ISE 및 FirePOWER Integration for Identity Services 문제 해결

목차

소개

이 문서에서는 Cisco NGIPS(Next Generation Intrusion Prevention System)에서 TrustSec 인식 정책을 구성하고 트러블슈팅하는 방법에 대해 설명합니다.NGIPS 버전 6.0은 ISE(Identity Services Engine)와의 통합을 지원하므로 ID 기반 인식 정책을 구축할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA(Adaptive Security Appliance) VPN 컨피그레이션
- Cisco AnyConnect Secure Mobility Client 컨피그레이션
- Cisco FirePower Management Center 기본 구성
- Cisco ISE 컨피그레이션
- Cisco TrustSec 솔루션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Microsoft Windows 2012 CA(Certificate Authority)
- Cisco ASA 버전 9.3
- Cisco ISE 소프트웨어 버전 1.4
- Cisco AnyConnect Secure Mobility Client 버전 4.2
- Cisco FMC(FirePower Management Center) 버전 6.0
- Cisco FirePower NGIPS 버전 6.0

구성

FMC(FirePower Management Center)는 FirePower용 관리 플랫폼입니다.ISE 통합과 관련된 두 가지 유형의 기능이 있습니다.

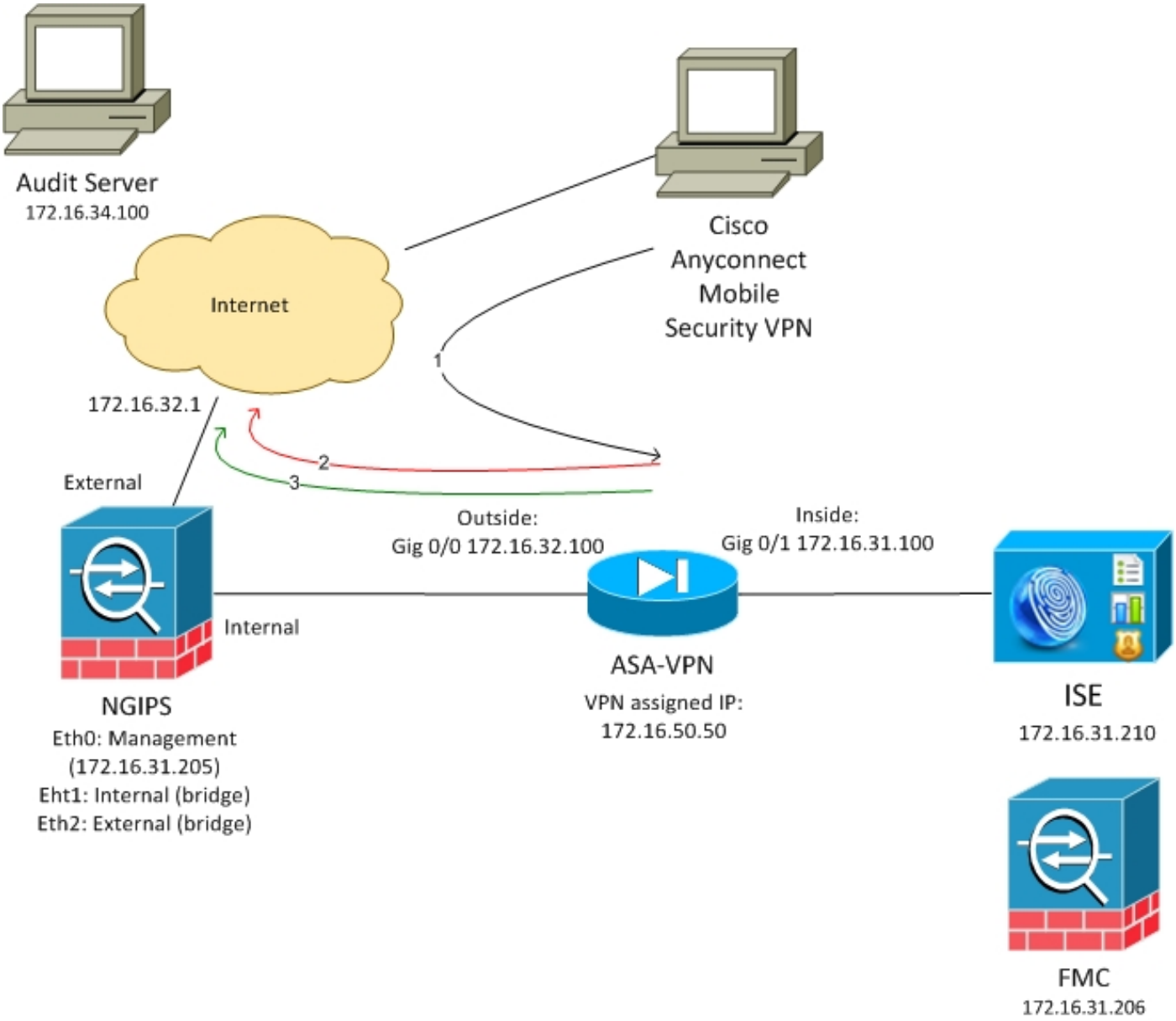
- 리미디에이션 - FMC가 ISE를 통해 공격자를 격리할 수 있습니다. ISE는 액세스 디바이스에서 권한 부여 상태를 동적으로 변경하여 제한된 네트워크 액세스를 제공합니다.이 솔루션에는 두 가지 세대의 제품이 있습니다.

  1. ISE에 대한 EPS(Endpoint Protection Service) API 호출을 사용하는 레거시 Perl 스크립트
  2. ISE에 대한 pxGrid 프로토콜 호출을 사용하는 새로운 모듈(이 모듈은 버전 5.4에서만 지원됨 - 6.0에서는 지원되지 않음, 6.1에서 기본 지원 예정)

- Policy(정책) - FMC가 TrustSec SGT(Security Group Tag)를 기반으로 정책을 구성할 수 있습니다.

이 문서에서는 두 번째 기능에 대해 중점적으로 설명합니다.리미디에이션 예에서는 참조 섹션을 참조하십시오.

네트워크 다이어그램



FMC는 두 가지 규칙을 포함하는 액세스 제어 정책으로 구성됩니다.

- 맞춤형 URL을 사용하는 HTTP 트래픽 거부(공격-url)
- 사용자 지정 URL(공격 URL)이 있는 HTTP 트래픽을 허용하지만 사용자가 ISE에 의해 감사(9) SGT 태그에 할당된 경우에만 허용

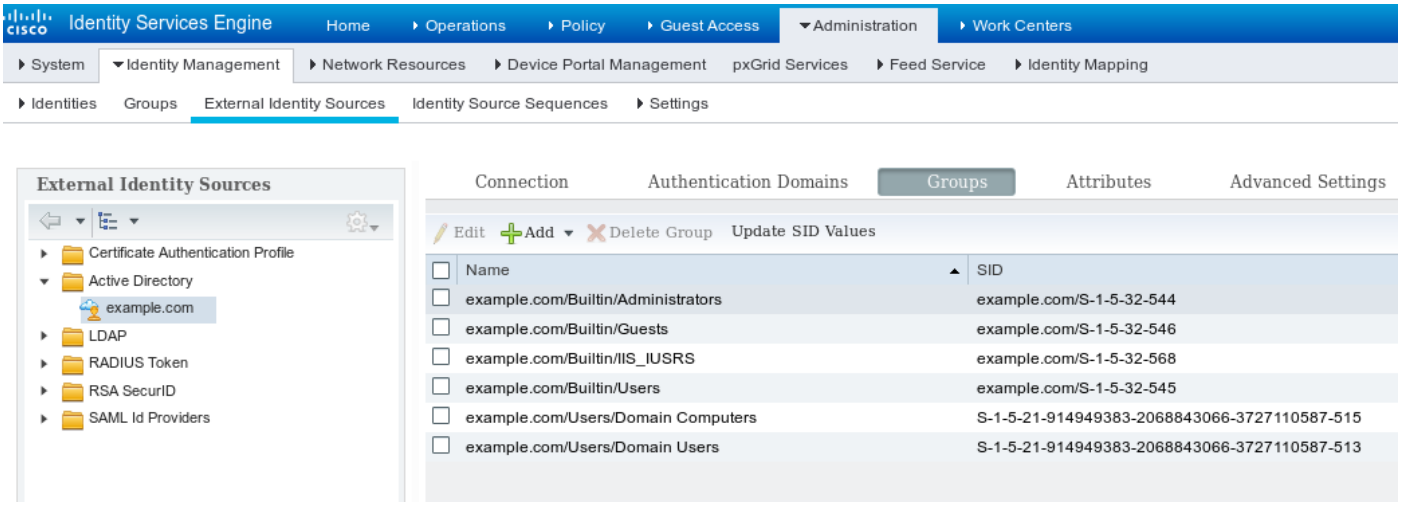
ISE는 Administrator 그룹에 속하고 네트워크 액세스를 위해 ASA-VPN 디바이스를 사용하는 모든 Active Directory 사용자에게 감사 태그를 할당하기로 결정합니다.

사용자는 ASA에서 VPN 연결을 통해 네트워크에 액세스합니다.그런 다음 사용자는 URL 공격 URL을 사용하여 감사된 서버에 액세스를 시도하지만 감사 SGT 그룹에 할당되지 않았으므로 실패합니다.이를 수정하면 연결에 성공합니다.

ISE

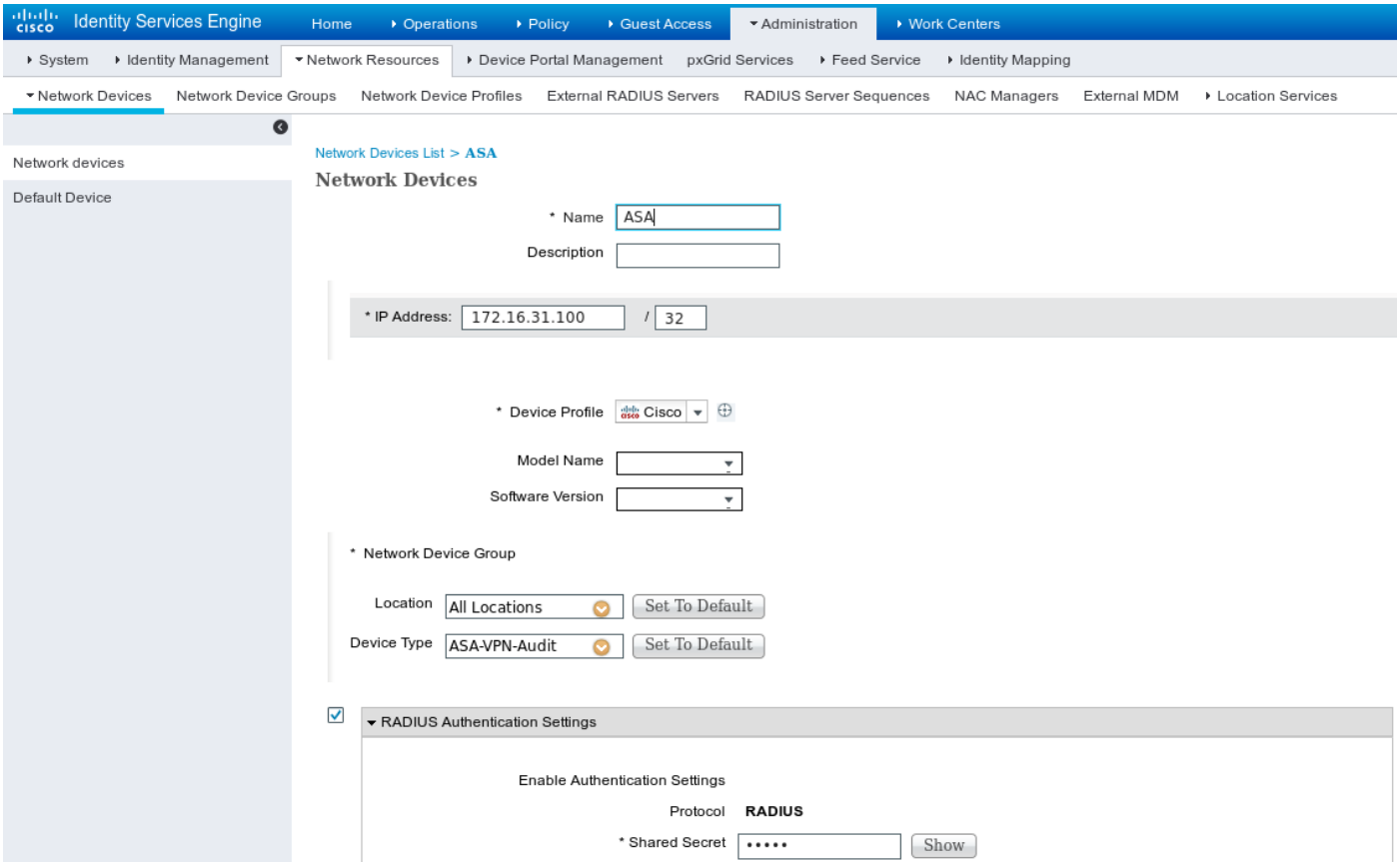
Active Directory

AD 통합을 구성해야 하며 올바른 그룹을 가져와야 합니다(권한 부여 규칙 조건에 Administrators 그룹이 사용됨).



네트워크 액세스 디바이스

ASA가 네트워크 디바이스로 추가됩니다.다음 이미지에 표시된 대로 사용자 지정 그룹 ASA-VPN-Audit가 사용됩니다.



pxGrid 및 MnT용 인증서

FMC는 ISE에서 두 서비스를 모두 사용합니다.

