Probleemoplossing voor ISE en FirePOWER-integratie voor identiteitsservices

Inhoud

Inleiding

Dit document beschrijft hoe u vertrouwen op TechSec kunt configureren en problemen oplossen bij Cisco Next Generation Inbraakpreventiesysteem (NGIPS). NGIPS versie 6.0 ondersteunt integratie met Identity Services Engine (ISE) zodat een bewust beleid op basis van identiteit kan worden ontwikkeld.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco adaptieve security applicatie (ASA) VPN-configuratie
- Cisco AnyConnect Secure Mobility Client-configuratie
- Cisco FirePOWER Management Center - basisconfiguratie
- Cisco ISE-configuratie
- Cisco TrustSec-oplossingen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Microsoft Windows 2012 certificaatinstantie (CA)
- Cisco ASA versie 9.3
- Cisco ISE-softwareversies 1.4
- Cisco AnyConnect Secure Mobility Client versies 4.2
- Cisco FirePOWER Management Center (FMC) versie 6.0
- Cisco FirePOWER NGIPS versie 6.0

Configureren

FirePower Management Center (FMC) is het beheerplatform voor FirePOWER. Er zijn twee soorten functies verbonden aan ISE-integratie:

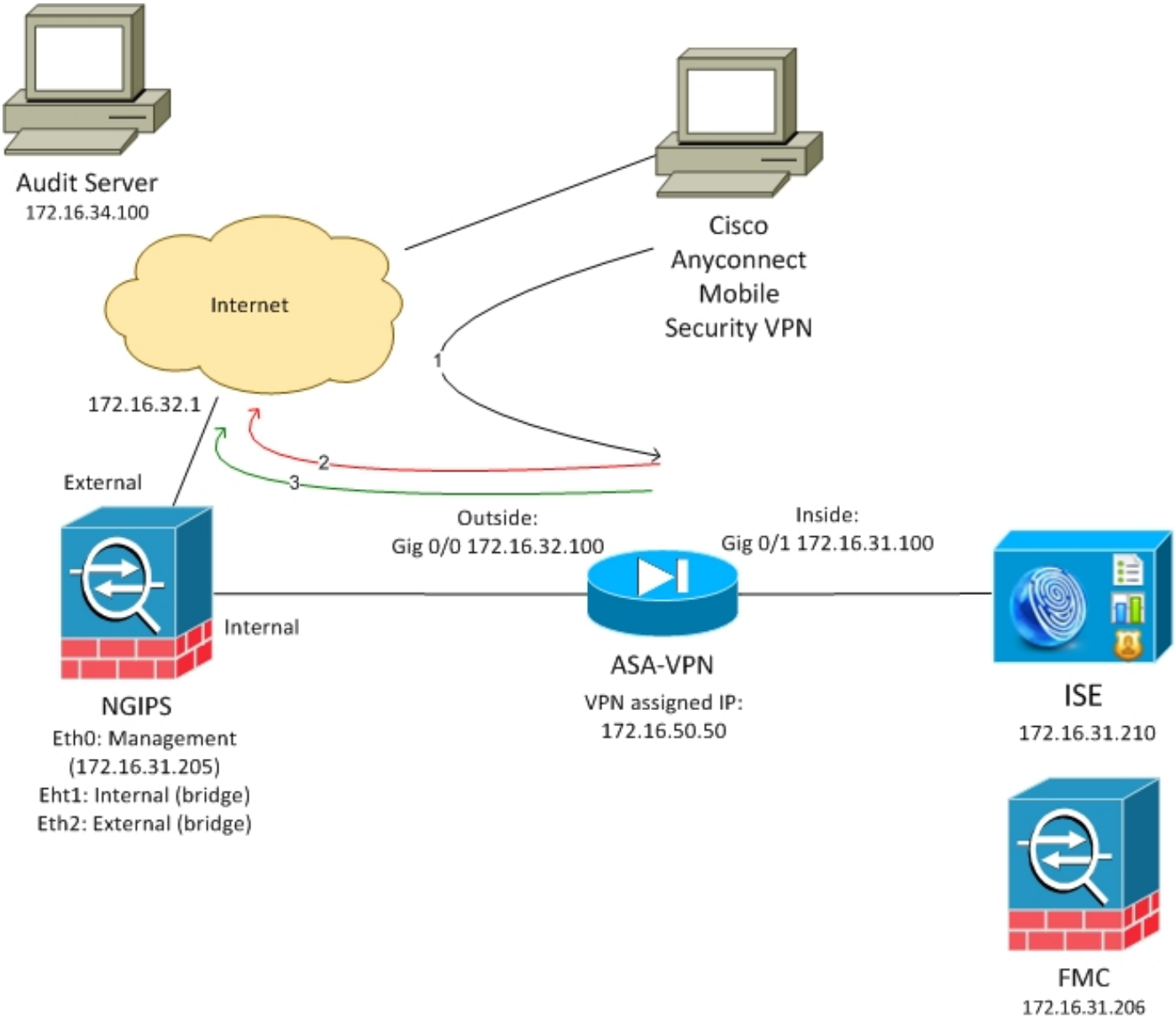
- Remediation - stelt het VCC in staat de aanslagpleger in quarantaine te plaatsen via ISE, die dynamisch de status van de vergunning verandert op toegangsapparaat dat beperkte toegang tot het netwerk biedt. Deze oplossing biedt twee generaties:

1. Verouderde populariteit bij gebruik van EPS API-aanroepen (Endpoint Protection Service) naar ISE.
2. Nieuwe module met behulp van pxGrid-protocolaanroep op ISE (deze module wordt alleen ondersteund in versie 5.4 - niet ondersteund in 6.0, standaard ondersteuning gepland in 6.1).

- Beleid - stelt FMC in staat om beleid te configureren op basis van Tabellen van de Veiligheidsgroep (SGT).

Dit artikel is gericht op de tweede functionaliteit. Lees voor een voorbeeld van verbetering de referenties

Netwerkdiagram



FMC is ingesteld met een toegangscontrolebeleid dat twee regels bevat:

- Ontken voor HTTP-verkeer met aangepaste URL (aanval-URL)
- Sta voor HTTP-verkeer met aangepaste URL (aanval-URL) toe maar alleen als de gebruiker wordt toegewezen aan de SGT-tag (9) door ISE

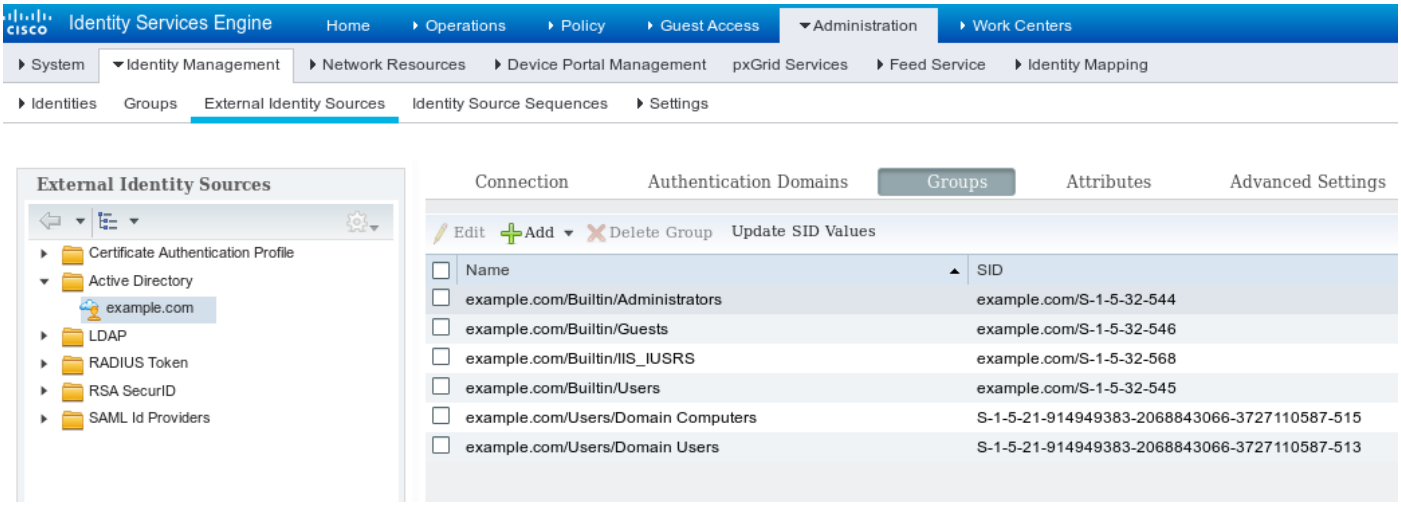
ISE beslist de tag Audit toe te wijzen aan alle gebruikers van de Actieve Map die aan de groep van de Beheerder behoren en ASA-VPN voor netwerktoegang gebruiken.

Gebruiker heeft toegang tot een netwerk via VPN-verbinding op de ASA. De gebruiker probeert dan toegang te krijgen tot de Audated server via URL aanval-url, maar faalt omdat hij niet is toegewezen aan de Controlegroep SGT. Zodra dat is geregeld, is de verbinding succesvol.

