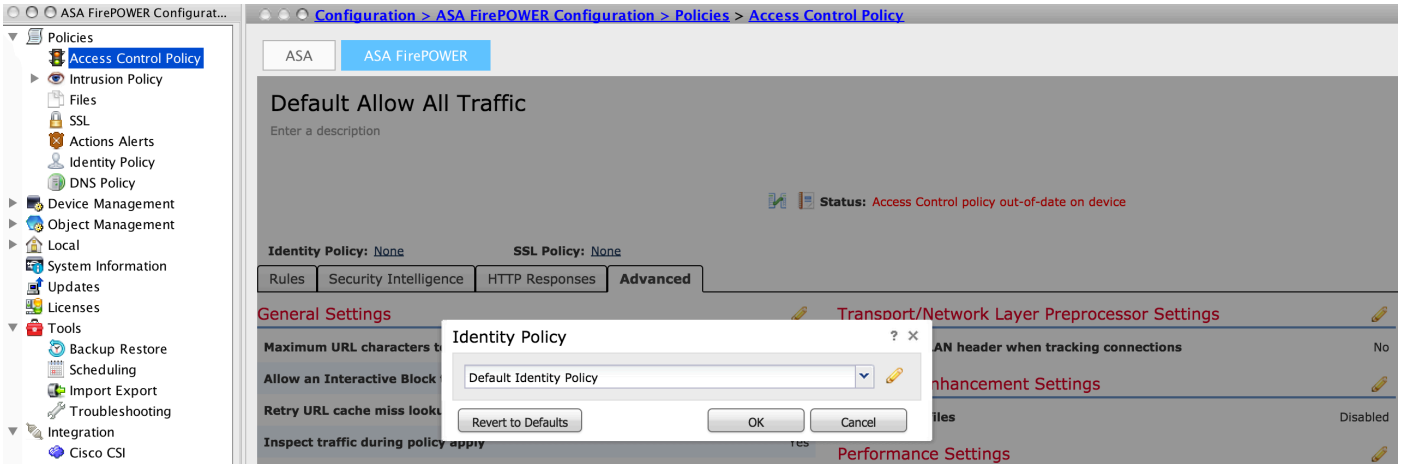


이제 Store **ASA Firepower Changes(ASA Firepower 변경 사항 저장)**를 클릭하여 ID 정책의 컨피그레이션을 저장합니다.

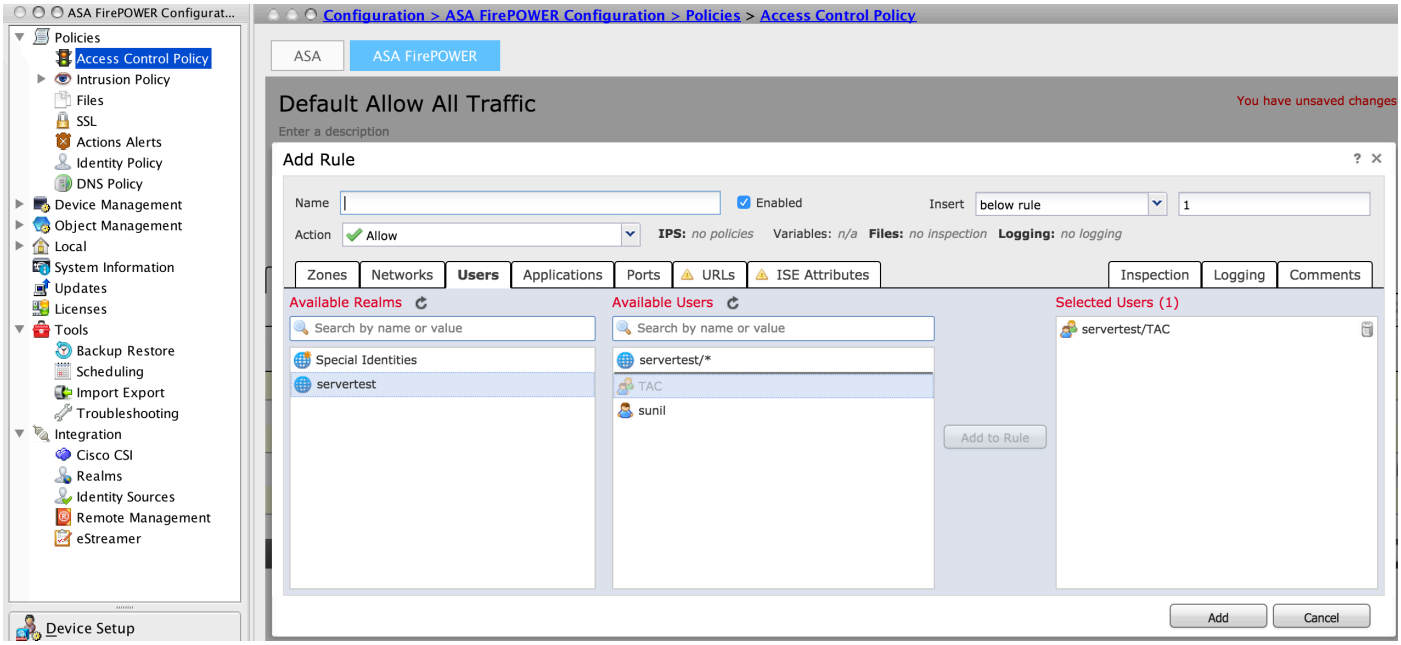
5단계. 액세스 제어 정책을 구성합니다.