- SGT 및 프로파일링 데이터 쿼리를 위한 pxGrid
- 벌크 세션 다운로드를 위한 모니터링 및 보고(MnT)

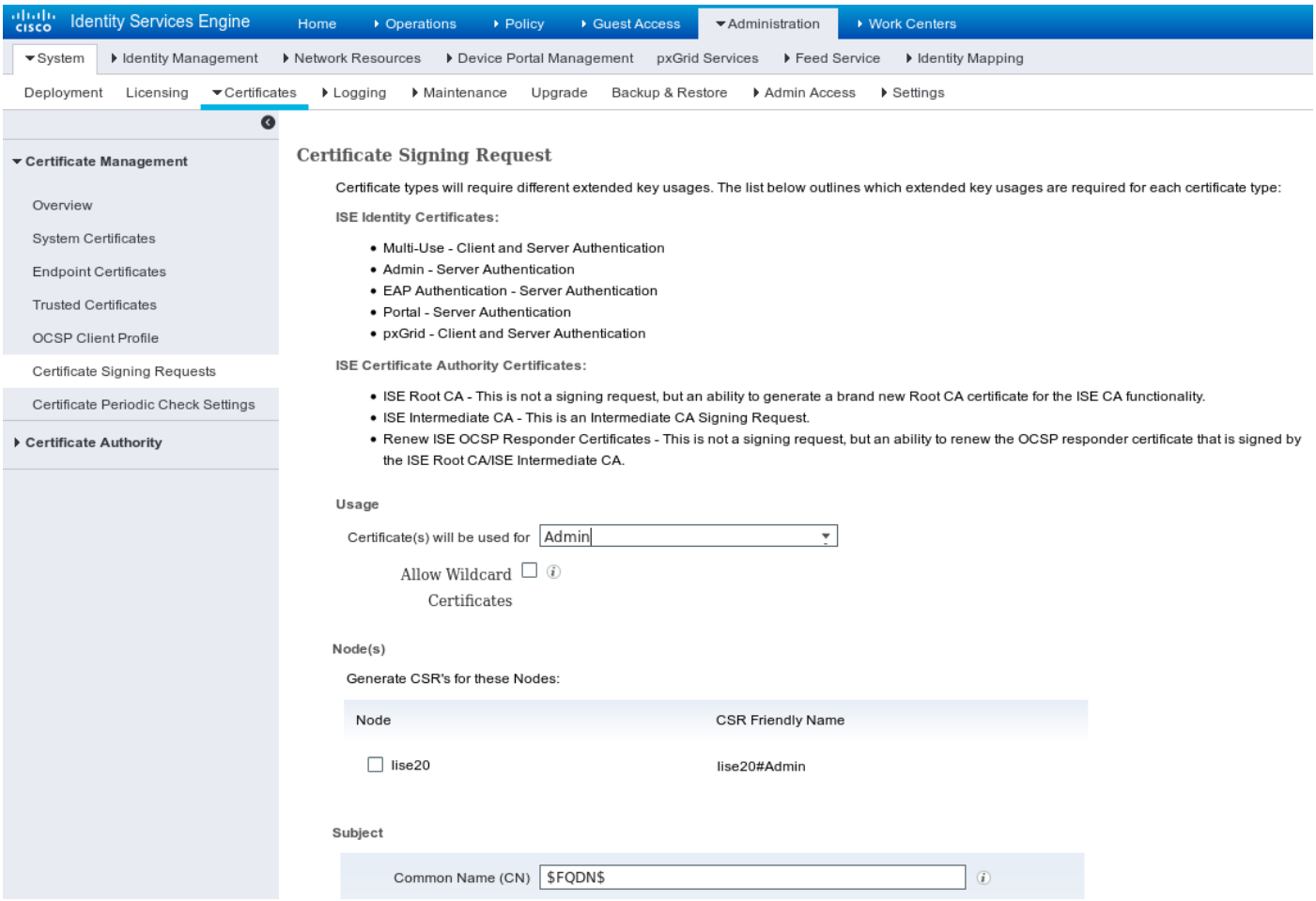
이렇게 하면 FMC에서 인증된 세션의 IP 주소, 사용자 이름 및 SGT 태그를 알 수 있으므로 MnT 가용성이 매우 중요합니다.이에 따라 올바른 정책을 적용할 수 있습니다.NGIPS는 ASA와 같이 기본적으로 SGT 태그(인라인 태깅)를 지원하지 않습니다.그러나 ASA와는 반대로, 숫자 대신 SGT 이름

을 지원합니다.

이러한 요구 사항 때문에 ISE와 FMC는 서로 다른 서비스(인증서)를 신뢰해야 합니다. MnT는 서버 측 인증서만 사용하며 pxGrid는 클라이언트와 서버측 인증서를 모두 사용합니다.

Microsoft CA는 모든 인증서에 서명하는 데 사용됩니다.

MnT(관리자 역할) ISE는 다음 이미지에 표시된 대로 CSR(certificate signing request)을 생성해야 합니다.



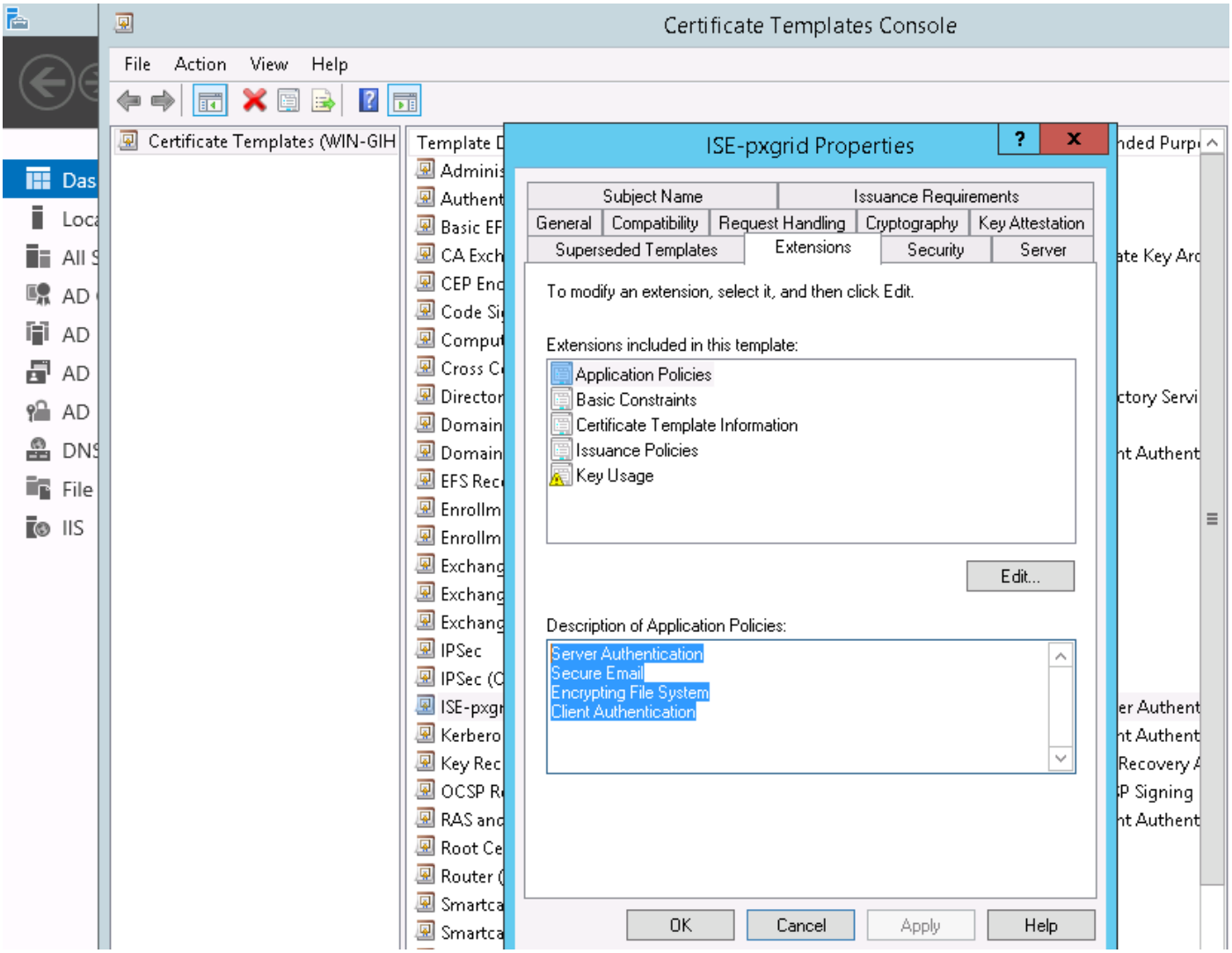
Microsoft CA에서 서명한 후에는 **Bind Certificate** 옵션을 통해 가져와야 합니다.

pxGrid 서비스의 경우 유사한 프로세스를 따라야 합니다.옵션 **에 사용되는 인증서는 pxGrid를** 선택해야 합니다.

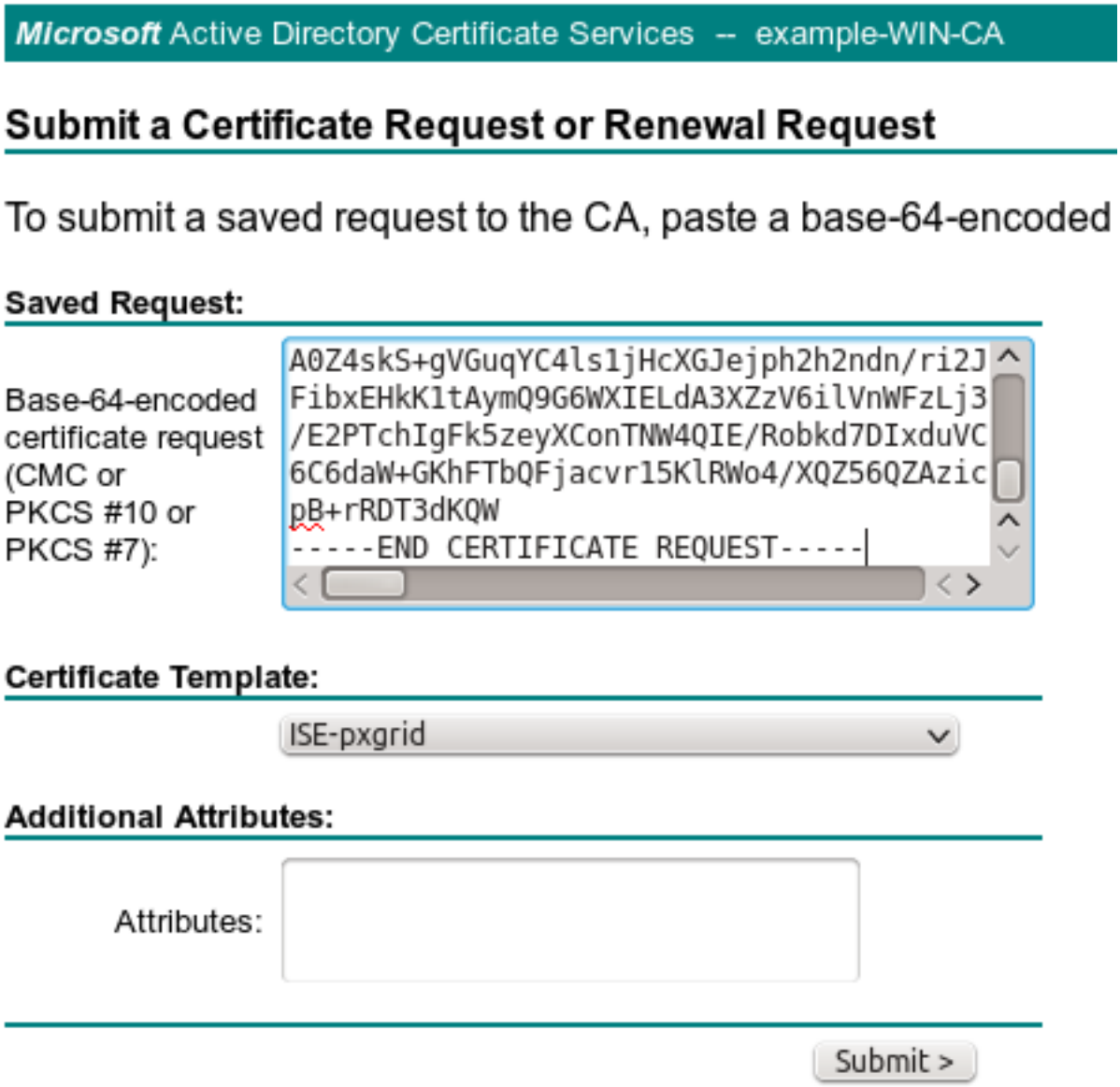
동일한 주체 이름을 가진 두 개의 인증서는 사용할 수 없으므로 OU 또는 O 섹션(예: pxGrid)에 다른 값을 추가할 수 있습니다.

> **참고:**ISE와 FMC의 모든 FQDN(Fully Qualified Domain Name)에 대해 올바른 DNS 레코드가 DNS 서버에 구성되어 있는지 확인하십시오.

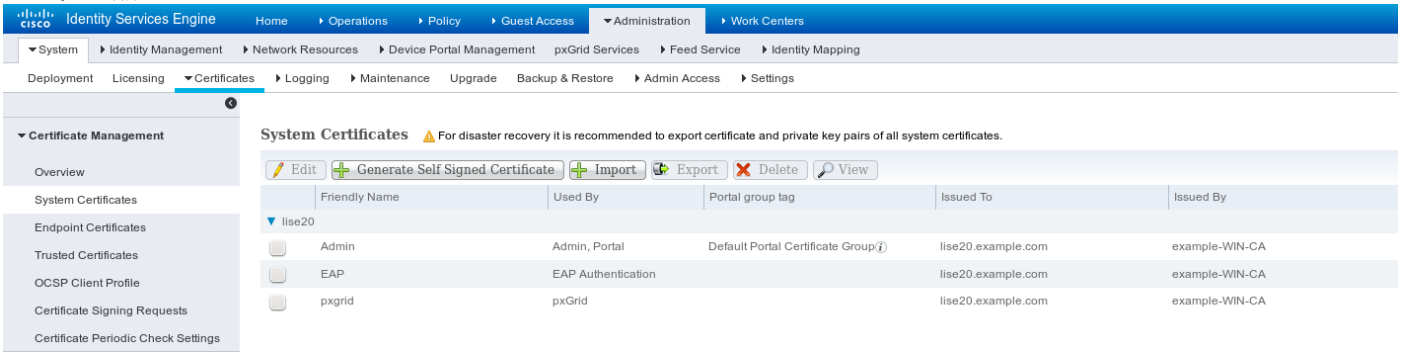
관리 인증서와 pxGrid 인증서의 유일한 차이점은 서명 프로세스입니다.pxGrid 인증서에는 Microsoft CA의 클라이언트 및 서버 인증 사용자 지정 템플릿에 대한 확장 키 사용 옵션이 있어야 하므로 다음 작업에 사용할 수 있습니다.