ISE

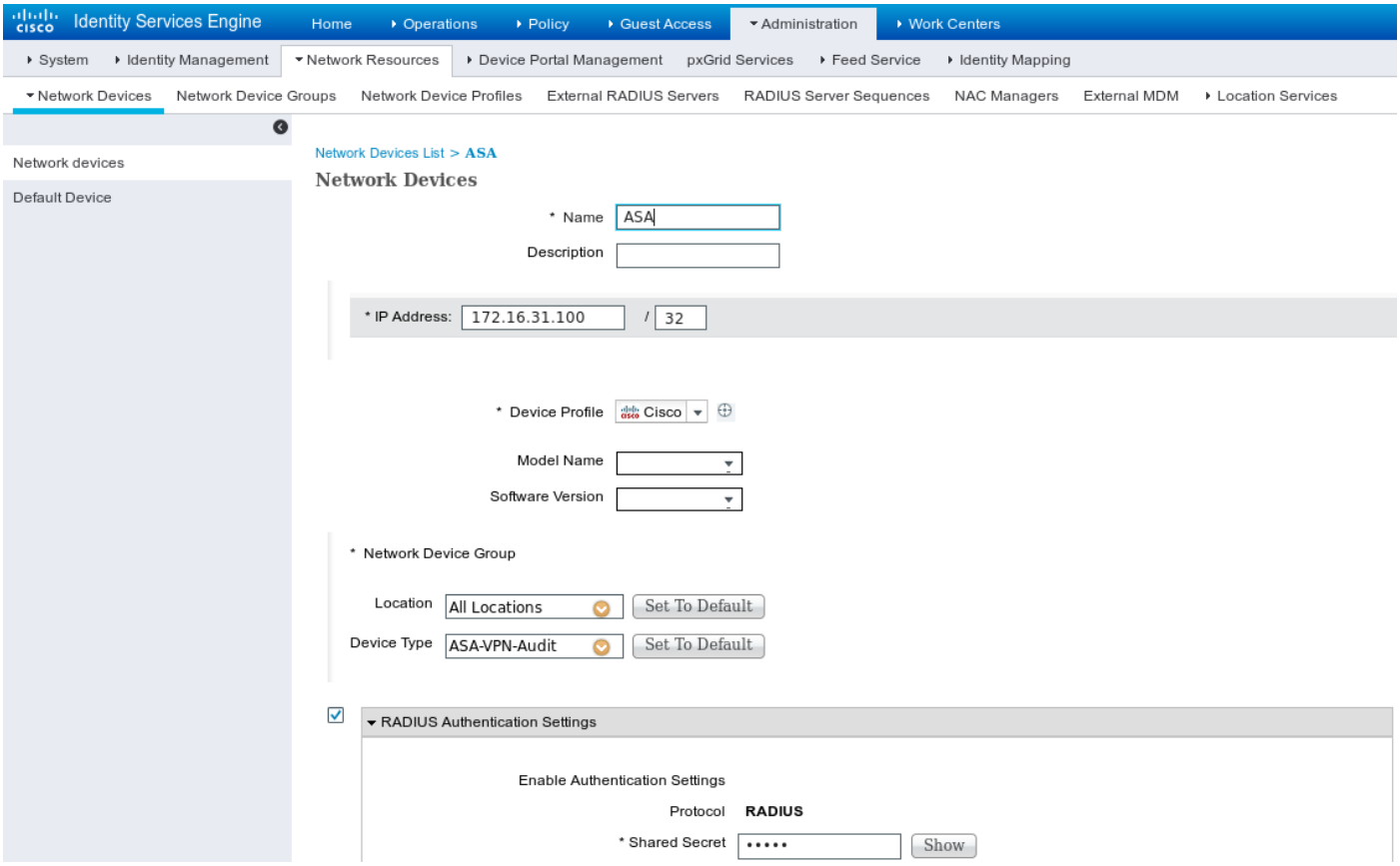
Actieve map

AD-integratie moet worden geconfigureerd en de juiste groepen moeten worden opgehaald (beheerdersgroep wordt gebruikt voor de vergunningsregel):



Netwerktoegangsapparaat

ASA wordt toegevoegd als netwerkapparaat. Aangepaste groep ASA-VPN-Audit wordt gebruikt, zoals in deze afbeelding:



Certificaten voor pxGrid en MnT

FMC gebruikt beide services op ISE:

- pxGrid voor SGT en profilering van gegevens
- Monitoring and Reporting (MnT) voor bulksessiedownload

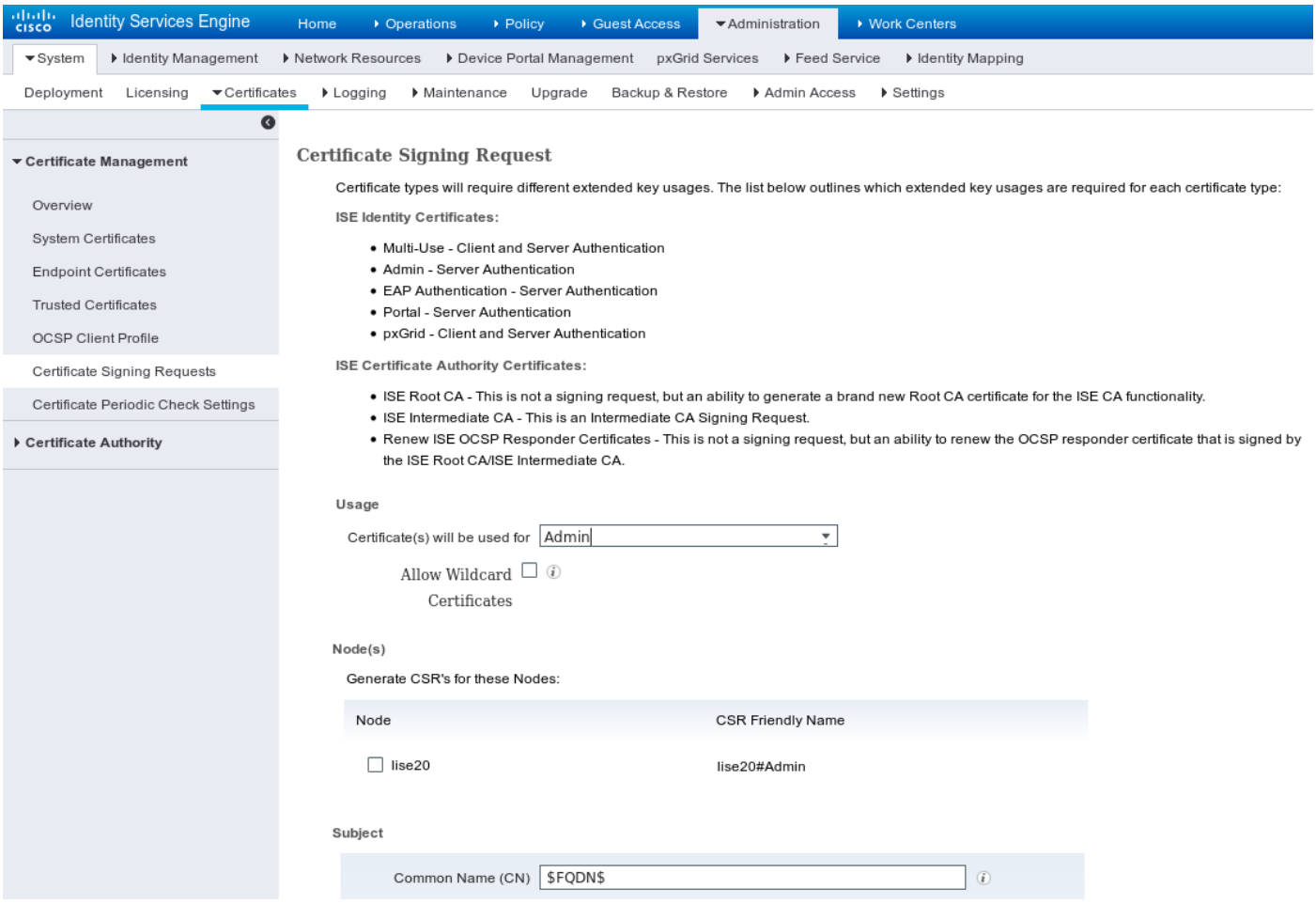
De beschikbaarheid van MnT is zeer belangrijk aangezien FMC op deze manier wordt geïnformeerd wat het IP-adres is van geauthenticeerde sessie, ook de gebruikersnaam en SGT tag. Op basis daarvan kan het juiste beleid worden toegepast. Merk op dat NGIPS Native SGT-

tags (inline tagging) zoals de ASA niet ondersteunt. Maar in tegenstelling tot ASA ondersteunt het SGT namen in plaats van alleen getallen.

Vanwege deze vereisten moeten zowel ISE als FMC elkaar vertrouwen (certificaat). MnT gebruikt enkel server side certificaat, pxGrid gebruikt zowel client als server side certificaat.

Microsoft CA wordt gebruikt om alle certificaten te ondertekenen.

Voor MnT (Admin-rol) moet ISE certificaat signaalaanvraag (CSR) genereren, zoals in deze afbeelding wordt getoond:



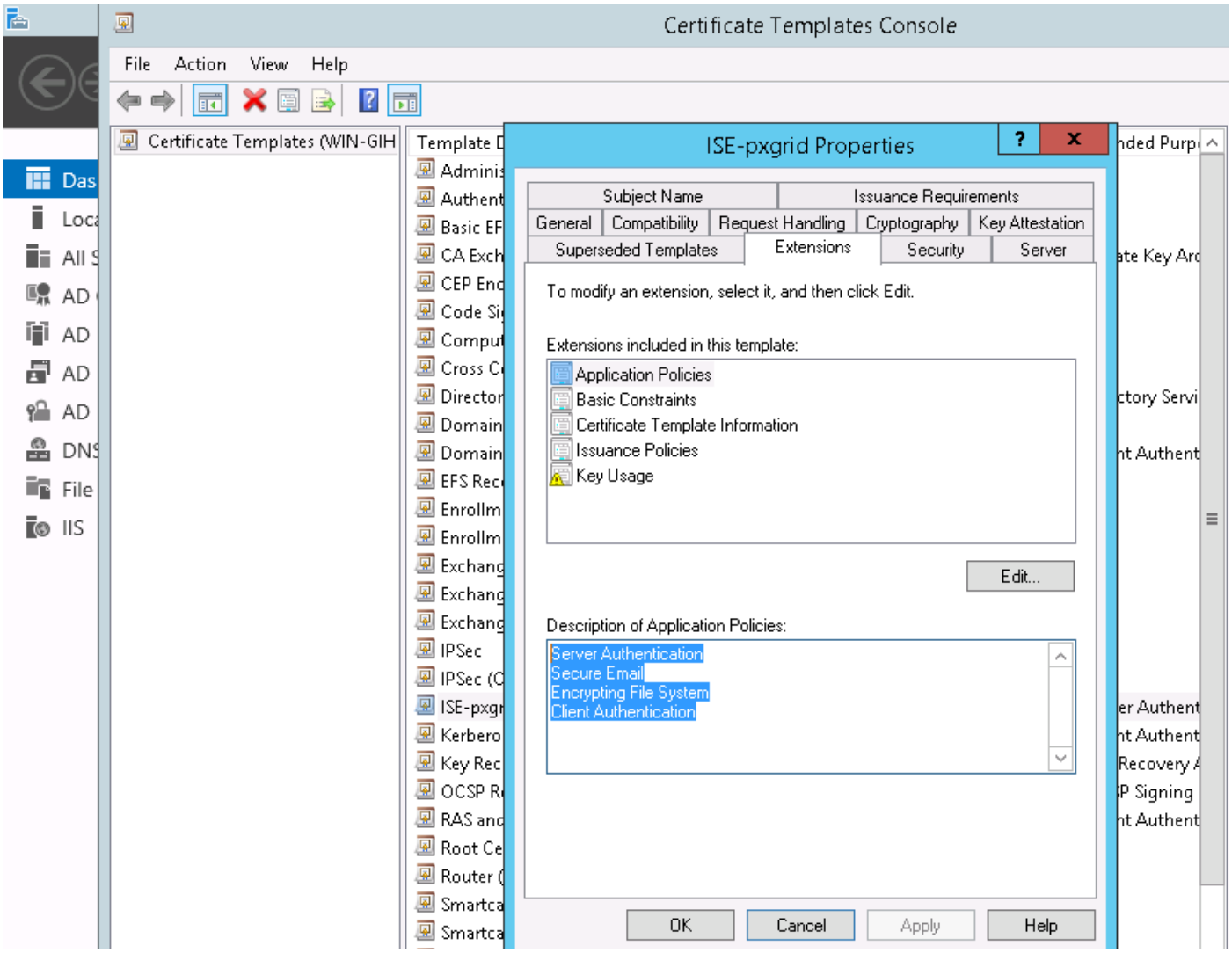
Nadat u door Microsoft CA bent ondertekend, moet u het product via de optie **Bind- certificaat** importeren.

Een soortgelijk proces moet worden gevolgd voor de PxGrid-service. **Certificaat(en) worden gebruikt voor de** optie moet PxGrid zijn geselecteerd.