Configuration(컨피그레이션) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Policies(정책) > Access Control Policy(액세스 제어 정책)로 이동합니다.**

ID **정책**(왼쪽 상단 모서리)을 클릭하고 드롭다운 목록에서 이전 단계에서 구성한 ID 정책을 선택하고 **OK(확인)를** 클릭합니다(이 이미지에 표시된 대로).



클릭 **규칙 추가** 새 규칙을 추가하려면 **사용자** 이 이미지에 표시된 대로 액세스 제어 규칙을 적용할 사용자를 선택하고 Add(추가)를 클릭합니다..



클릭 **ASA Firepower 변경 사항 저장** 액세스 제어 정책의 컨피그레이션을 저장합니다.

6단계. 액세스 제어 정책을 구축합니다.

액세스 제어 정책을 구축해야 합니다.정책을 적용하기 전에 모듈에 액세스 제어 정책이 오래되었다는 표시가 나타납니다. 센서에 변경 사항을 배포하려면 **[배포]**를 클릭하고 **[FirePOWER 변경 사항 배포] 옵션**을 선택한 다음 팝업 창에서 [구축]을 클릭합니다.

> **참고:**버전 5.4.x에서 센서에 액세스 정책을 적용하려면 Apply ASA FirePOWER Changes(ASA FirePOWER 변경 사항 적용)를 클릭해야 합니다.

> **참고:**Monitoring(모니터링) > ASA Firepower Monitoring(ASA Firepower 모니터링) > Task Status(작업 상태)로 이동합니다.구성 변경 적용 작업을 완료해야 합니다.

7단계. 사용자 이벤트 모니터링

Monitoring(**모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Real-Time Eventing(실시간 이벤트)**으로 이동하여 사용자가 사용 중인 트래픽 유형을 모니터링합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Analysis **> Users(사용자)**로 이동하여 트래픽 흐름과 연결된 User authentication/Authentication type/User-IP mapping/access 규칙을 확인합니다.

Firepower Module과 사용자 에이전트 간 연결(수동 인증)

Firepower Module은 사용자 에이전트에서 사용자 작업 로그 데이터를 수신하기 위해 TCP 포트 3306을 사용합니다.

Firepower 모듈의 서비스 상태를 확인하려면 FMC에서 이 명령을 사용합니다.

```
admin@firepower:~$ netstat -tan | grep 3306
```

FMC에서 패킷 캡처를 실행하여 사용자 에이전트와의 연결을 확인합니다.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

FMC와 Active Directory 간 연결

Firepower 모듈은 Active Directory에서 사용자 데이터베이스를 검색하기 위해 TCP 포트 389를 사용합니다.

Firepower 모듈에서 패킷 캡처를 실행하여 Active Directory와의 연결을 확인합니다.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

영역 구성에 사용된 사용자 자격 증명에 AD의 사용자 데이터베이스를 가져올 수 있는 충분한 권한이 있는지 확인합니다.

영역 컨피그레이션을 확인하고 사용자/그룹이 다운로드되고 사용자 세션 시간 초과가 올바르게 구성되었는지 확인합니다.

Monitoring ASA Firepower Monitoring Task Status(ASA Firepower 모니터링 작업 상태 모니터링)로 이동하고 이 이미지와 같이 작업 사용자/그룹 다운로드가 성공적으로 완료되었는지 확인합니다.

ASA와 엔드 시스템 간의 연결(활성 인증)

활성 인증, Firepower module Identity policy 및 ASA(captive-portal 명령)에서 인증서와 포트가 올바르게 구성되었는지 확인합니다. 기본적으로 ASA 및 Firepower 모듈은 액티브 인증을 위해 TCP 포트 885에서 수신합니다.

활성 규칙 및 적중 횟수를 확인하려면 ASA에서 이 명령을 실행합니다.

```
ASA# show asp table classify domain captive-portal

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

정책 구성 및 정책 구축

Realm(영역), Authentication(인증) 유형, User Agent(사용자 에이전트) 및 Action(작업) 필드가 ID 정책에서 올바르게 구성되었는지 확인합니다.

ID 정책이 액세스 제어 정책과 올바르게 연결되었는지 확인합니다.

Monitoring(모니터링) > ASA Firepower Monitoring(ASA Firepower 모니터링) > Task Status(작업 상태)로 이동하고 Policy Deployment(정책 구축)가 성공적으로 완료되었는지 확인합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems
- Single-Sign-On 및 종속 포털 인증을 위해 Firepower Appliance와 Active Directory 통합 구성