Microsoft 웹 서비스를 사용하여 pxGrid CSR에 서명하는 방법은 다음 이미지에 나와 있습니다.

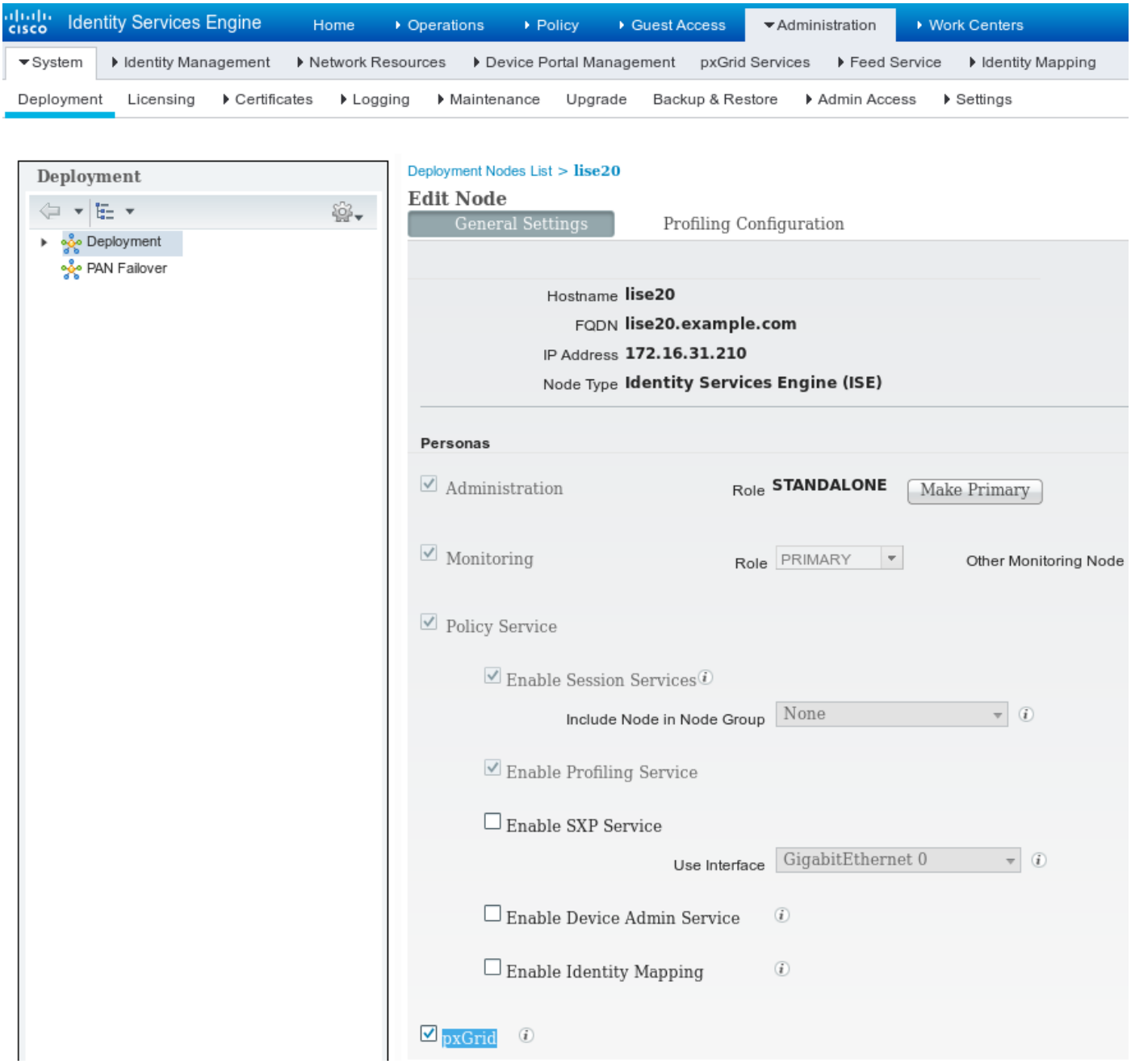


끝 ISE에는 다음 이미지에 표시된 대로 신뢰할 수 있는 CA(Microsoft)가 서명한 Admin 및 pxGrid 인증서가 있어야 합니다.

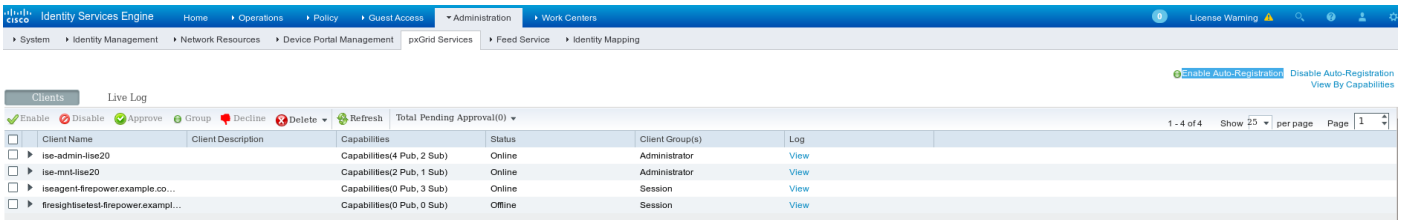


pxGrid 서비스

다음 이미지와 같이 특정 노드에 대한 올바른 인증서 pxGrid 역할을 활성화해야 합니다.



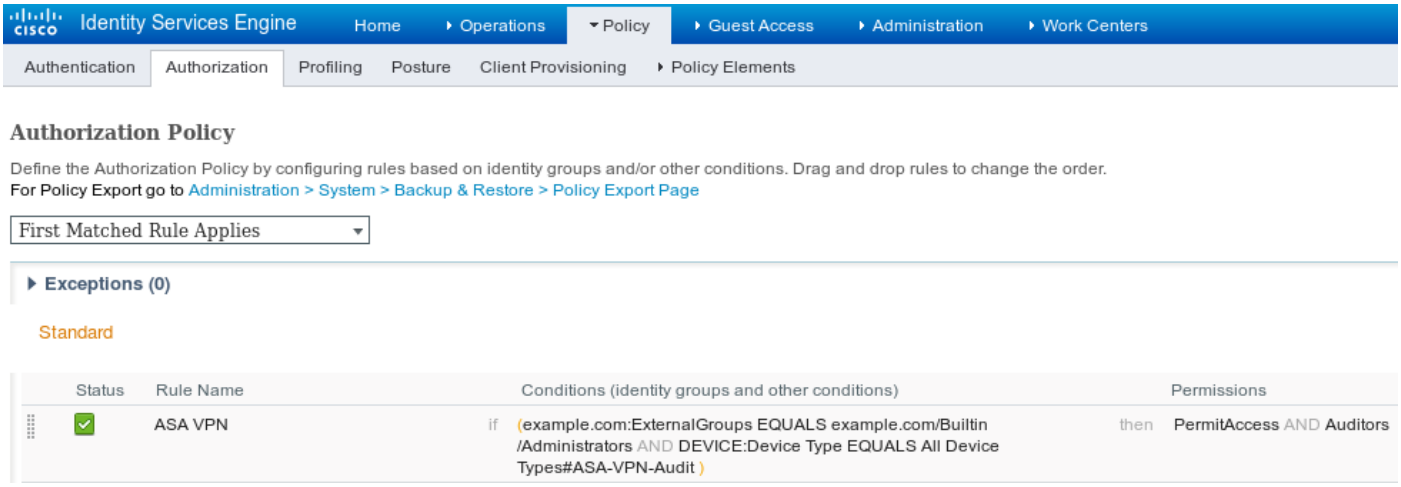
그리고 자동 승인을 사용하도록 설정해야 합니다.



권한 부여 정책

기본 인증 정책이 사용됩니다(로컬 사용자를 찾을 수 없는 경우 AD 조회가 수행됩니다).

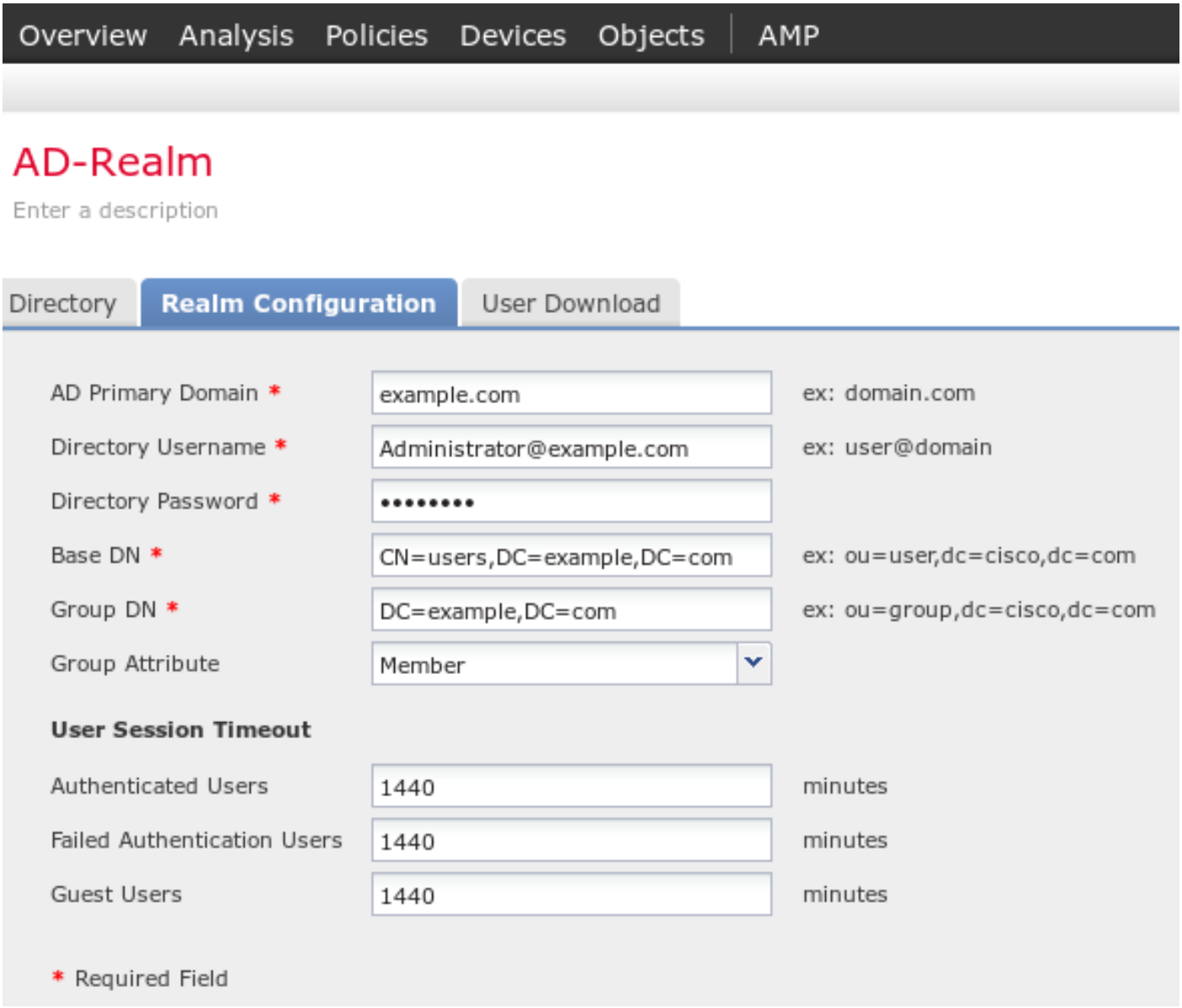
전체 네트워크 액세스를 제공하도록 권한 부여 정책이 구성되었습니다(권한:ASA-VPN을 통해 인증되고 Active Directory 그룹 관리자에 속하는 사용자를 위한 PermitAccess(허용) - 해당 사용자의 SGT 태그 감사자가 반환됩니다.