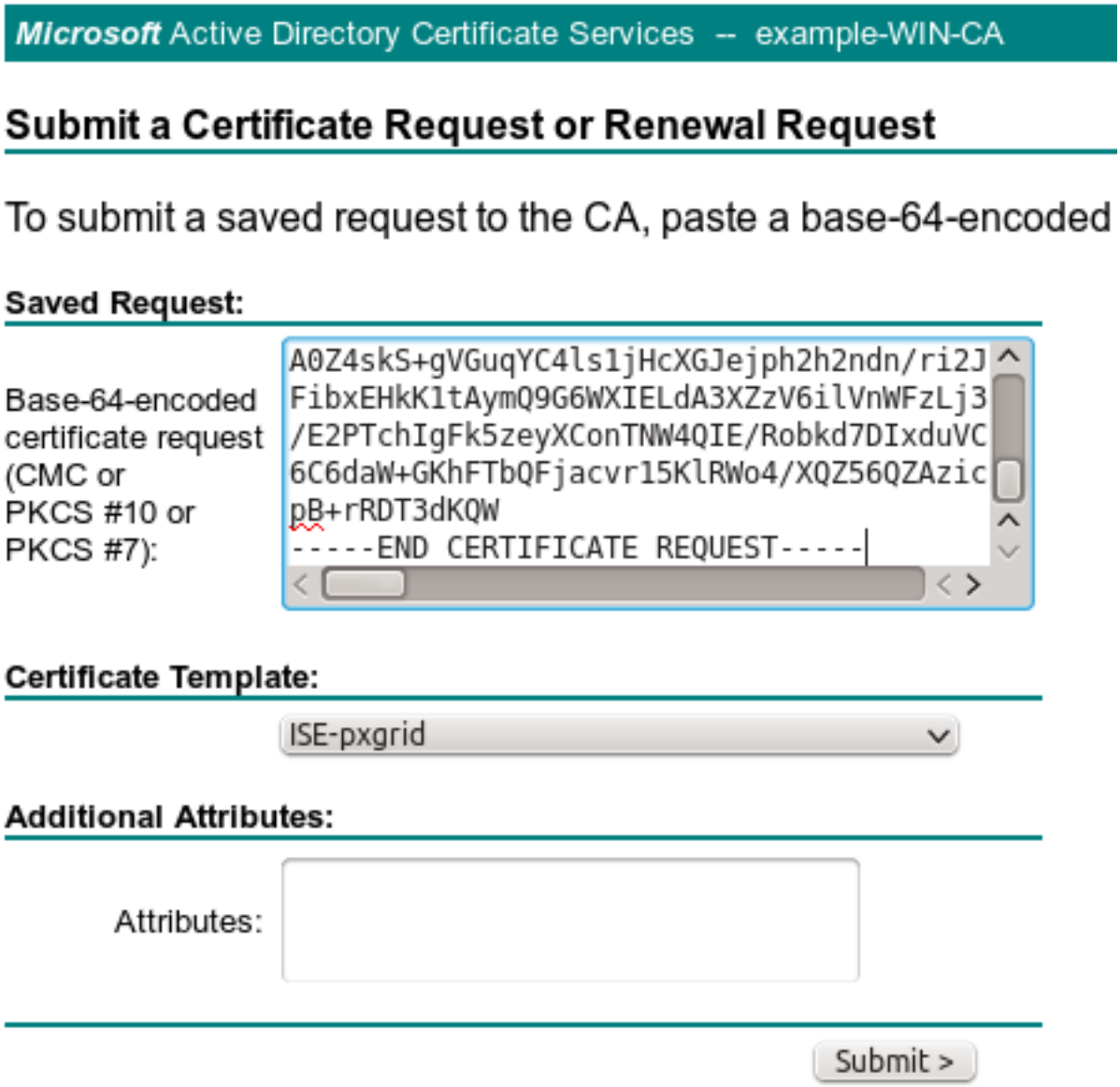
Aangezien er geen twee certificaten met identieke Onderwerp-naam kunnen zijn, is het volledig aanvaardbaar om verschillende waarde toe te voegen voor OU- of O-sectie (bijvoorbeeld pxGrid).

> Opmerking: Zorg ervoor dat voor elke FQDN-naam (Full Qualified Domain Name, FQDN) voor zowel ISE als FMC, de juiste DNS-record is ingesteld op DNS-server.

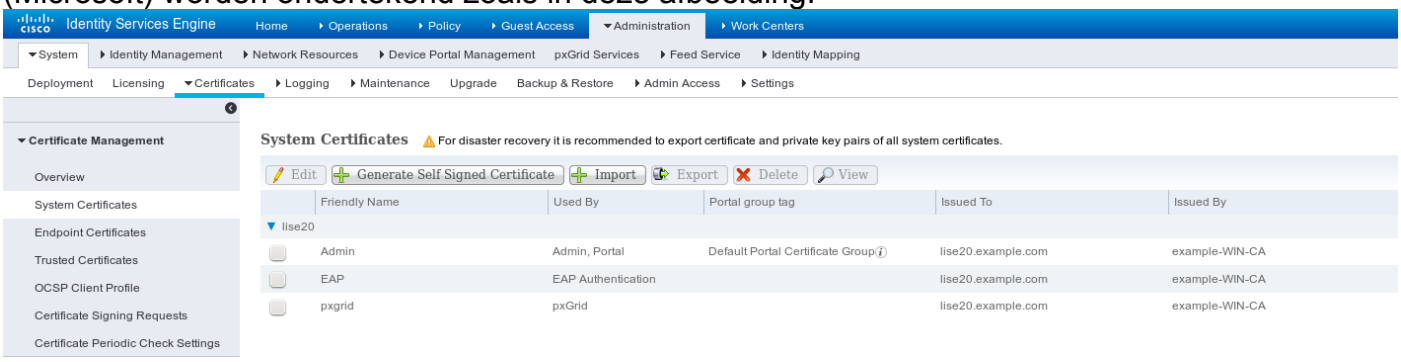
Het enige verschil tussen Admin en pxGrid certificaat is bij het ondertekenen van proces. Aangezien pxGrid-certificaten uitgebreide toetsuitbreidingsopties voor zowel client- als serververificatie op Microsoft CA moeten zijn gebruikt, kan hiervoor worden gebruikt:



Hoe u Microsoft Web Service gebruikt om pxGrid CSR te ondertekenen wordt in deze afbeelding getoond:

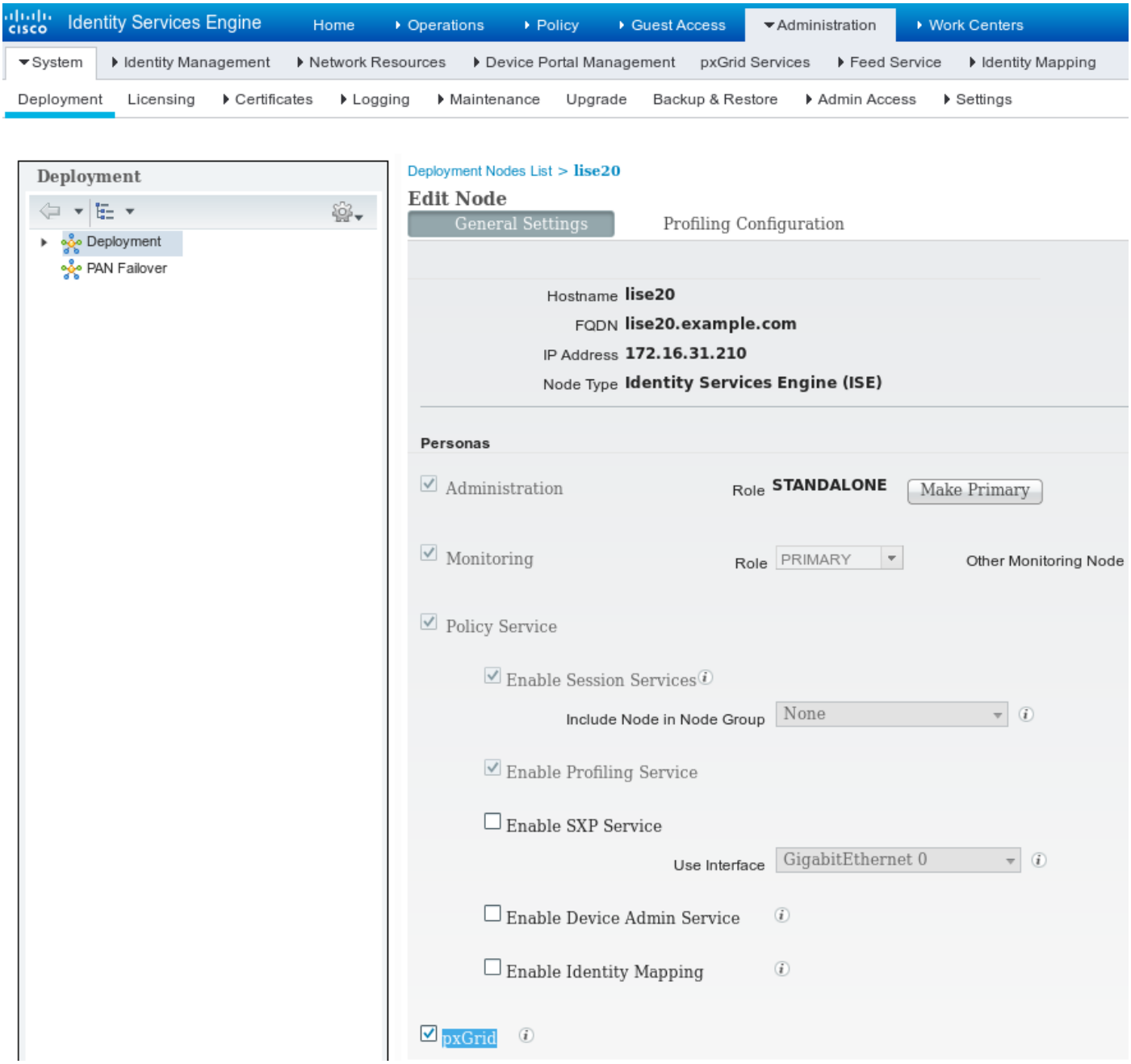


Aan het eind moet ISE Admin en pxGrid certificaten hebben die door de vertrouwde CA (Microsoft) worden ondertekend zoals in deze afbeelding:

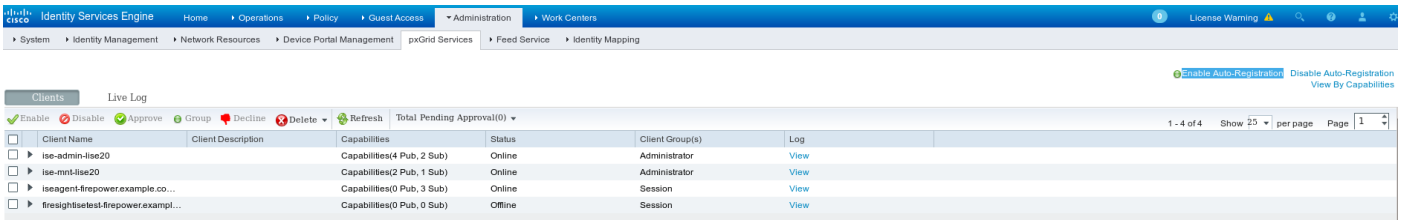


PxGrid-service

Met de juiste certificaten moet de pxGrid-rol voor specifiek knooppunt zijn ingeschakeld, zoals in deze afbeelding:



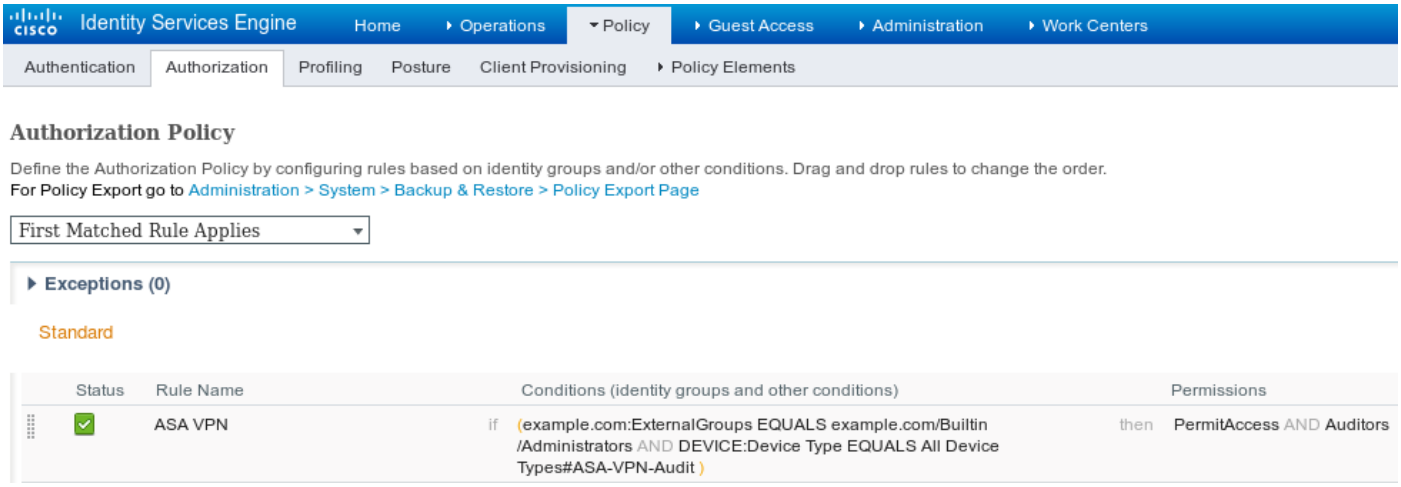
De automatische goedkeuring moet worden ingesteld op:



machtigingsbeleid

Standaard authenticatiebeleid wordt gebruikt (AD raadpleging wordt uitgevoerd als lokale gebruiker niet gevonden wordt).

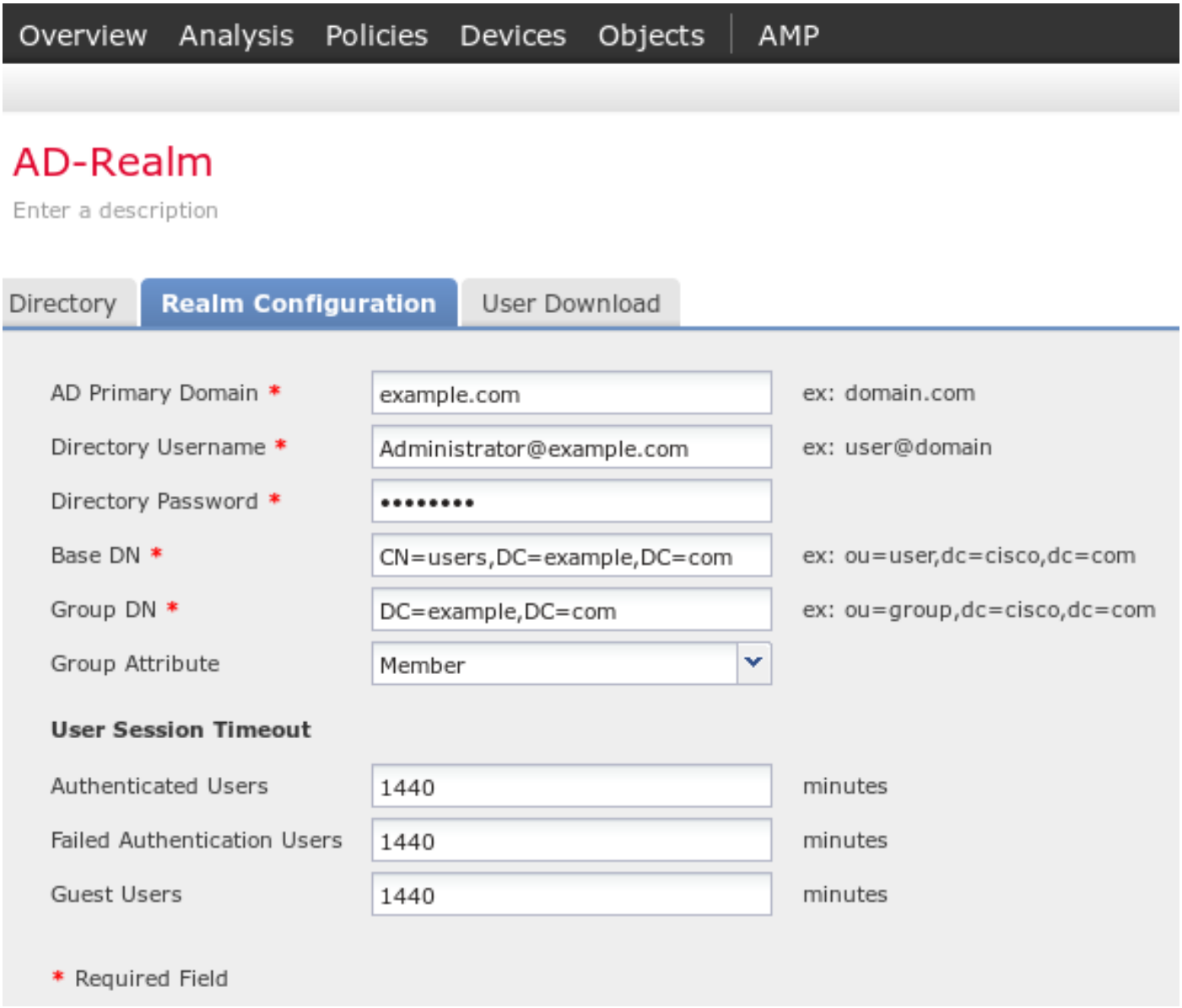
Het machtigingsbeleid is ingesteld om volledige toegang tot het netwerk te verlenen (Toestemming: PermitAccess) voor gebruikers die zich via ASA-VPN authentiseren en behoren tot Active Directory Group Administrator's - voor deze gebruikers wordt de SGT-tag-accountants teruggegeven:



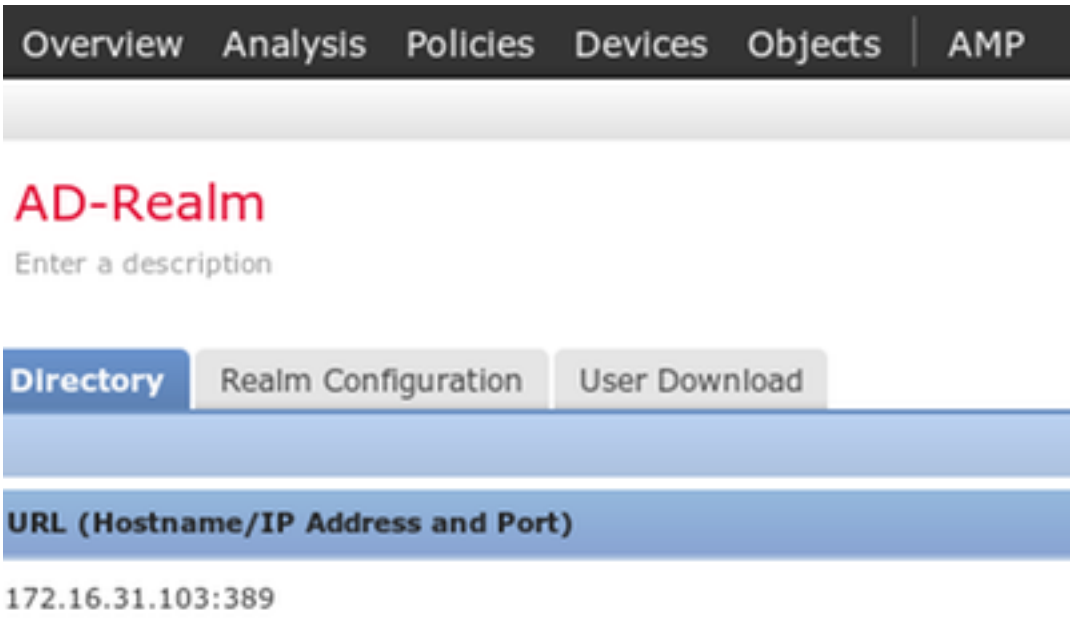
FMC

Actieve map

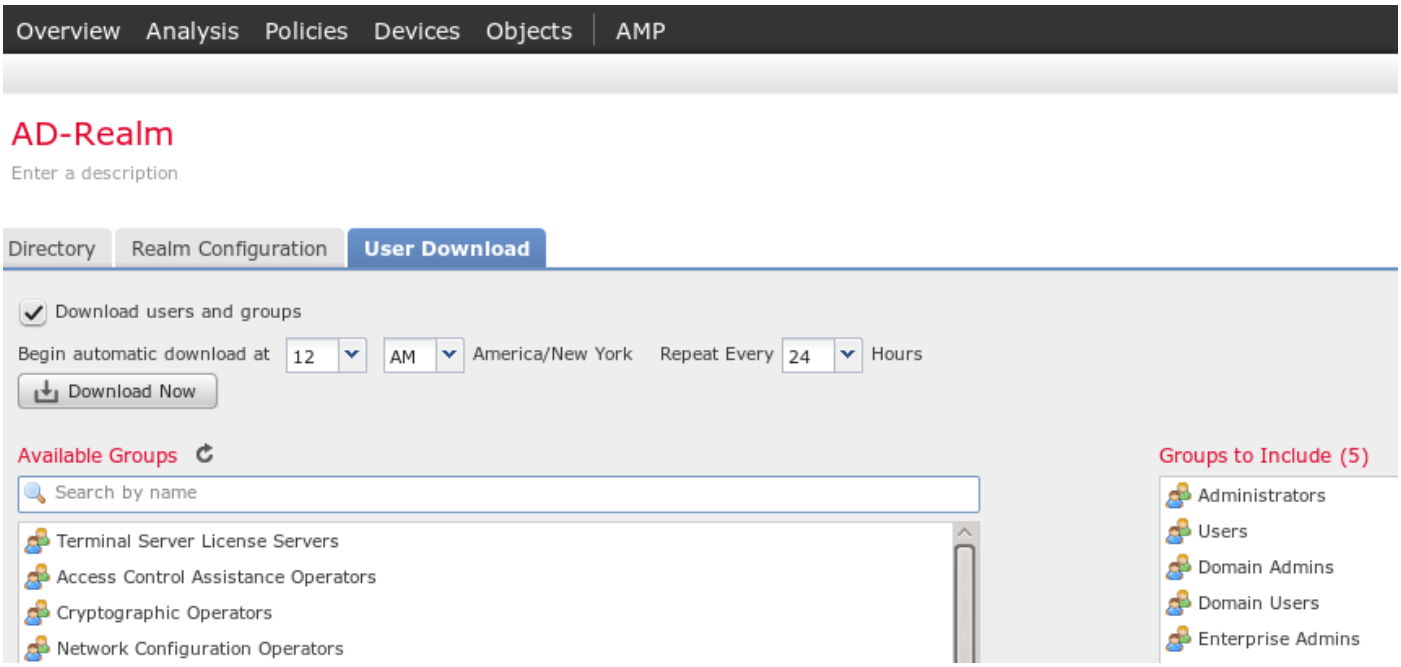
Omgekeerde configuratie is vereist om met ISE-integratie te kunnen werken (om identiteitsbeleid te gebruiken en groepslidmaatschap voor passief gewaarmerkte gebruikers terug te halen). Realm kan worden ingesteld voor Active Directory of Lichtgewicht Directory Access Protocol (LDAP). In dit voorbeeld wordt AD gebruikt. Via **systeem > Integratie > Realm**:



Standaardindexinstellingen worden gebruikt:

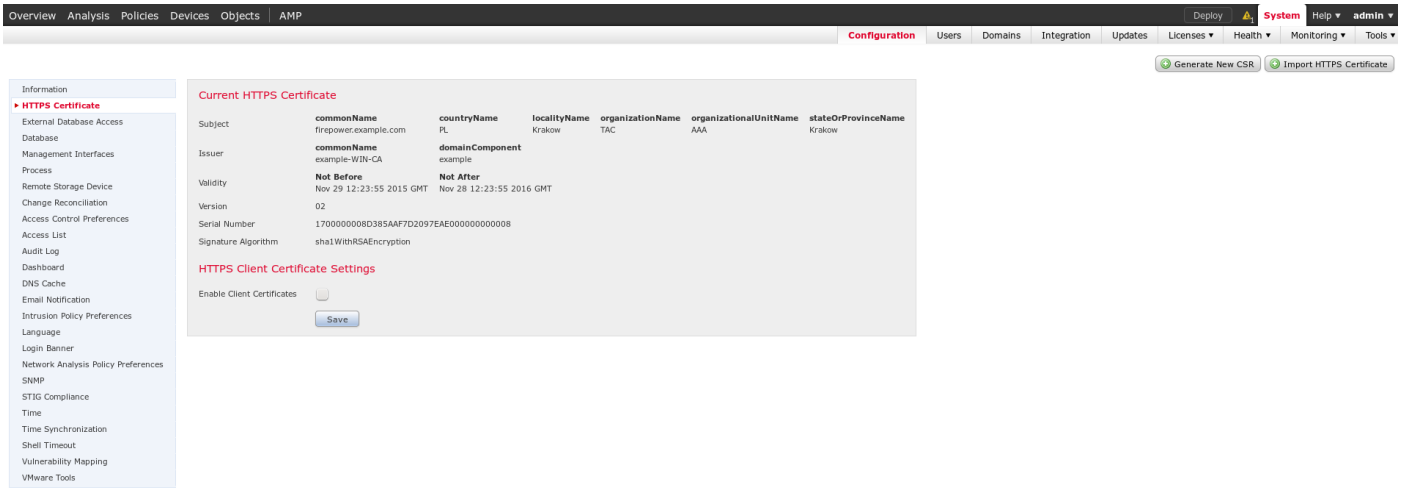


En sommige AD groepen worden opgeroepen (te gebruiken als extra voorwaarde in toegangscontroleregels):

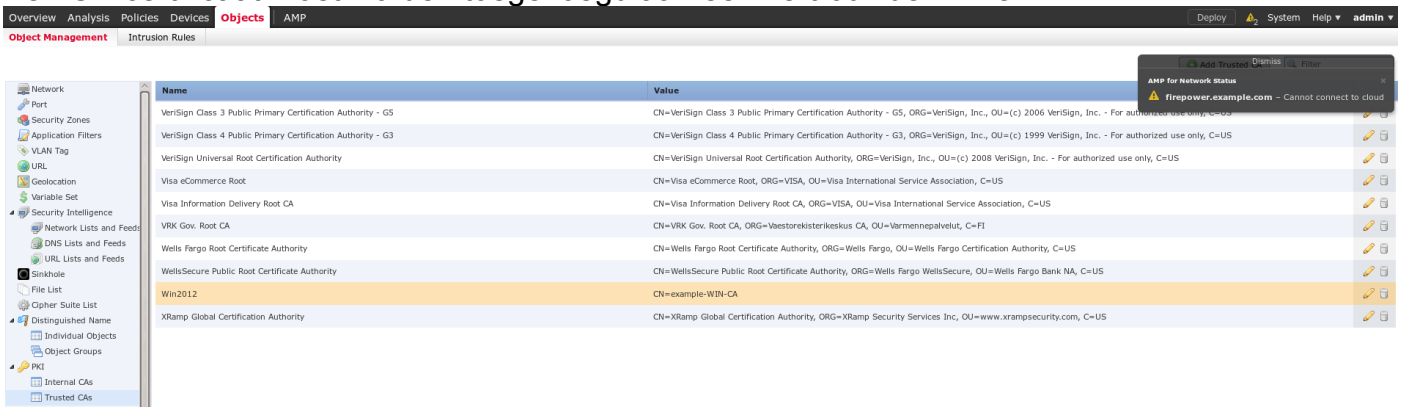


Certificaten voor Admin en PxGrid

Hoewel niet vereist, is het een goede praktijk om CSR te genereren voor toegang tot de beheerder. Meld aan dat CSR gebruikmaakt van een betrouwbaar AD en het ondertekende certificaat terugimporteert, zoals in deze afbeelding:



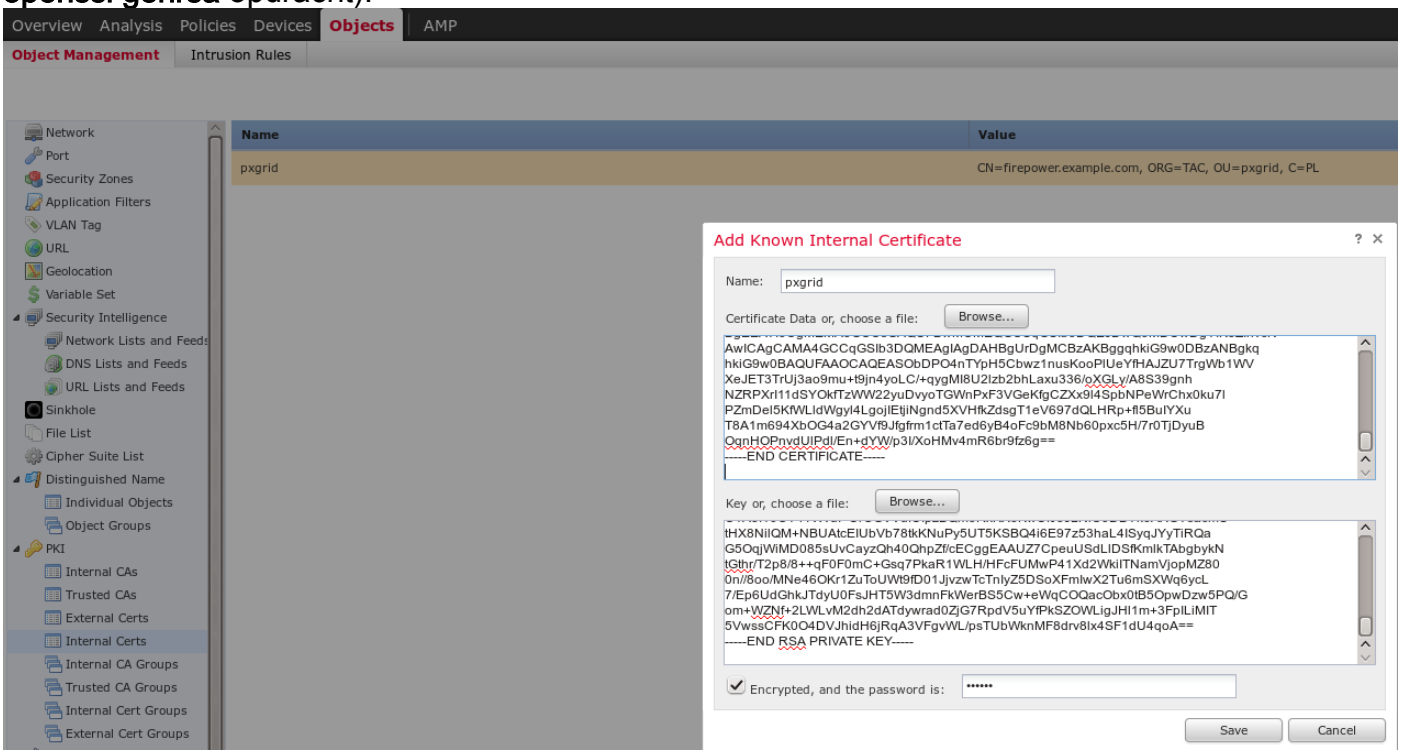
Een CA-certificaat moet worden toegevoegd aan een vertrouwde winkel:



De laatste stap is het genereren van het PxGrid-certificaat dat door FMC gebruikt wordt om toestemming te geven aan ISE PxGrid-service. Om CSR CLI te genereren moet worden gebruikt (of een andere externe machine met openssl-gereedschap).