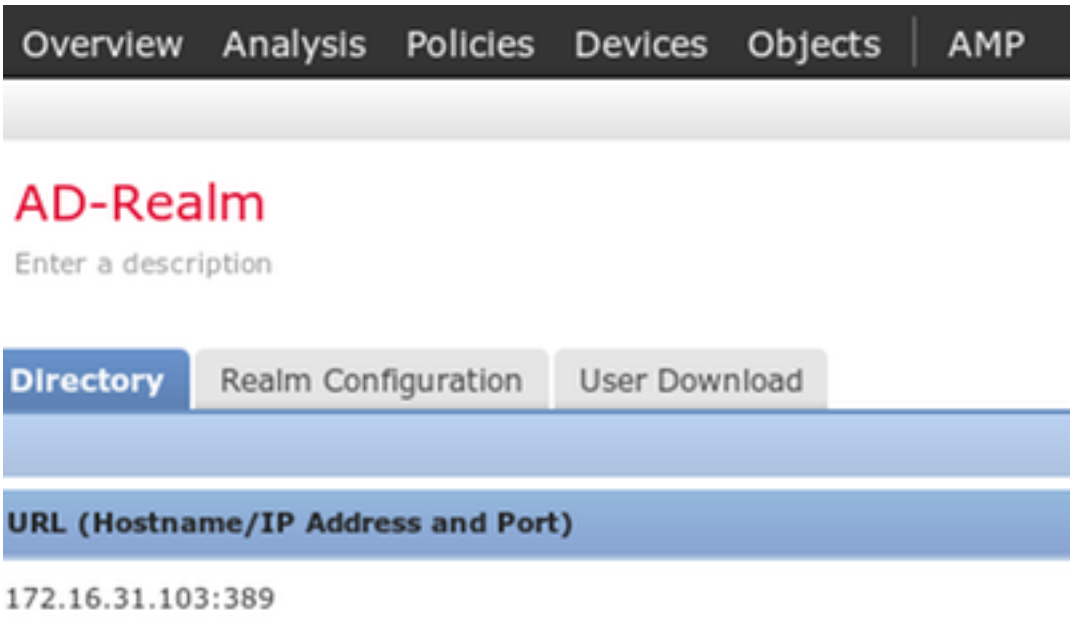
FMC

Active Directory 영역

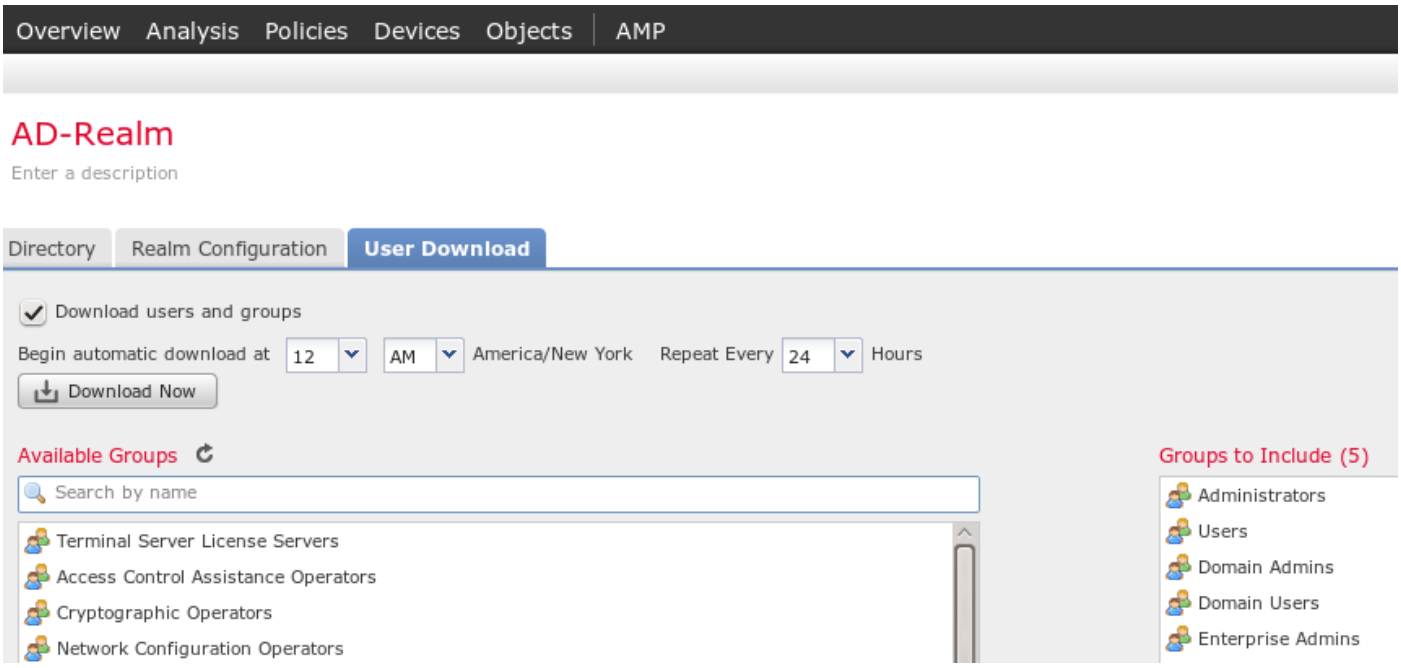
ISE 통합 작업을 수행하려면 영역 컨피그레이션이 필요합니다(ID 정책을 사용하고 수동으로 인증된 사용자의 그룹 멤버십을 검색하려면). Active Directory 또는 LDAP(Lightweight Directory Access Protocol)에 대해 영역을 구성할 수 있습니다. 이 예에서는 AD를 사용하고 있습니다.**System > Integration > Realm**에서:



표준 디렉터리 설정이 사용됩니다.

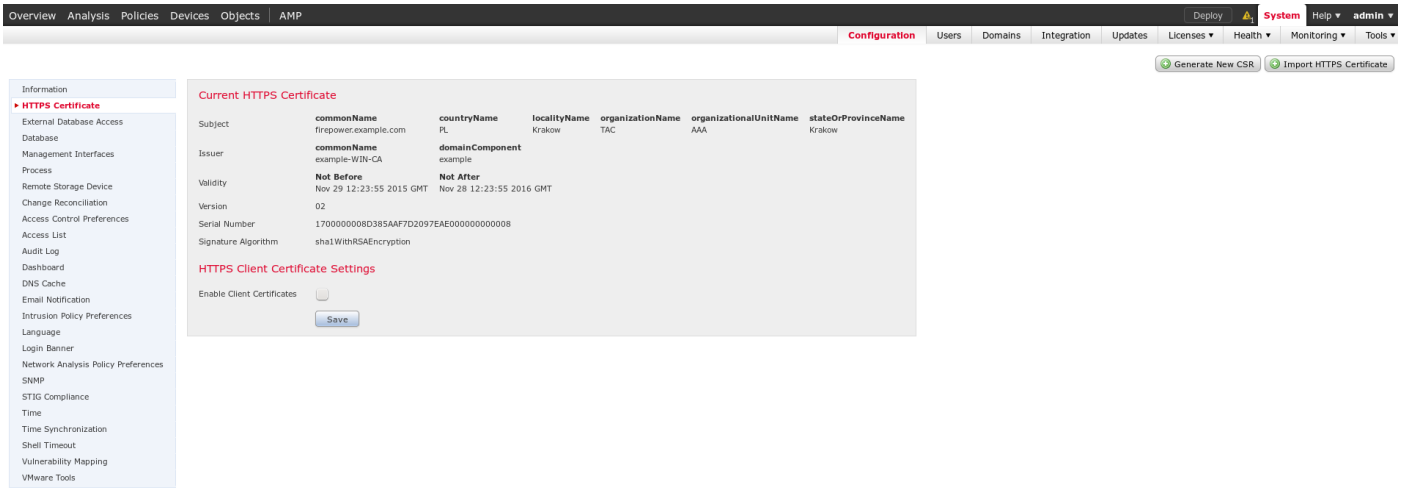


그리고 일부 AD 그룹이 검색됩니다(액세스 제어 규칙에서 추가 조건으로 사용).

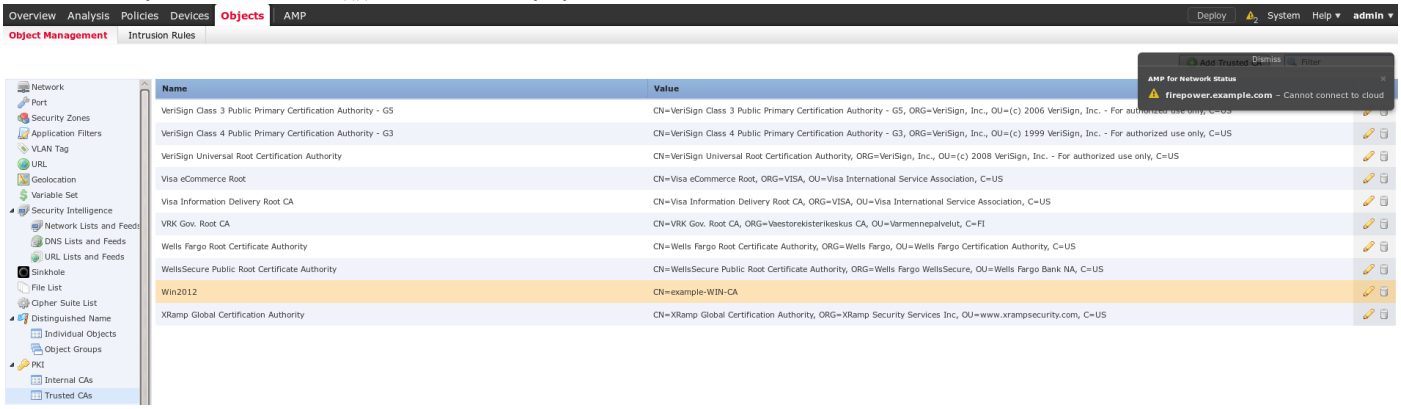


관리자 및 pxGrid용 인증서

필수 사항은 아니지만 관리자 액세스를 위해 CSR을 생성하는 것이 좋습니다.신뢰할 수 있는 AD를 사용하여 CSR에 서명하고 다음 이미지에 표시된 대로 서명된 인증서를 다시 가져옵니다.



CA 인증서를 신뢰할 수 있는 저장소에 추가해야 합니다.

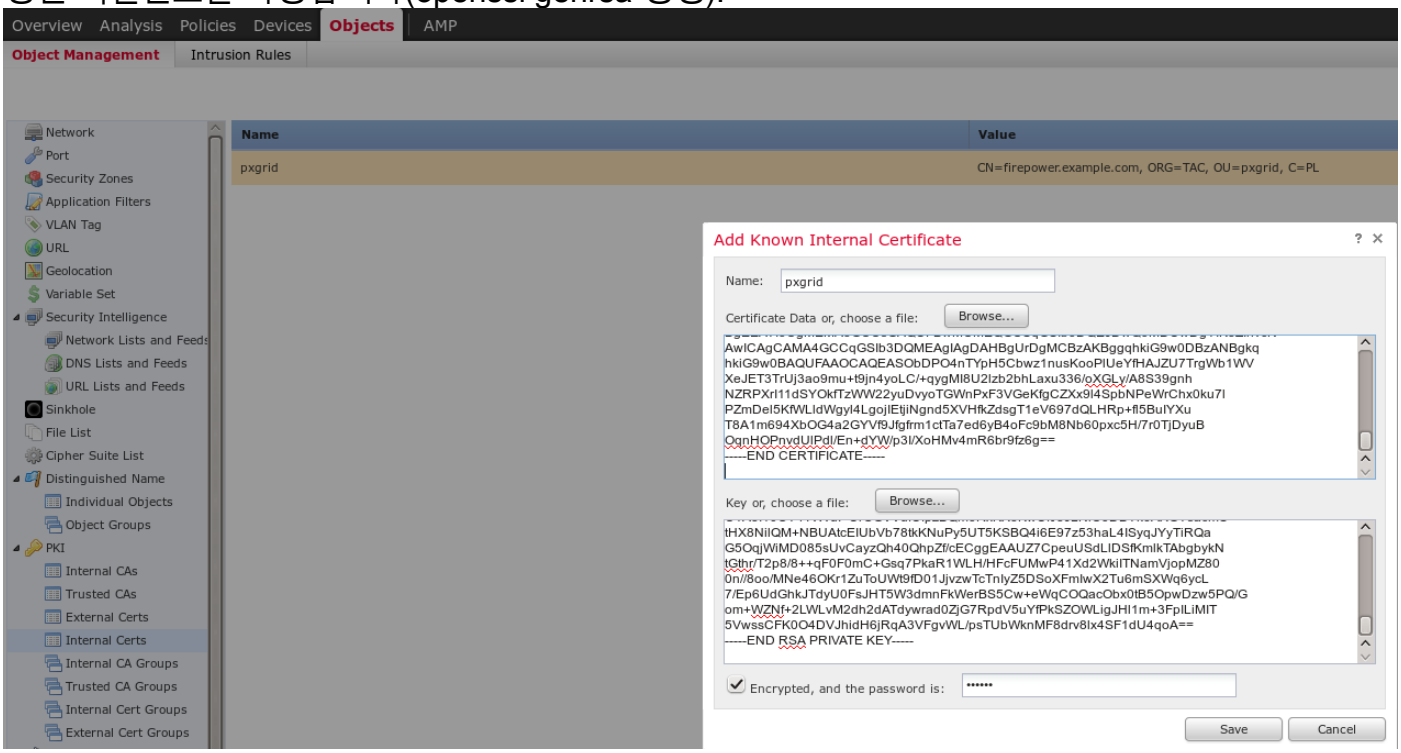


마지막 단계는 ISE pxGrid 서비스에 권한을 부여하기 위해 FMC에서 사용하는 pxGrid 인증서를 생성하는 것입니다.CSR CLI를 생성하려면(또는 openssl 툴을 사용하는 기타 외부 시스템)을 사용해

야 합니다.

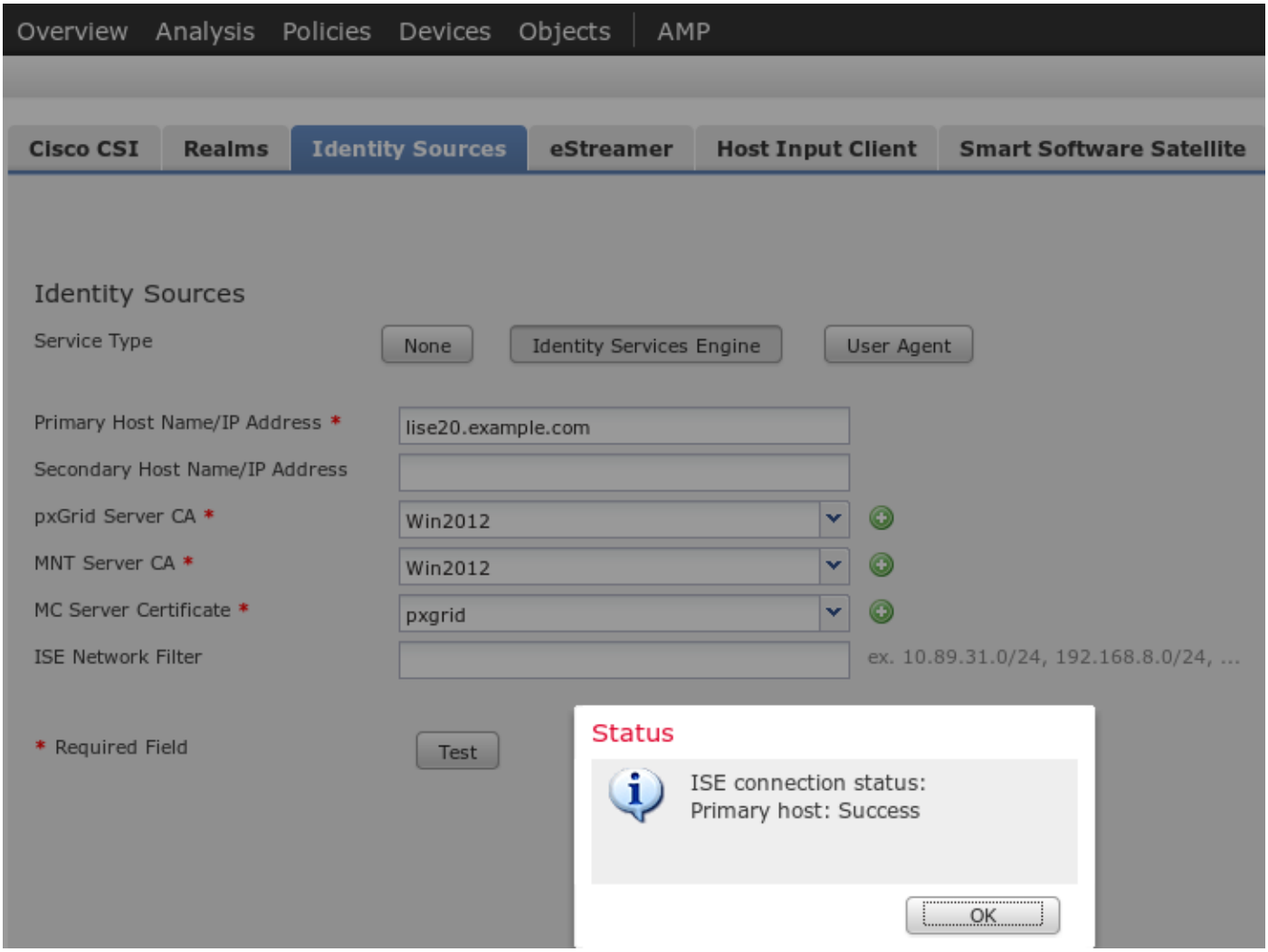
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#
root@firepower:~# openssl req -new -key fire.key -out fire.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Code []:PL
State or Province Name []:
Locality Name []:
Organization Name []:Cisco
Organizational Unit Name []:TAC
Common Name []:firepower.example.com
Email Address []:
root@firepower:~#
```

fire.csr을 생성한 후 Microsoft CA(pxGrid 템플릿)를 사용하여 서명합니다. 개인 키(fire.key) 및 서명된 인증서(fire.pem)를 FMC 내부 인증서 저장소로 다시 가져옵니다.개인 키의 경우 키 생성 중에 설정된 비밀번호를 사용합니다(openssl genrsa 명령).



ISE 통합

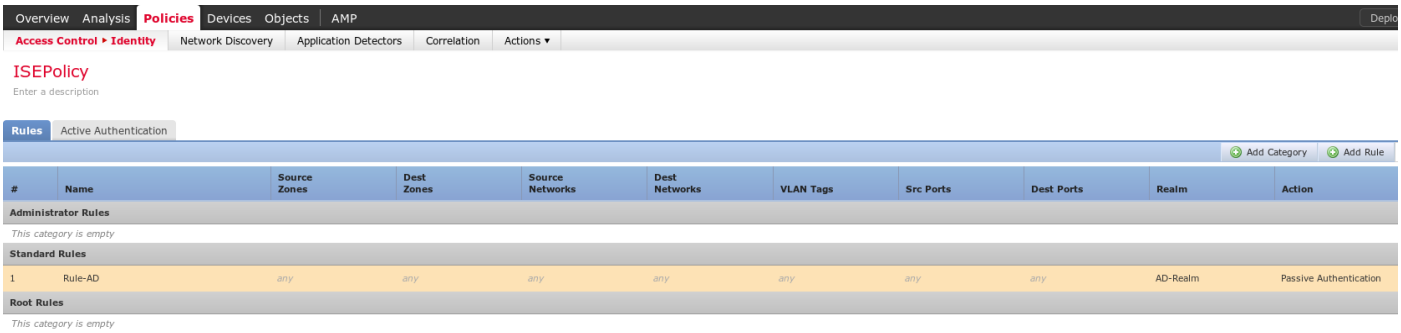
모든 인증서가 설치되면 **System > Integration**에서 ISE 통합을 **구성합니다**.



가져온 CA를 pxGrid 및 MnT 서비스 인증서 검증에 모두 사용합니다.MC(Management Console)의 경우 pxGrid에 대해 생성된 내부 인증서를 사용합니다.

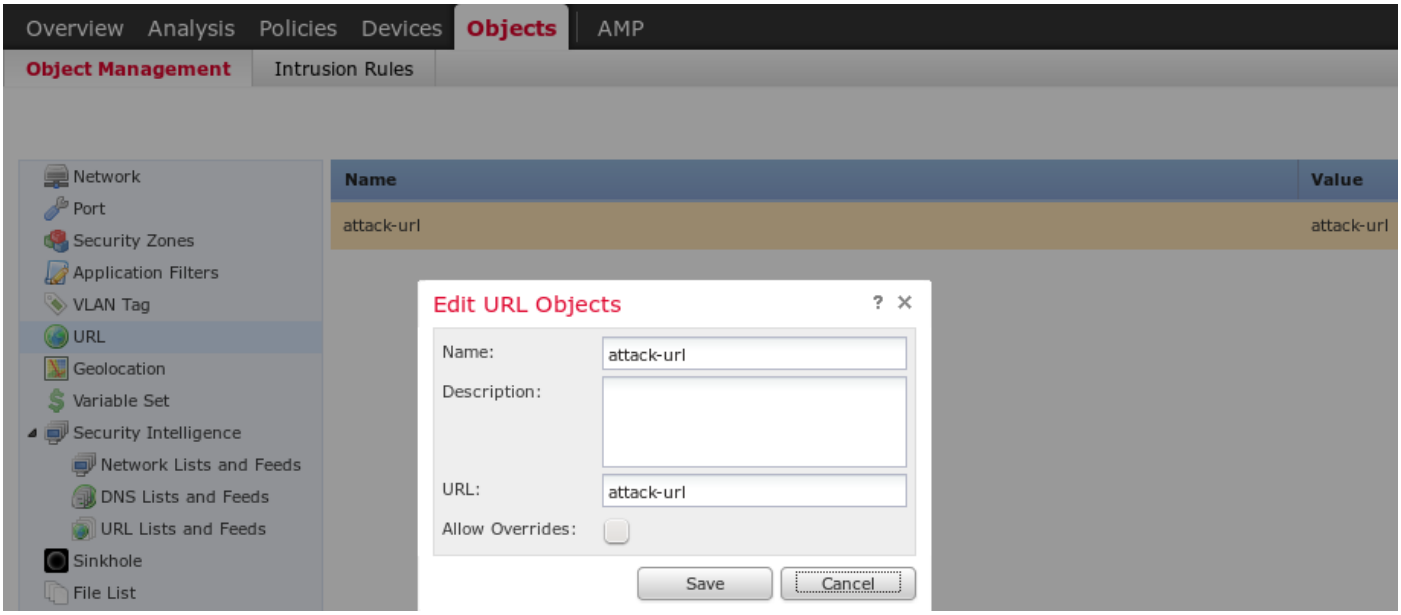
ID 정책

패시브 인증을 위해 이전에 구성된 AD 영역을 활용하는 ID 정책을 구성합니다.

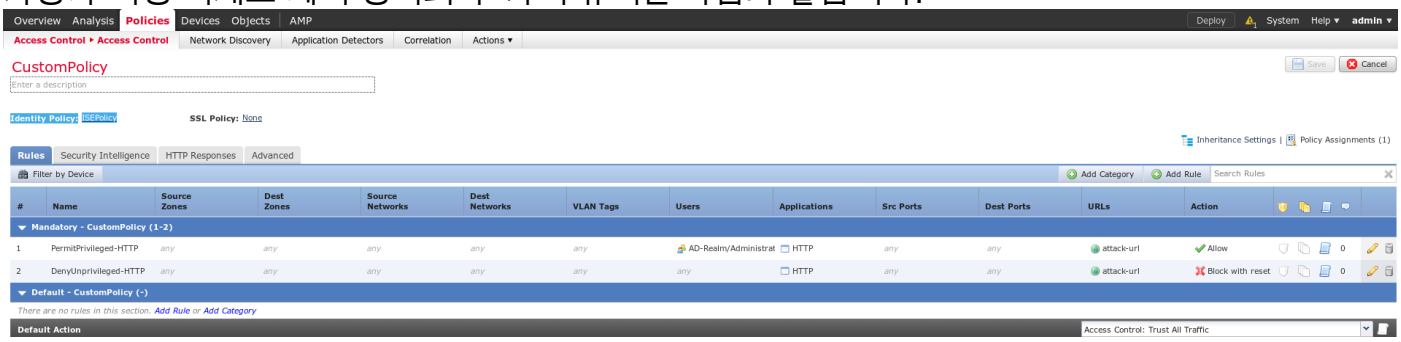


액세스 제어 정책

이 예에서는 사용자 지정 URL이 생성되었습니다.