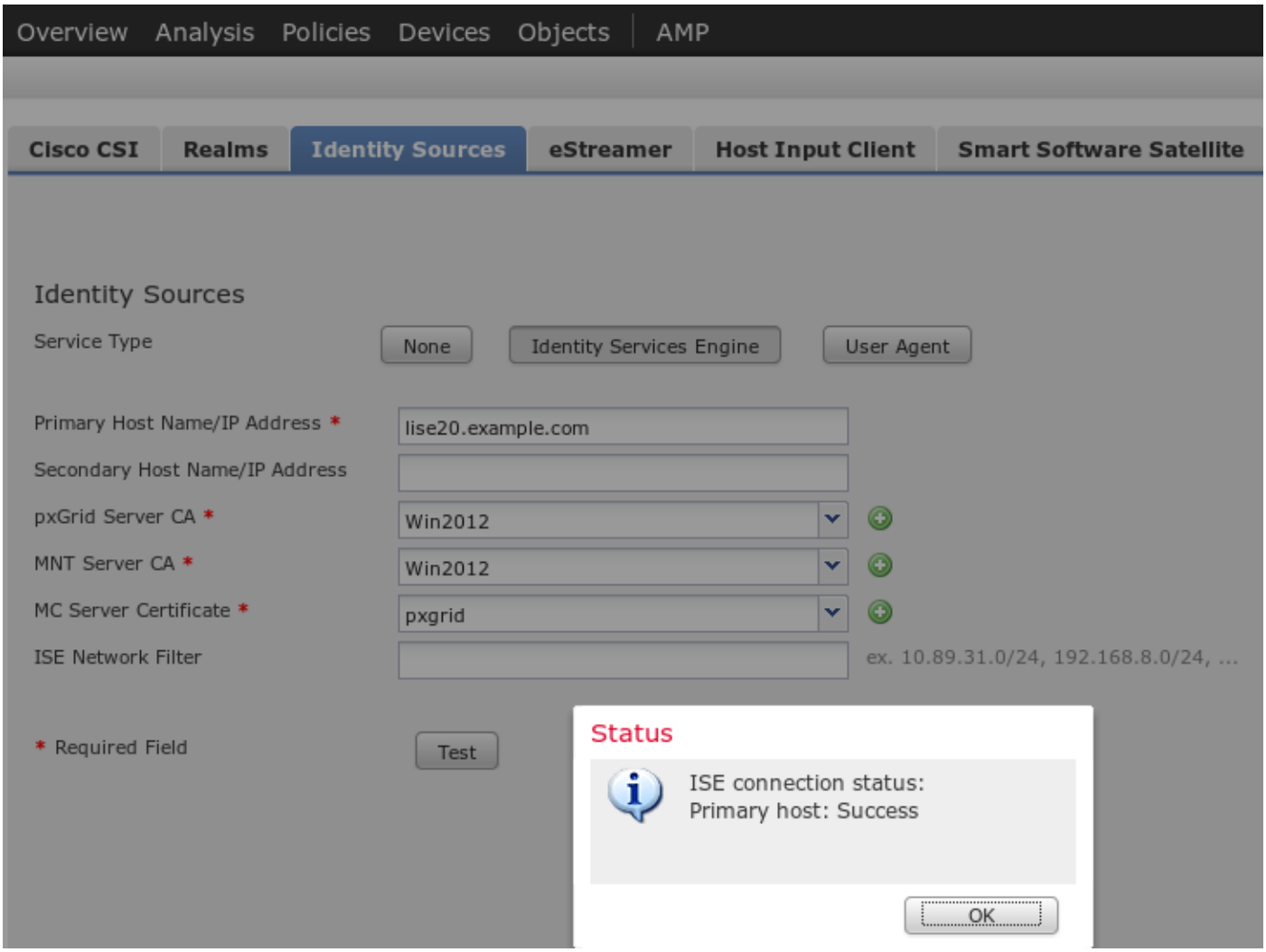
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#
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:~#
```

Zodra het vuur.csr is gegenereerd, teken het met Microsoft CA (pxGrid-sjabloon). Import van privé-sleutel (Fire.key) en ondertekend certificaat (fire.pem) naar FMC Interne certificaatwinkel. Gebruik voor privé-toets het wachtwoord dat is ingesteld tijdens het genereren van de toets (**openssl genrsa** opdracht):



ISE-integratie

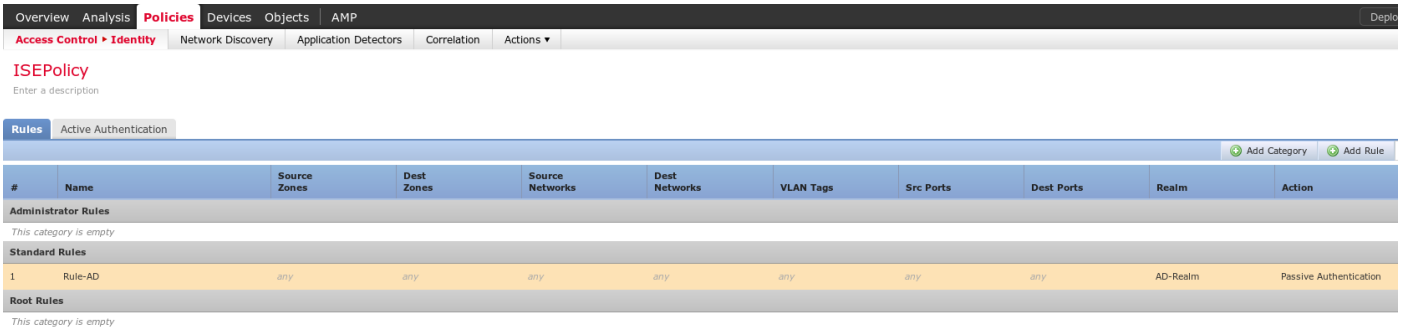
Nadat alle certificaten zijn geïnstalleerd moet u ISE-integratie vanaf **System > Integration** configureren:



Gebruik de geïmporteerde CA voor zowel PxGrid- als MnT-servicecertificaten. Gebruik voor Management Console (MC) intern certificaat dat gegenereerd is voor pxGrid.

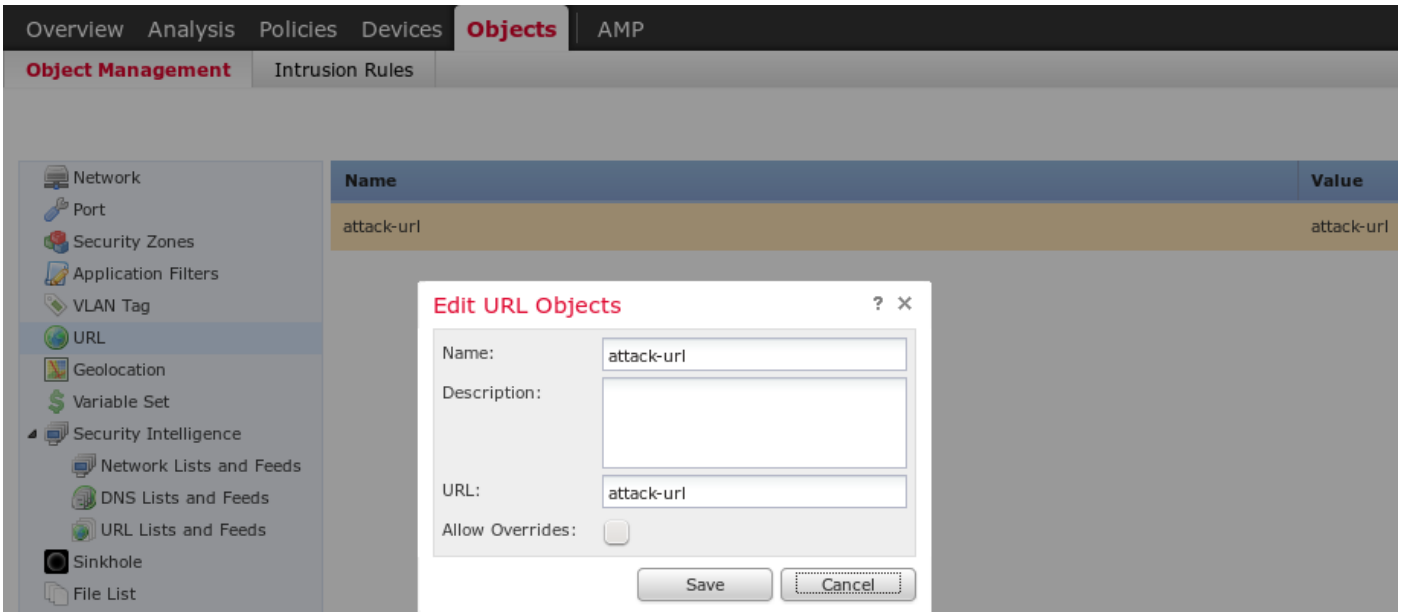
identiteitsbeleid

Configureer het identiteitsbeleid dat eerder ingesteld AD-teken gebruikt voor passieve verificatie:

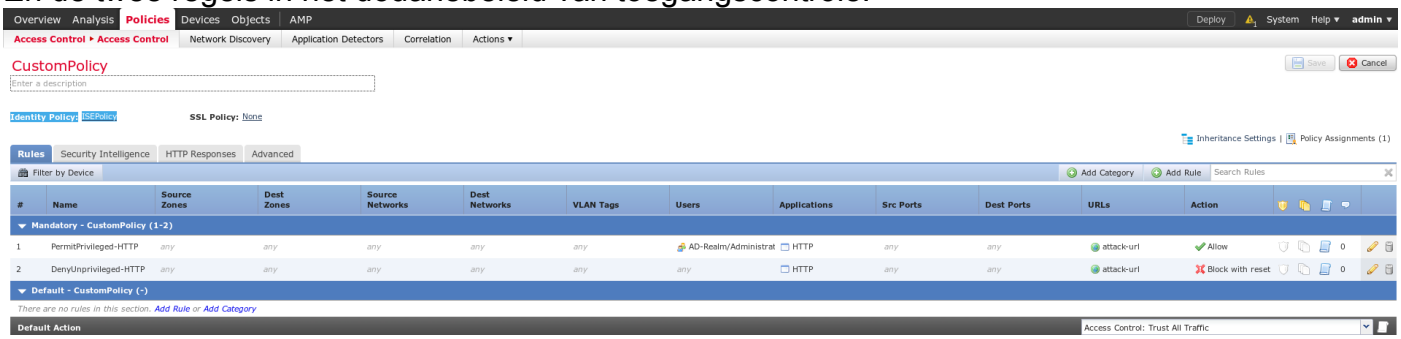


Toegangsbeheerbeleid

Dit voorbeeld is de aangepaste URL gemaakt:



En de twee regels in het douanebeleid van toegangscontrole:

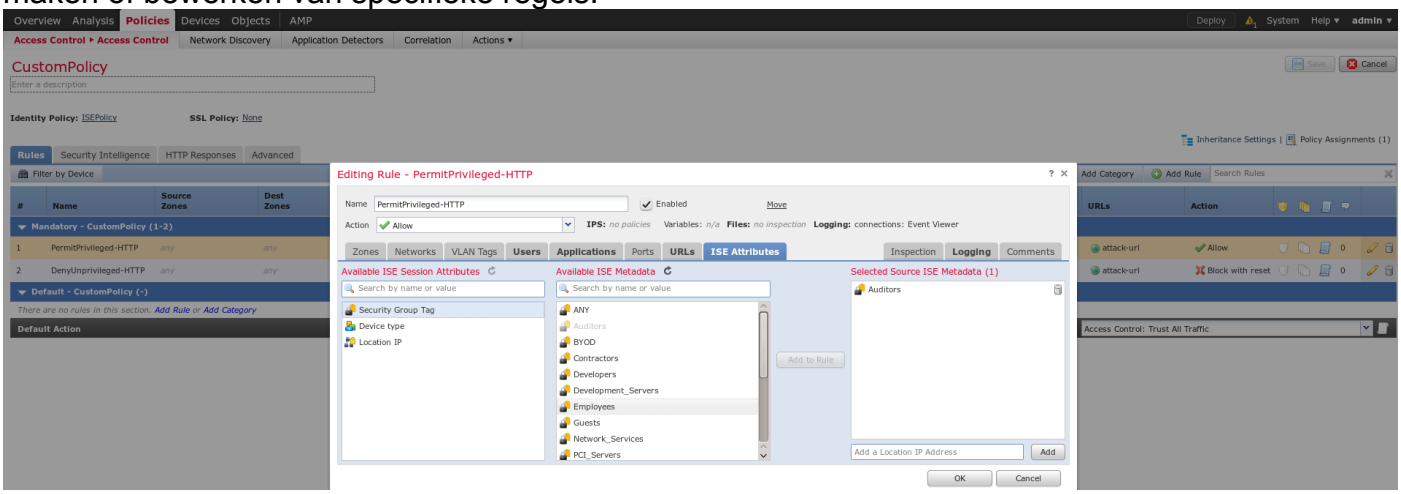


PermitPrivileged-HTTP-regel staat alle gebruikers toe die tot AD Administrators groep behoren die SGT-tag hebben gekregen. Accountants om HTTP-aanval op alle doelen uit te voeren.