사용자 지정 액세스 제어 정책의 두 가지 규칙은 다음과 같습니다.

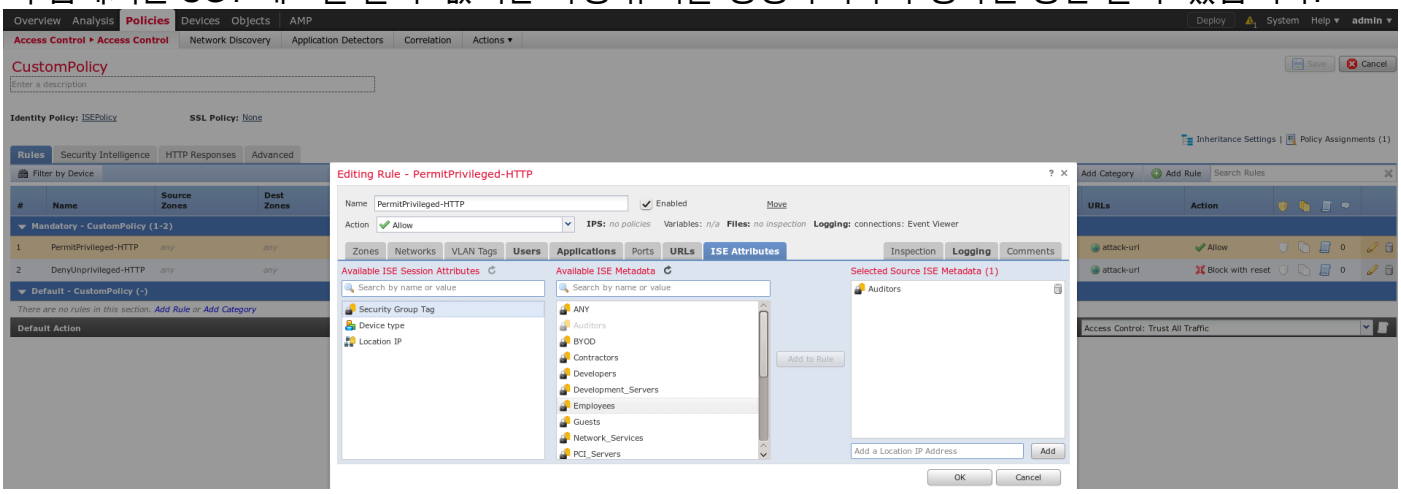


PermitPrivileged-HTTP 규칙은 SGT 태그가 할당된 AD 관리자 그룹에 속한 모든 사용자를 허용합니다.감사자는 모든 대상에 대해 HTTP 공격을 실행합니다.

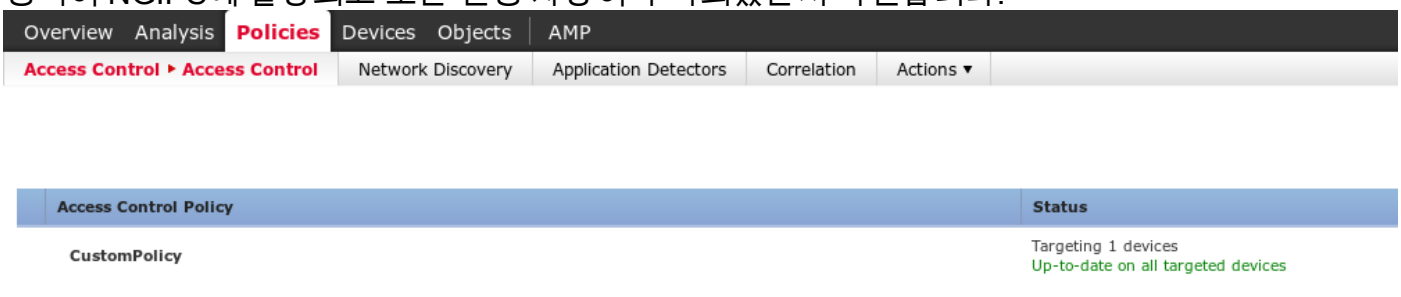
DenyUnprivileged-HTTP는 다른 모든 사용자에게 해당 작업을 거부합니다.

또한 이전에 생성한 ID 정책이 이 액세스 제어 정책에 할당되었음을 확인합니다.

이 탭에서는 SGT 태그를 볼 수 없지만 특정 규칙을 생성하거나 수정하는 동안 볼 수 있습니다.

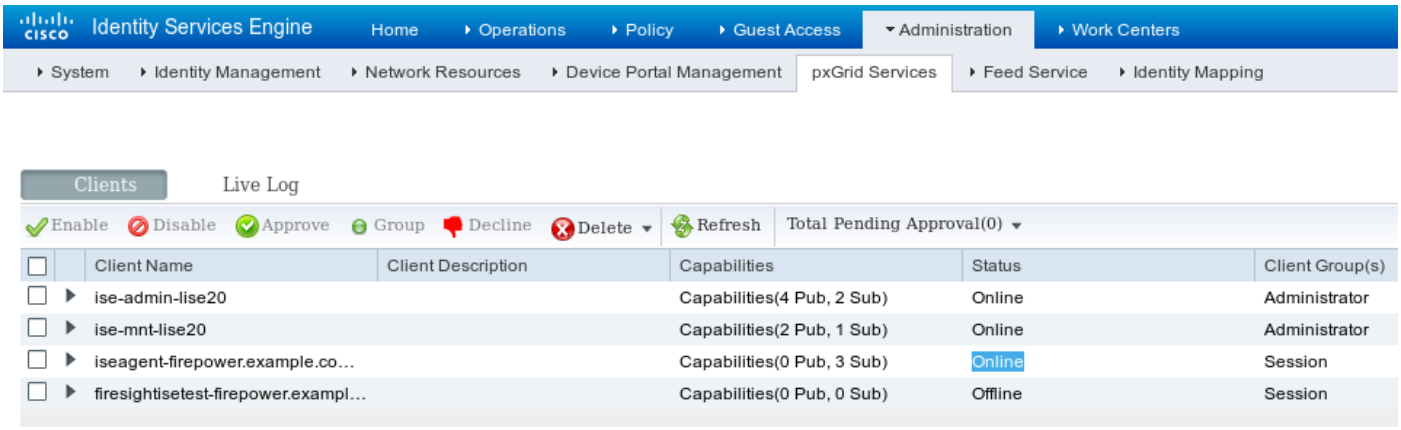


정책이 NGIPS에 할당되고 모든 변경 사항이 구축되었는지 확인합니다.

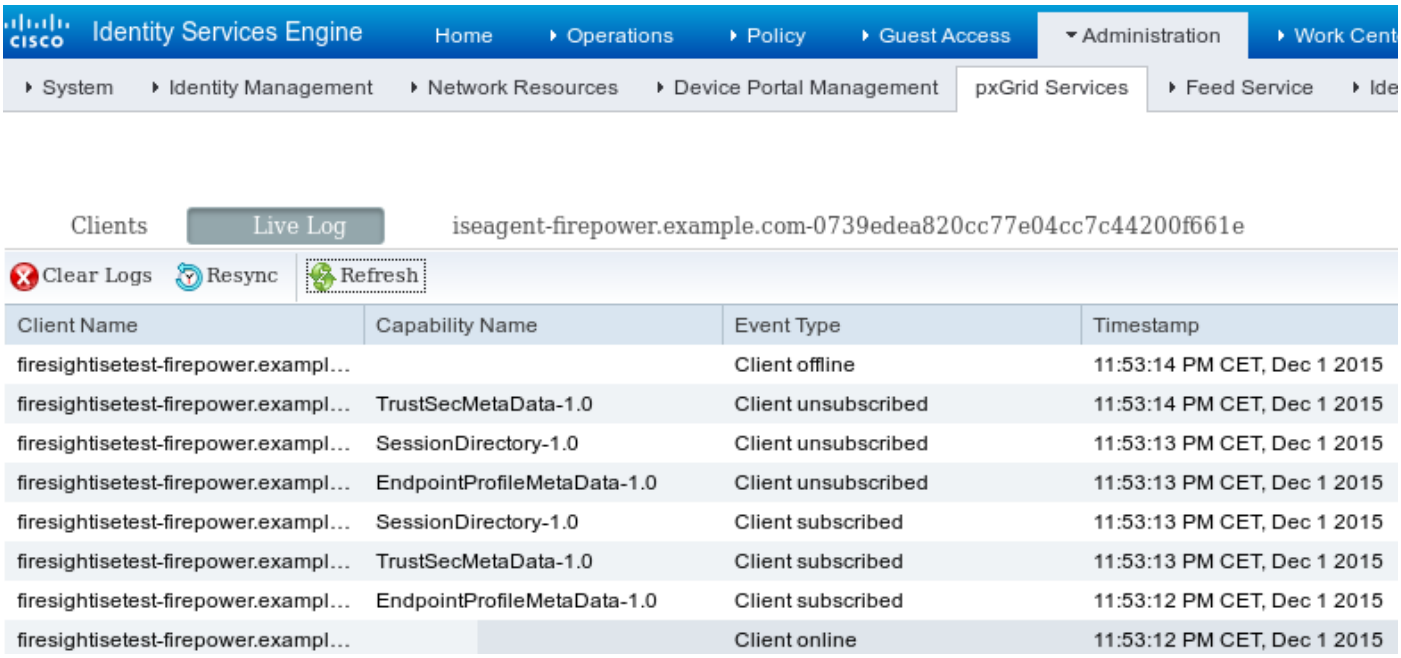


다음을 확인합니다.

모든 것이 올바르게 구성된 후 ISE는 세션 서비스에 가입하는 pxGrid 클라이언트를 확인해야 합니다(상태 Online).



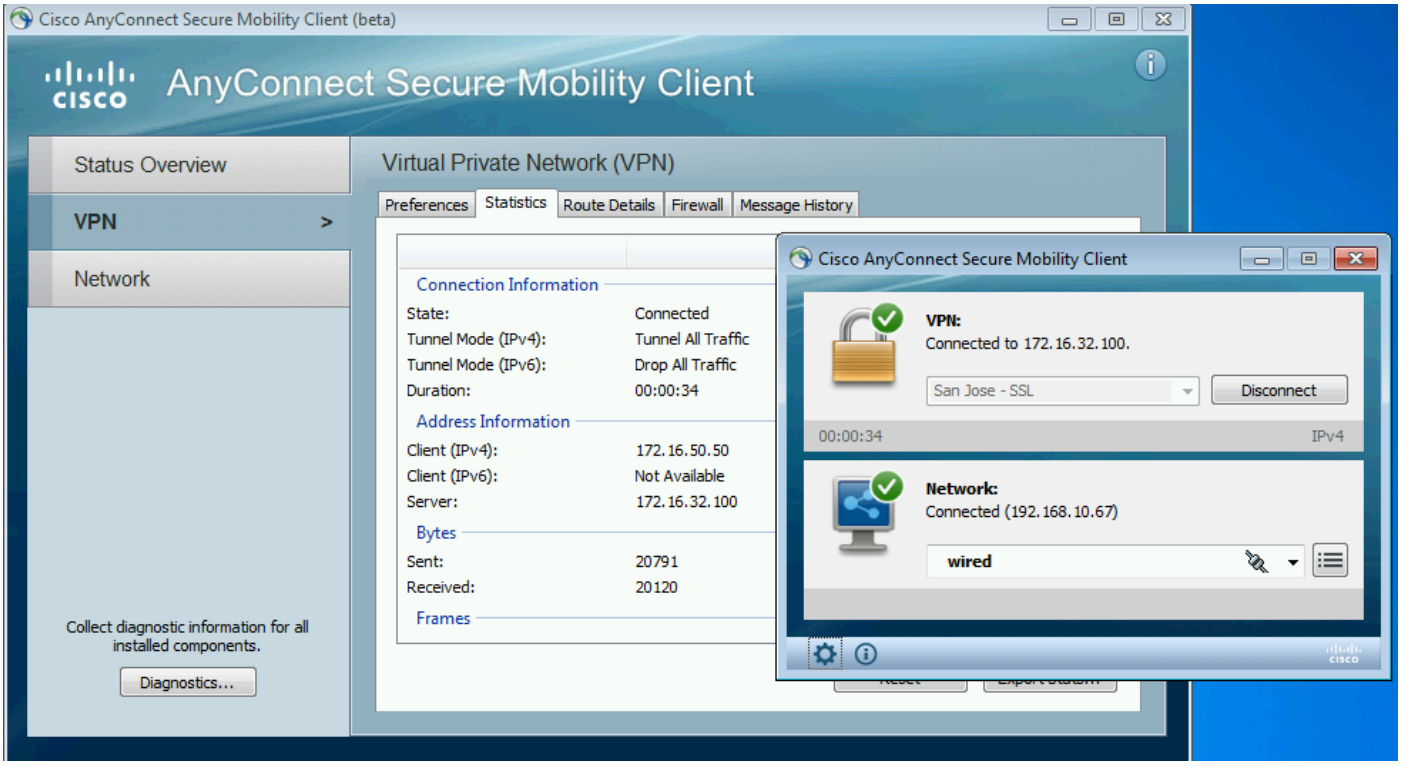
로그에서 FMC가 TrustSecMetaData(SGT 태그) 서비스에 가입했는지 확인할 수도 있습니다. 모든 태그를 가져오고 구독이 해제되었습니다.



VPN 세션 설정

ISE에 대한 권한 부여가 올바른 SGT 태그를 반환하지 않는 경우 시나리오에 대해 첫 번째 테스트가 수행됩니다(NGIPS는 감사 테스트를 허용하지 않음).

VPN 세션이 UP이면 AnyConnect User Interface(UI)에서 자세한 정보를 제공할 수 있습니다.

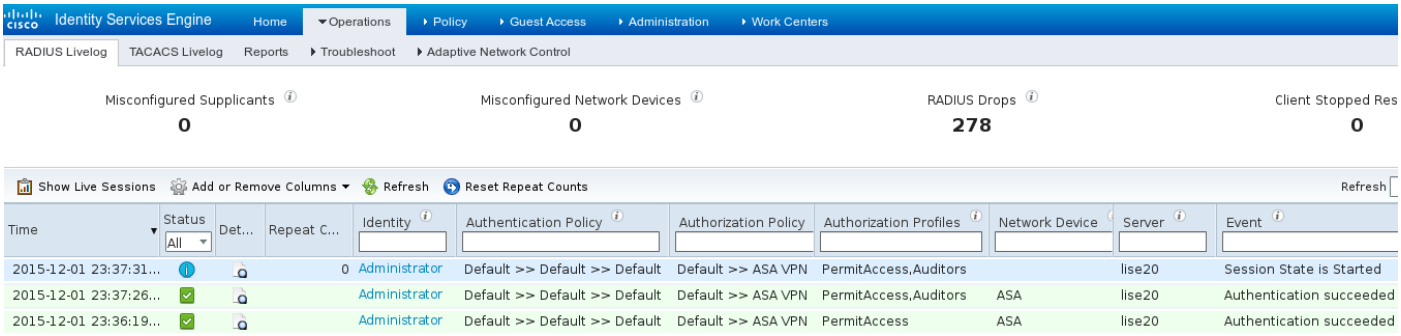


ASA는 세션이 설정되었는지 확인할 수 있습니다.

```
asav# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Administrator          Index        : 1
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.67
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel:
(1)AES128

Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel:
(1)SHA1

Bytes Tx     : 11428                  Bytes Rx     :
24604

Group Policy : POLICY                 Tunnel Group :
SSLVPN

Login Time   : 12:22:59 UTC Wed Dec 2
2015

Duration     :
0h:01m:49s


Inactivity   :
0h:00m:00s


VLAN Mapping : N/A                    VLAN         :
none

Audt Sess ID : ac101f6400001000565ee2a3
```

ASA에서 이 인증에 대해 반환되는 SGT 태그가 표시되는지 확인하십시오.ASA가 TrustSec에 대해 구성되지 않았으므로 해당 정보는 건너뜁니다.

ISE는 또한 성공적인 권한 부여(23:36:19의 로그) 보고 중 - SGT 태그가 반환되지 않음:



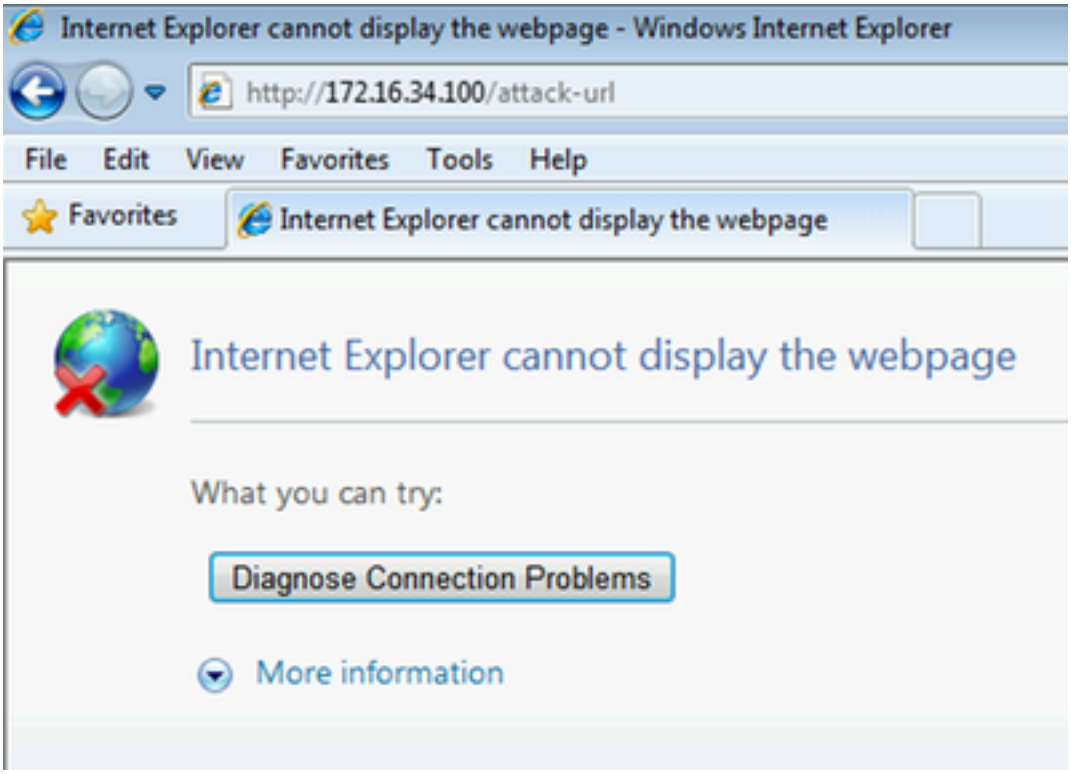
MnT에서 세션 데이터를 가져오는 FMC

이 단계에서 /var/log/messages의 FMC는 관리자 사용자 이름에 대한 새 세션(pxGrid 서비스의 구독자로 수신됨)을 보고하고 그룹 멤버쉽에 대한 AD 조회를 수행합니다.

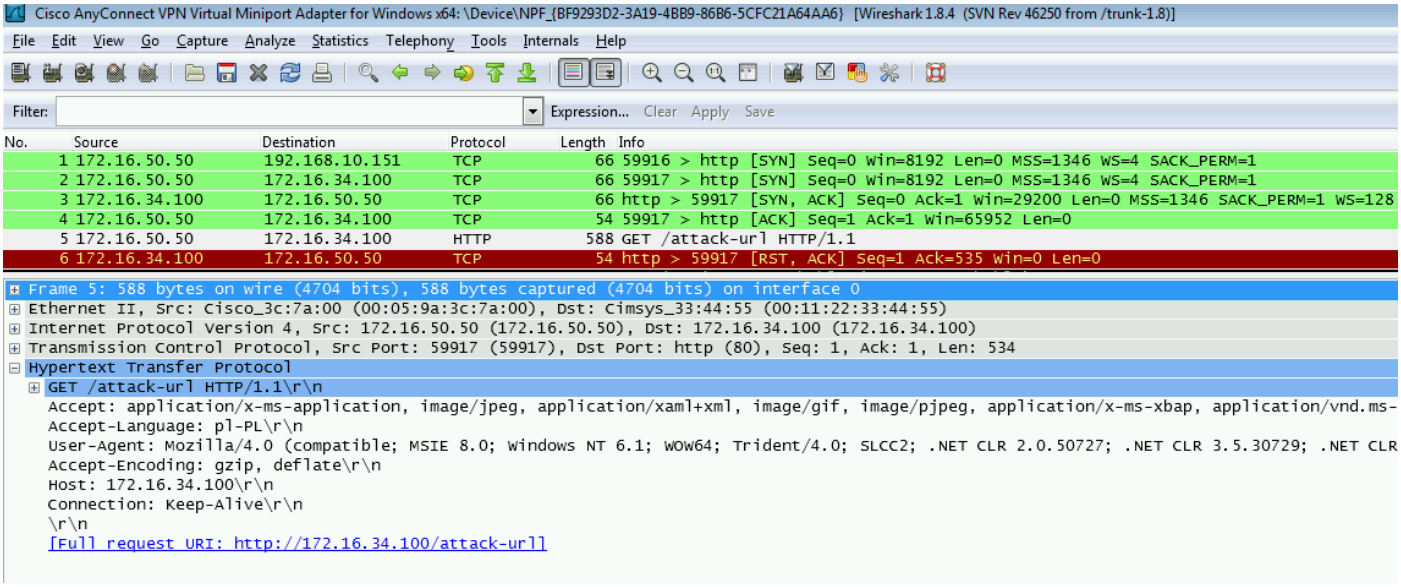
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

권한이 없는 네트워크 액세스

이 단계에서 사용자가 웹 브라우저를 열고 감사된 서버에 액세스하려고 하면 연결이 종료됩니다.



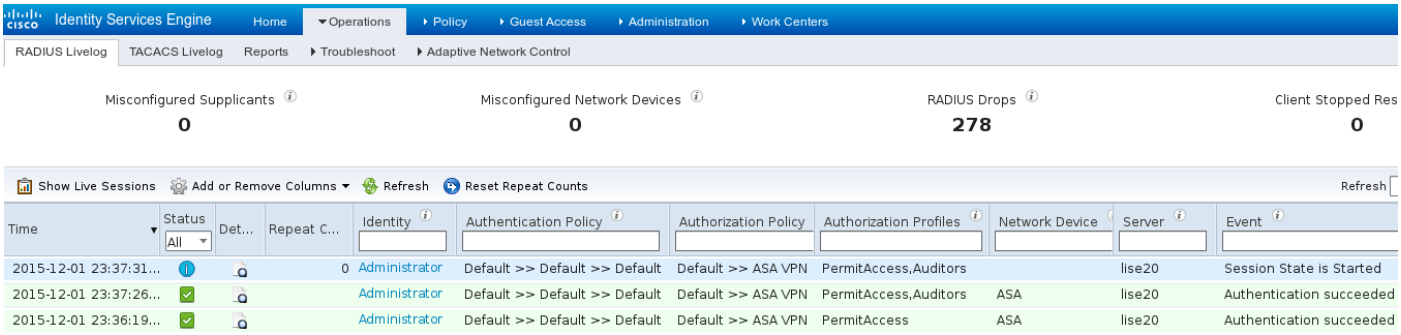
클라이언트에서 가져온 패킷 캡처를 통해 확인할 수 있습니다(FMC 컨피그레이션에 따라 TCP RST 전송).



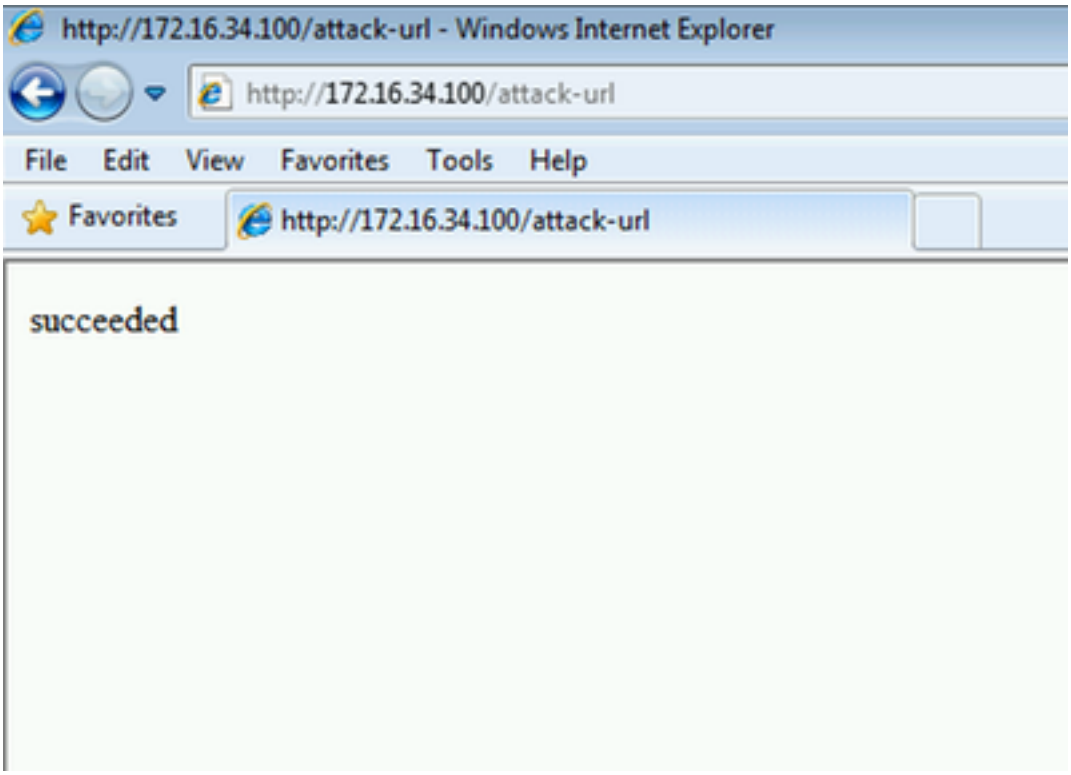
ISE가 반환하도록 구성되면 감사 태그 ASA 세션이 보고합니다.

```
asav# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Administrator          Index        : 1
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.67
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel:
(1)AES128

Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel:
(1)SHA1

Bytes Tx     : 11428                  Bytes Rx     :
24604

Group Policy : POLICY                 Tunnel Group :
SSLVPN

Login Time   : 12:22:59 UTC Wed Dec 2
2015

Duration     :
0h:01m:49s


Inactivity   :
0h:00m:00s


VLAN Mapping : N/A                    VLAN         :
none

Audt Sess ID : ac101f6400001000565ee2a3
Security Grp : 9
```

ISE는 또한 성공적인 권한 부여(23:37:26의 로그)를 보고합니다. SGT 태그 감사자는 다음과 같이 반환됩니다.

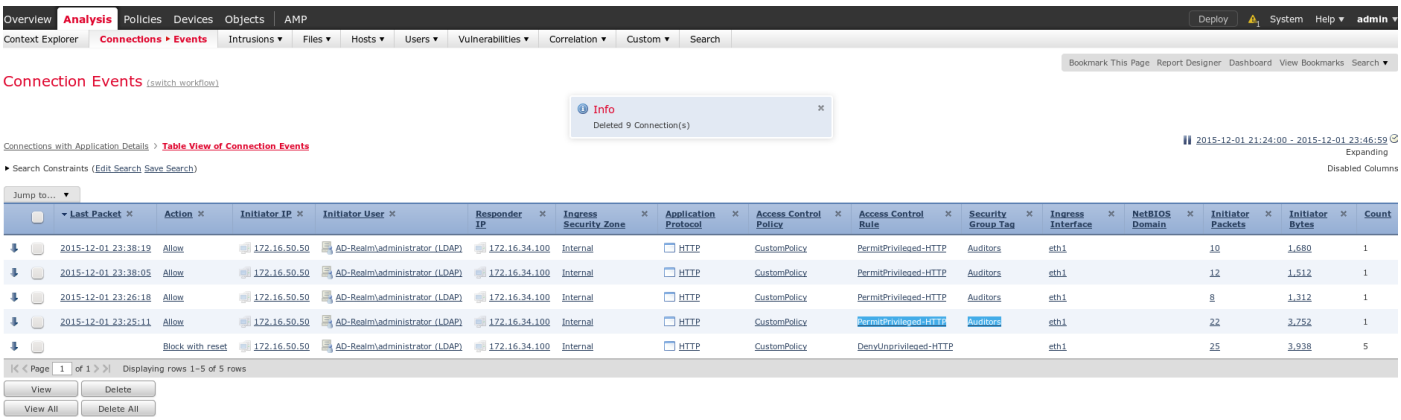


사용자는 다음과 같은 서비스에 액세스할 수 있습니다.



FMC 로깅 액세스

이 활동은 연결 이벤트 보고서에서 확인할 수 있습니다.



먼저, 사용자에게 SGT 태그가 할당되지 않았고 DenyUnprivileged-HTTP 규칙을 적중했습니다.감사자 태그가 ISE에 의해 할당되고 FMC에 의해 검색되면 PermitPrivileged-HTTP가 사용되고 액세스가 허용됩니다.

또한 일반적으로 액세스 제어 규칙 및 보안 그룹 태그가 마지막 열 중 하나로 표시되므로 가로로 스

크롤 막대를 사용해야 하므로 여러 열이 제거되었습니다. 이 사용자 정의 뷰는 나중에 저장하고 다시 사용할 수 있습니다.

문제 해결

FMC 디버그

ID 서비스를 담당하는 adi 구성 요소의 로그를 확인하려면 /var/log/messages 파일을 확인합니다.

```
[23509] ADI_ISE_Test_Help:ADI_ISE_Test_Help [INFO] Parsing command line arguments...
[23509] ADI_ISE_Test_Help:adi.DirectoryTestHandler [INFO] test: ISE connection.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing ISE Connection objects...

[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Preparing subscription objects...

[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
EndpointProfileMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
EndpointProfileMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
TrustSecMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
TrustSecMetaDataCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] subscribed successfully to
SessionDirectoryCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] registered callback for capability
SessionDirectoryCapability
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Connecting to ISE server...
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Beginning to connect to ISE server...

[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: _reconnection_thread started
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: pxgrid connection init done successfully
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: connecting to host lise20.example.com .......
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: stream opened
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: EXTERNAL authentication complete
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:44 [
INFO]: authenticated successfully (sasl mechanism: EXTERNAL)
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: successfully subscribed
message repeated 2 times
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Queried 1 bulk download
hostnames:lise20.example.com:8910
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] ...successfully connected to ISE
server.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Starting bulk download
[23514] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: curl_easy_setopt() for CURLOPT_URL:
'https://lise20.example.com:8910/pxgrid/mnt/sd/getSessionListByTime'
[8893] ADI:ADI [INFO] : sub command emits:'* Trying 172.16.31.210...'
[8893] ADI:ADI [INFO] : sub command emits:'* Connected to lise20.example.com (172.16.31.210)
port 8910 (#0)'
[8893] ADI:ADI [INFO] : sub command emits:'* Cipher selection:
ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH'
[8893] ADI:ADI [INFO] : sub command emits:'* SSL connection using TLSv1.2 / DHE-RSA-AES256-
```

```
SHA256'
[8893] ADI:ADI [INFO] : sub command emits:'* Server certificate:'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I subject: CN=lise20.example.com'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I start date: 2015-11-21 14:40:36 GMT'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I expire date: 2017-11-20 14:40:36 GMT'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I common name: lise20.example.com (matched)'

[8893] ADI:ADI [INFO] : sub command emits:'* ^I issuer: DC=com; DC=example; CN=example-WIN-
CA'
[8893] ADI:ADI [INFO] : sub command emits:'* ^I SSL certificate verify ok.'
[8893] ADI:ADI [INFO] : sub command emits:'> POST /pxgrid/mnt/sd/getSessionListByTime
HTTP/1.1^M'
[8893] ADI:ADI [INFO] : sub command emits:'Host: lise20.example.com:8910^M'
[8893] ADI:ADI [INFO] : sub command emits:'Accept: */*^M'
[8893] ADI:ADI [INFO] : sub command emits:'Content-Type: application/xml^M'
[8893] ADI:ADI [INFO] : sub command emits:'user:firesightisetest-firepower.example.com-
0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com^M'
[8893] ADI:ADI [INFO] : sub command emits:'Content-Length: 269^M'
[8893] ADI:ADI [INFO] : sub command emits:'^M'
[8893] ADI:ADI [INFO] : sub command emits:'* upload completely sent off: 269 out of 269 bytes'

[8893] ADI:ADI [INFO] : sub command emits:'< HTTP/1.1 200 OK^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Date: Tue, 01 Dec 2015 23:10:45 GMT^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Content-Type: application/xml^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Content-Length: 1287^M'
[8893] ADI:ADI [INFO] : sub command emits:'< Server: ^M'
[8893] ADI:ADI [INFO] : sub command emits:'< ^M'
[8893] ADI:ADI [INFO] : sub command emits:'* Connection #0 to host lise20.example.com left
intact'
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] bulk download processed 0 entries.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] disconnecting pxgrid
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: Starting reconnection stop
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: _reconnection_thread exited
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: stream closed; err_dom=(null) 2015-12-01T23:10:45 [ INFO]: clientDisconnectedCb ->
destroying client object
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: pxgrid connection shutdown done successfully
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: Exiting from event base loop
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: successfully disconnected
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: connection disconnect done .....
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying pxgrid reconnection
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying underlying pxgrid
connection
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying pxgrid config
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] ISE identity feed destructor called

[23509] ADI_ISE_Test_Help:ADI_ISE_Test_Help [INFO] /usr/local/sf/bin/adi_iseTestHelp cleanly
exits.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: pxgrid library has been uninitialized
[8893] ADI:ADI [INFO] Parent done waiting, child completed with integer status 0
```

보다 자세한 디버그를 가져오려면 (sudo 후 루트에서) adi 프로세스를 종료하고 debug 인수로 실행할 수 있습니다.

```
root@firepower:/var/log# ps ax | grep adi
24047 ?        Sl     0:00 /usr/local/sf/bin/adi
```

```
24090 pts/0    S+     0:00 grep adi
root@firepower:/var/log# kill -9 24047
root@firepower:/var/log# /usr/local/sf/bin/adi --debug
Dec 01 23:14:34 firepower SF-IMS[24106]: [24106] ADI:adi.Adi [DEBUG] adi.cpp:319:HandleLog():
ADI Created, awaiting config
Dec 01 23:14:34 firepower SF-IMS[24106]: [24106] ADI:config [DEBUG]
config.cpp:289:ProcessConfigGlobalSettings(): Parsing global settings
<..........a lot of detailed output with data.......>
```

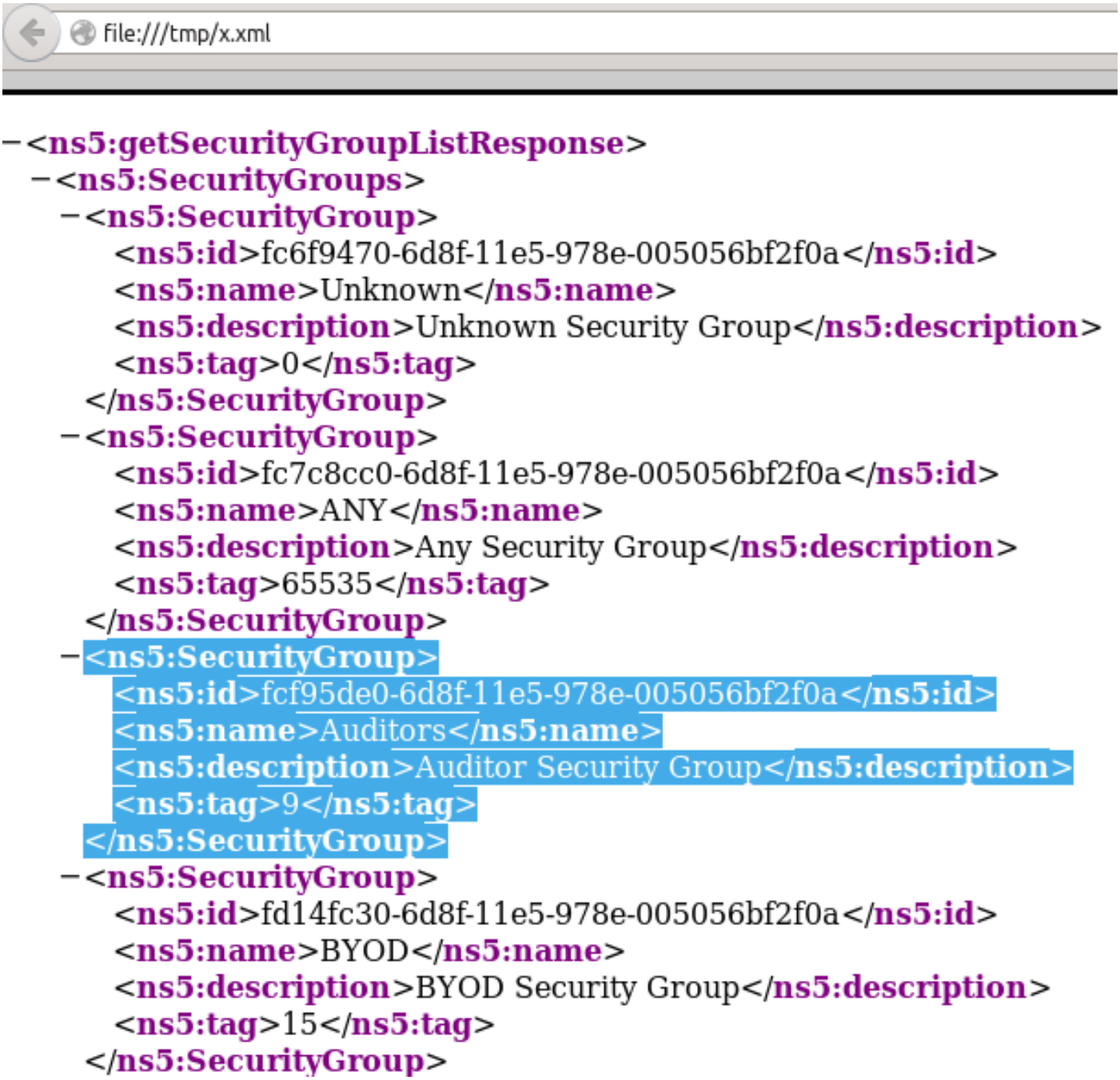
pxGrid를 통한 SGT 쿼리

ISE Integration(ISE 통합) 섹션에서 **Test(테스트)** 버튼을 클릭하거나 SGT 목록이 새로 고쳐질 때 작업이 실행되며 액세스 제어 정책에서 규칙을 추가합니다.

```
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.ISEConnection [DEBUG]
adi.cpp:319:HandleLog(): Querying Security Group metaData...
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): pxgrid_connection_query(connection*:0x10c7da0, capability: 0x1064510,
request:<getSecurityGroupListRequest xmlns='http://www.cisco.com/pxgrid/identity'/>)...
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK|<ns5:getSecurityGroupListResponse
xmlns:ns2='http://www.cisco.com/pxgrid' xmlns:ns3='http://www.cisco.com/pxgrid/net'
xmlns:ns4='http://www.cisco.com/pxgrid/admin' xmlns:ns5='http://www.cisco.com/pxgrid/identity'
xmlns:ns6='http://www.cisco.com/pxgrid/eps' xmlns:ns7='http://www.cisco.com/pxgrid/netcap'
xmlns:ns8='http://www.cisco.com/pxgrid/anc'><ns5:SecurityGroups><ns5:SecurityGroup><ns5:id>fc6f9
470-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Unknown</ns5:name><ns5:description>Unknown
Security
Group</ns5:description><ns5:tag>0</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc7c8c
c0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>ANY</ns5:name><ns5:description>Any Security
Group</ns5:description><ns5:tag>65535</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc
f95de0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Auditors</ns5:name><ns5:description>Auditor
Security
Group</ns5:description><ns5:tag>9</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd14fc
30-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>BYOD</ns5:name><ns5:description>BYOD Security
Group</ns5:description><ns5:tag>15</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd2fb
020-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Contractors</ns5:name><ns5:description>Contractor Security
Group</ns5:description><ns5:tag>5</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd4e34
a0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Developers</ns5:name><ns5:description>Developer
Security
Group</ns5:description><ns5:tag>8</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd6d2e
50-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Development_Servers</ns5:name><ns5:description>Development
Servers Security
Group</ns5:description><ns5:tag>12</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fda10
f90-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Employees</ns5:name><ns5:description>Employee
Security
Group</ns5:description><ns5:tag>4</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdbcd4
f0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Guests</ns5:name><ns5:description>Guest
Security
Group</ns5:description><ns5:tag>6</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdd9ab
c0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Network_Services</ns5:name><ns5:description>Network Services
Security
Group</ns5:description><ns5:tag>3</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdf4d4
e0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>PCI_Servers</ns5:name><ns5:description>PCI
Servers Security
Group</ns5:description><ns5:tag>14</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe11a
bb0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Point_of_Sale_Systems</ns5:name><ns5:description>Point of Sale
Security
Group</ns5:description><ns5:tag>10</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe2d2
```

2f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Servers</ns5:name><ns5:description>Production Servers
Security
Group</ns5:description><ns5:tag>11</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe487
320-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Users</ns5:name><ns5:description>Production User
Security
Group</ns5:description><ns5:tag>7</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe62d8
f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Quarantined_Systems</ns5:name><ns5:description>Quarantine
Security
Group</ns5:description><ns5:tag>255</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe7d
3ec0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Test_Servers</ns5:name><ns5:description>Test
Servers Security
Group</ns5:description><ns5:tag>13</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe99c
770-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>TrustSec_Devices</ns5:name><ns5:description>TrustSec Devices
Security
Group</ns5:description><ns5:tag>2</ns5:tag></ns5:SecurityGroup></ns5:SecurityGroups></ns5:getSec
urityGroupListResponse>]

해당 로그의 XML 내용을 더 잘 보려면 xml 파일에 복사하여 웹 브라우저에서 열 수 있습니다.특정 SGT(감사)가 수신되고 있으며 ISE에 정의된 다른 모든 SGT도 수신되고 있는지 확인할 수 있습니다.



REST API를 통해 MnT에 세션 쿼리

이는 테스트 작업의 일부입니다(MnT 호스트 이름 및 포트가 pxGrid를 통해 전달된다는 점에 유의하십시오). 벌크 세션 다운로드가 사용됩니다.

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK, p_node*:0x7f0ea6ffa8a8(<session
xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime
xmlns='http://www.cisco.com/pxgrid'>2015-12-
01T23:37:31.191+01:00</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt
tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-
Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E
6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceMgmtIntfID></deviceAttachPt
></interface><user><name
```

```
xmlns='http://www.cisco.com/pxgrid'>Administrator</name><ADUserDNSDomain>example.com</ADUserDNSD
omain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfi
le>Windows7-Workstation</endpointProfile><securityGroup>Auditors</securityGroup></session>)]
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.ISEConnection [DEBUG]
adi.cpp:319:HandleLog(): bulk download invoking callback on entry# 1
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.ISESessionEntry [DEBUG]
adi.cpp:319:HandleLog(): parsing Session Entry with following text:<session
xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime
xmlns='http://www.cisco.com/pxgrid'>2015-12-
01T23:37:31.191+01:00</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt
tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-
Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E
6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceMgmtIntfID></deviceAttachPt
></interface><user><name
xmlns='http://www.cisco.com/pxgrid'>Administrator</name><ADUserDNSDomain>example.com</ADUserDNSD
omain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfi
le>Windows7-Workstation</endpointProfile><securityGroup>Auditors</securityGroup></session>
```

구문 분석된 결과(1개의 활성 세션이 수신됨):

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.ISESessionEntry [DEBUG]
adi.cpp:319:HandleLog(): Parsing incoming DOM resulted in following ISESessionEntry:
{gid = ac101f6400007000565d597f, timestamp = 2015-12-01T23:37:31.191+01:00,
state = Started, session_id = 91200007, nas_ip = 172.16.31.100,
mac_addr = 08:00:27:23:E6:F2, ip = 172.16.50.50, user_name = Administrator,
sgt = Auditors, domain = example.com, device_name = Windows7-Workstation}
```

이 단계에서 NGIPS는 해당 사용자 이름(및 도메인)과 Realm-AD 사용자 이름의 상관관계를 분석합니다.

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.RealmContainer [DEBUG] adi.cpp:319
:HandleLog(): findRealm: Found Realm for domain example.com
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.ISEConnectionSub [DEBUG]
adi.cpp:319:HandleLog(): userName = 'Administrator' realmId = 2, ipAddress = 172.16.50.50
```

LDAP는 사용자 및 그룹 구성원 자격을 찾는 데 사용됩니다.

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.LdapRealm [INFO] adi.cpp:322:
HandleLog(): search '(|(sAMAccountName=Administrator))' has the following
DN: 'CN=Administrator,CN=Users,DC=example,DC=com'.
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.LdapRealm [DEBUG] adi.cpp:319:
HandleLog(): getUserIdentifier: searchfield sAMAccountName has display naming attr:
Administrator.
```

ISE 디버깅

pxGrid 구성 요소에 대해 TRACE 레벨 디버그를 활성화한 후에는 모든 작업을 확인할 수 있습니다(그러나 FMC에서와 같이 페이로드/데이터가 없음).

SGT 태그 검색의 예:

```
2015-12-02 00:05:39,352 DEBUG  [pool-1-thread-14][]
cisco.pxgrid.controller.query.CoreAuthorizationManager -::
:::- checking core authorization (topic=TrustSecMetaData, user=firesightisetest-
firepower.example.com
```

```
-0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com, operation=subscribe)...
2015-12-02 00:05:39,358 TRACE  [pool-1-thread-14][] cisco.pxgrid.controller.common.
LogAdvice -::::::- args: [TrustSecMetaData, subscribe, firesightisetest-firepower.example.com-
0739edea820cc77e04cc7c44200f661e@xg
rid.cisco.com]
2015-12-02 00:05:39,359 DEBUG  [pool-1-thread-14][] cisco.pxgrid.controller.persistence.
XgridDaoImpl -::::::-  groups [Any, Session] found for client firesightisetest-firepower.
example.com-0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com
2015-12-02 00:05:39,360 DEBUG  [pool-1-thread-14][] cisco.pxgrid.controller.persistence.
XgridDaoImpl -::::::- permitted rule found for Session TrustSecMetaData subscribe.
total rules found 1
```

버그

CSCuv32295 - ISE는 사용자 이름 필드에 도메인 정보를 보낼 수 있습니다.

CSCus53796 - REST 대량 쿼리용 호스트의 FQDN을 가져올 수 없습니다.

CSCuv43145 - PXGRID 및 ID 매핑 서비스 재시작, 트러스트 저장소 가져오기/삭제

참조

- ISE 및 FirePower Integration으로 리미디에이션 서비스 구성
- 분산 ISE 환경에서 pxGrid 구성
- Cisco pxGrid로 인증서를 구축하는 방법:CA 서명 ISE pxGrid 노드 및 CA 서명 pxGrid 클라이언트 구성
- ISE 버전 1.3 pxGrid와 IPS pxLog 애플리케이션 통합
- Cisco Identity Services Engine 관리자 가이드, 릴리스 2.0
- Cisco Identity Services Engine API 참조 가이드, 릴리스 1.2 - 외부 RESTful S 소개...
- Cisco Identity Services Engine API 참조 설명서, 릴리스 1.2 - 모니터링 RES 소개...
- Cisco Identity Services Engine 관리자 가이드, 릴리스 1.3
- 기술 지원 및 문서 - Cisco Systems