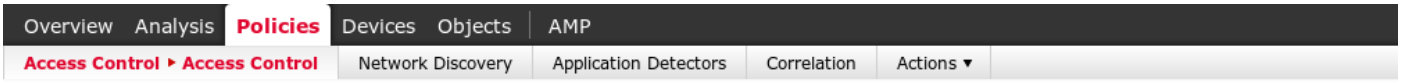
DenyUnbevoorrechte-HTTP ontkent die actie aan alle andere gebruikers.

Let ook op dat het vorige Identity Policy is toegewezen aan dit Access Control Policy.

Op dit tabblad is het niet mogelijk om SGT-tags te zien, maar deze zijn zichtbaar tijdens het maken of bewerken van specifieke regels:

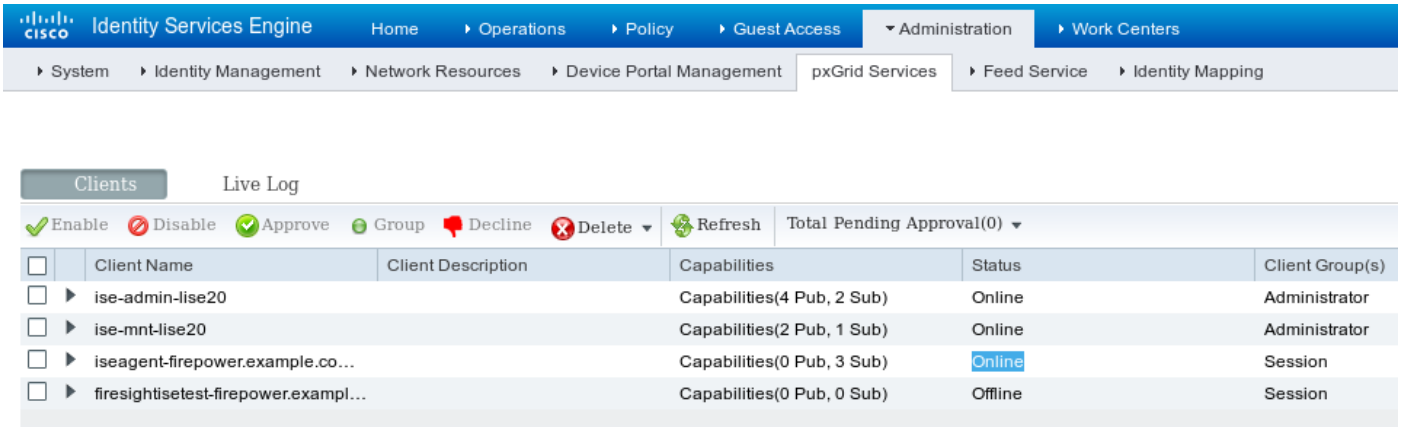


Zorg ervoor dat het beleid aan het NGIPS wordt toegewezen en alle wijzigingen worden uitgevoerd:

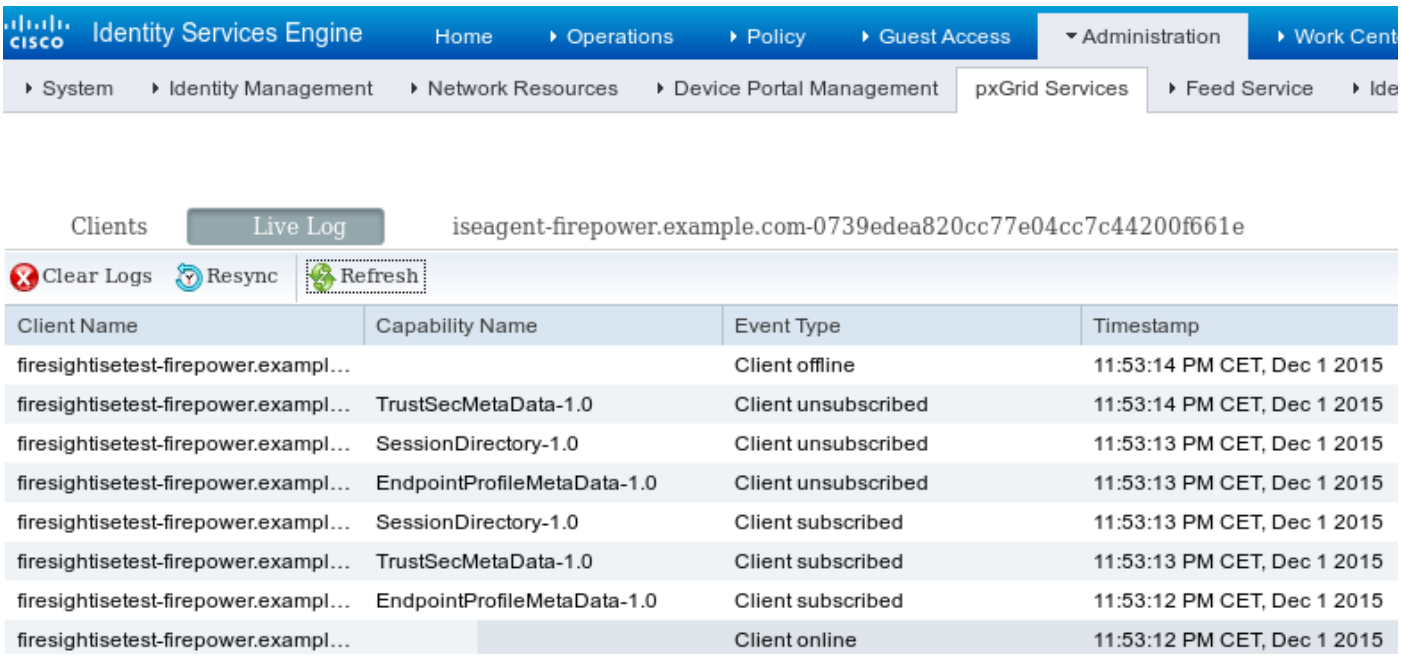


Verifiëren

Nadat alles correct is geconfigureerd zou ISE PxGrid-client moeten intekenen voor een sessieservice (status online).



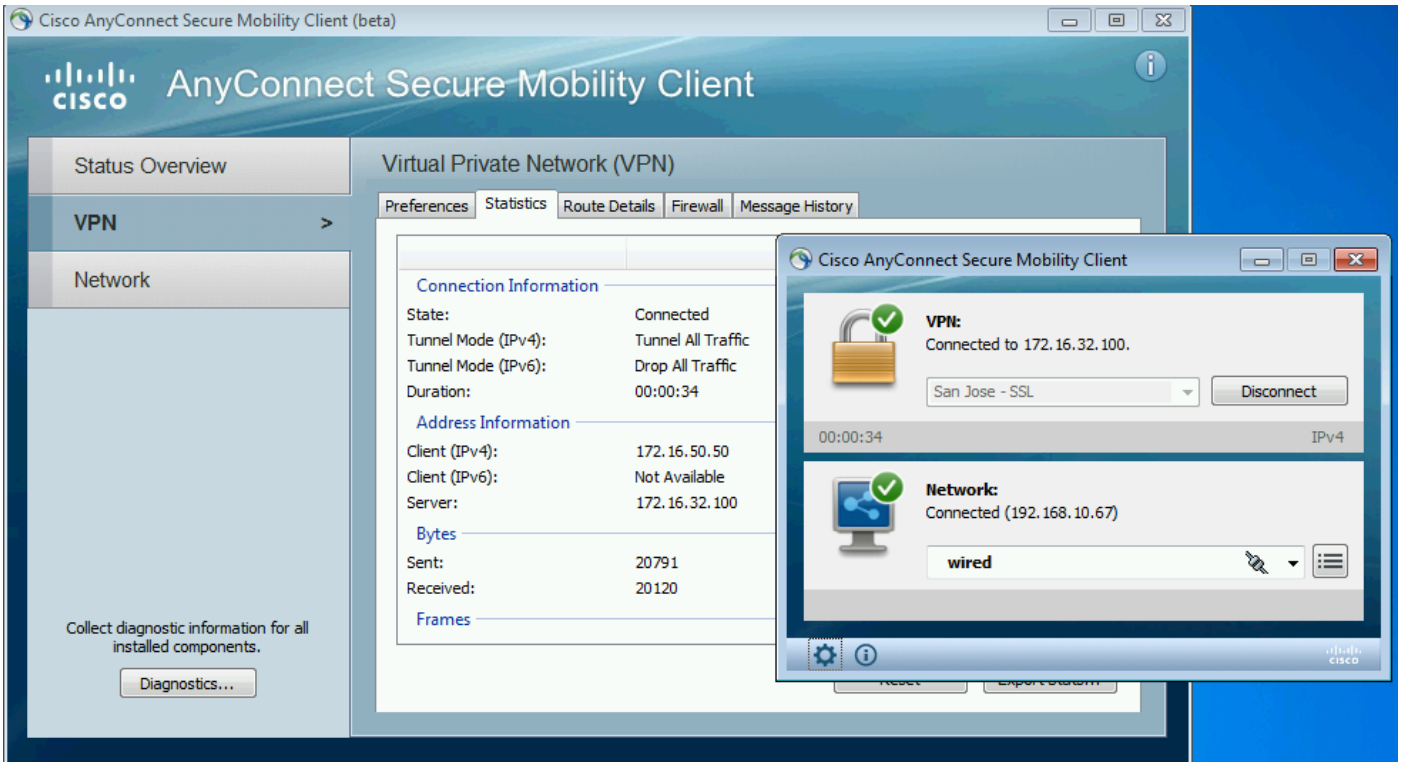
Uit de logbestanden kan ook worden bevestigd dat FMC zich heeft geabonneerd voor de service TrustSecMetaData (SGT-tags) - alle tags heeft ontvangen en niet heeft geabonneerd.



VPN-sessieinstelling

De eerste test wordt uitgevoerd bij een scenario waarbij de vergunning op ISE niet de juiste SGT-tag teruggeeft (NGIPS staat geen audittests toe).

Zodra VPN-sessie is UP kan AnyConnect User Interface (UI) meer details bieden:



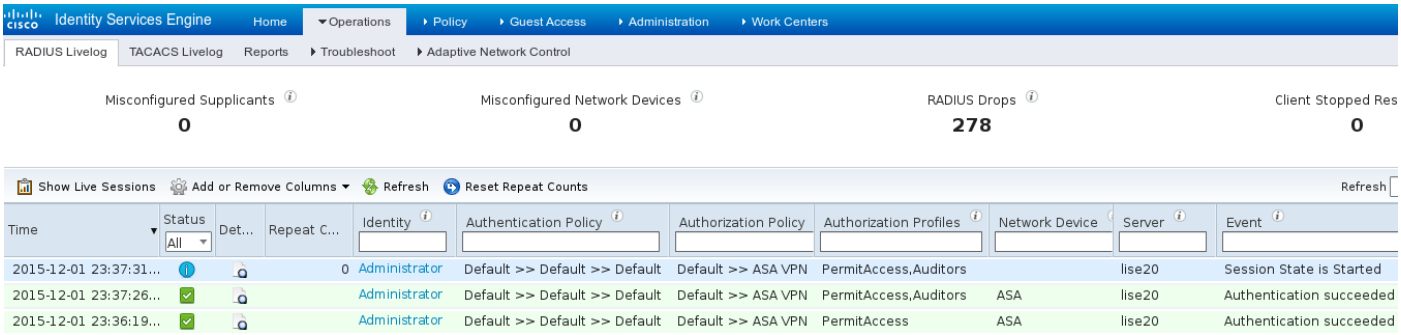
ASA kan bevestigen dat de sessie is vastgesteld:

```
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
```

Merk op dat ASA een SGT-tag voor deze verificatie ziet. ASA is niet ingesteld voor TrustSec - dus wordt de informatie toch overgeslagen.

ISE rapporteert ook over een succesvolle vergunning (het logboek om 23:36:19) - er is geen SGT-tag teruggegeven:



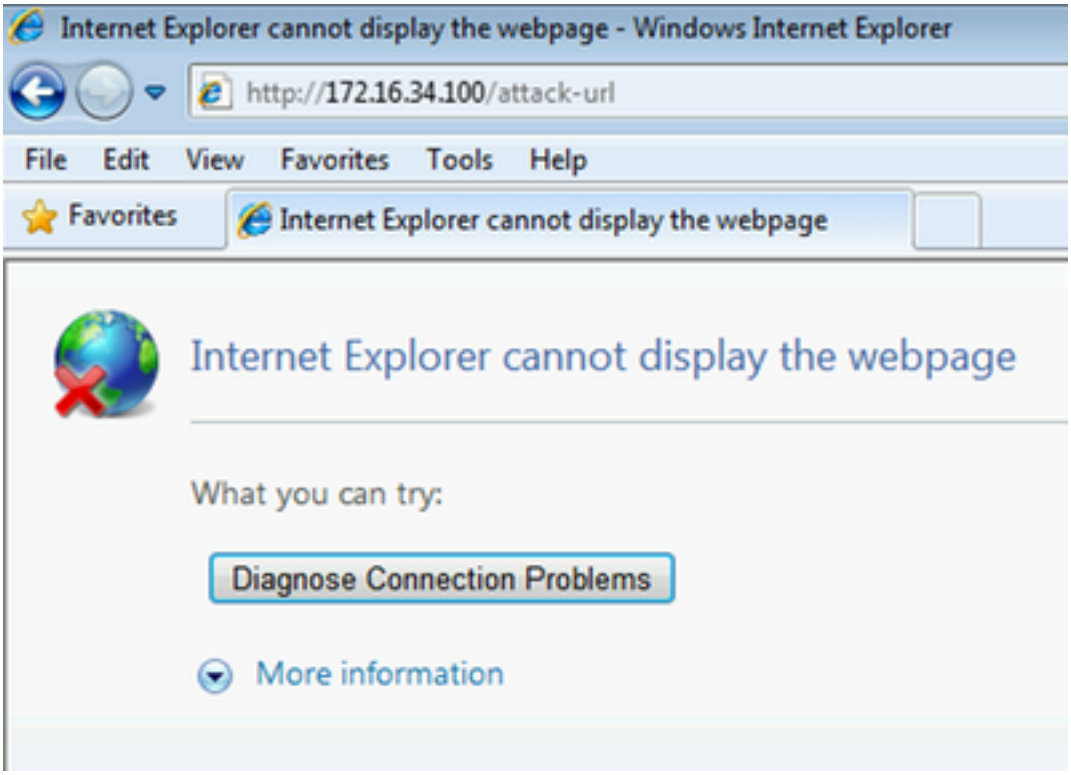
FMC krijgt sessiegegevens van MnT

In die fase rapporteert FMC in /var/log/messen een nieuwe sessie (ontvangen als abonnee voor pxGrid-service) voor Administrator-gebruikersnaam en AD-raadpleging voor groepslidmaatschap:

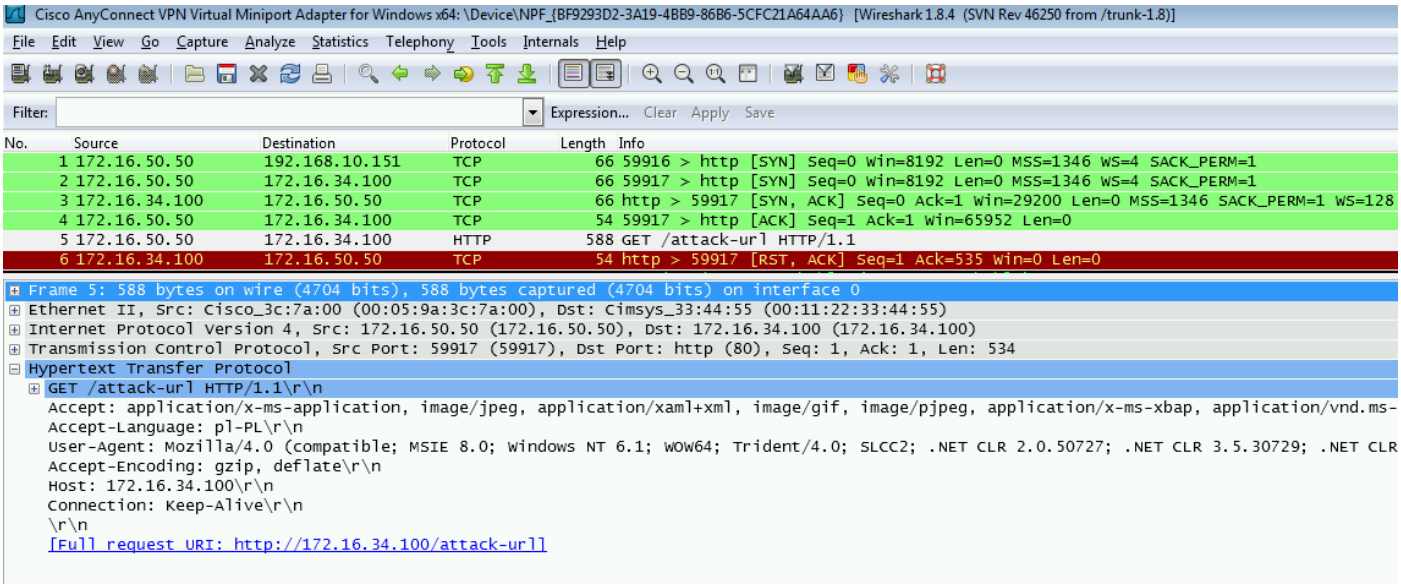
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

Onbevoorrechte en bevoorrechte netwerktoegang

Wanneer de gebruiker in dat stadium probeert een webbrowser te openen en een door een toegangscontrole gecontroleerde server te openen, wordt de verbinding beëindigd:



Het kan worden bevestigd door de pakketvastlegging die van de client is genomen (TCP RST verzenden als per FMC-configuratie):

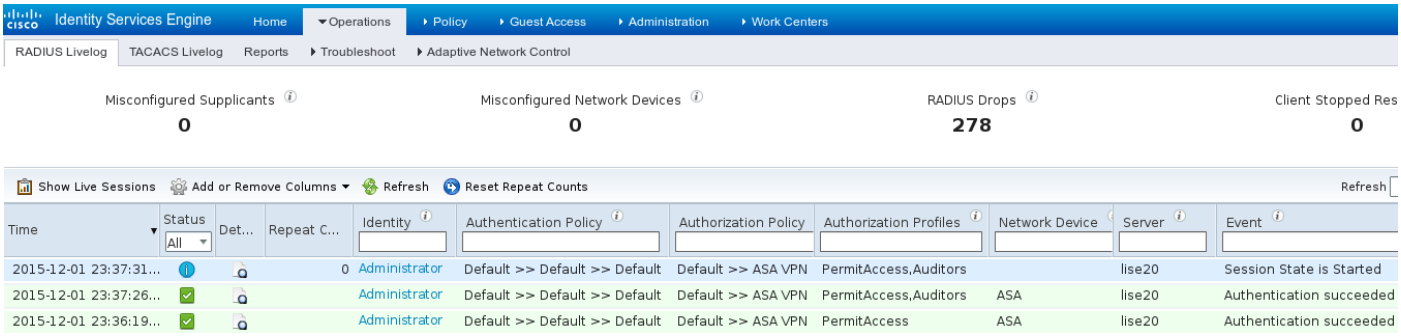


Zodra ISE is ingesteld om terug te keren, meldt de ASA-sessie van de audit:

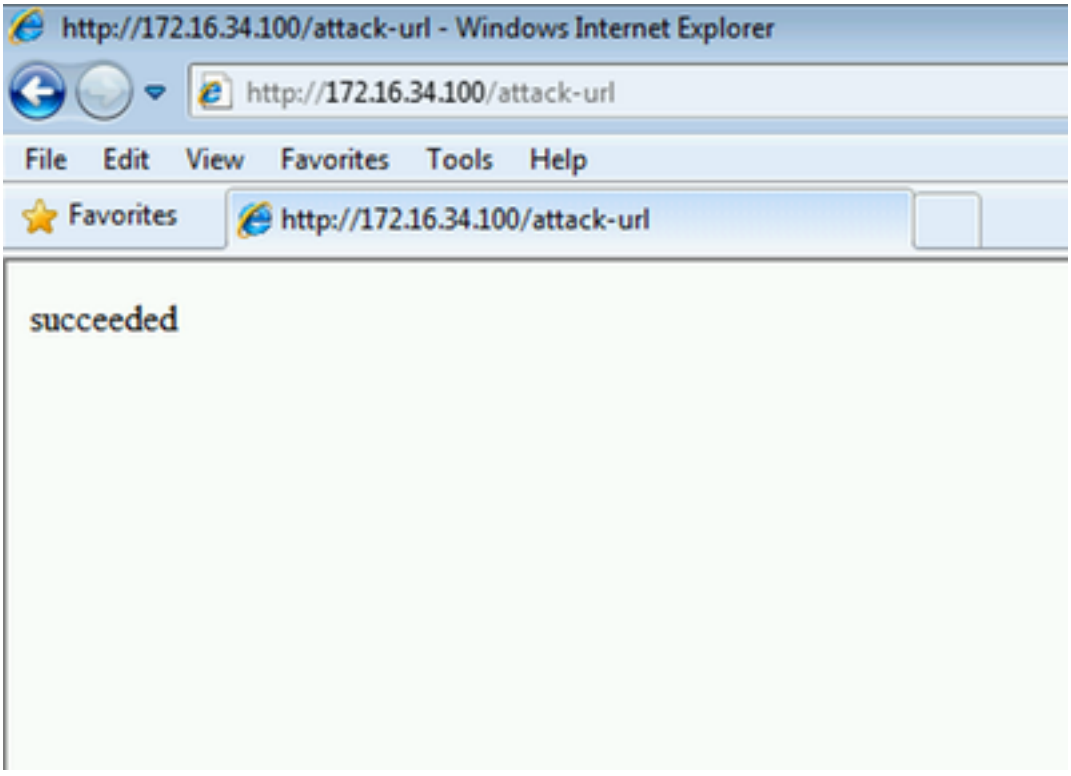
```
asav# show vpn-sessiondb anyconnect

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
```

ISE meldt ook een geslaagde vergunning (het logboek om 23:37:26) - SGT-tag Auditor wordt

teruggegeven:

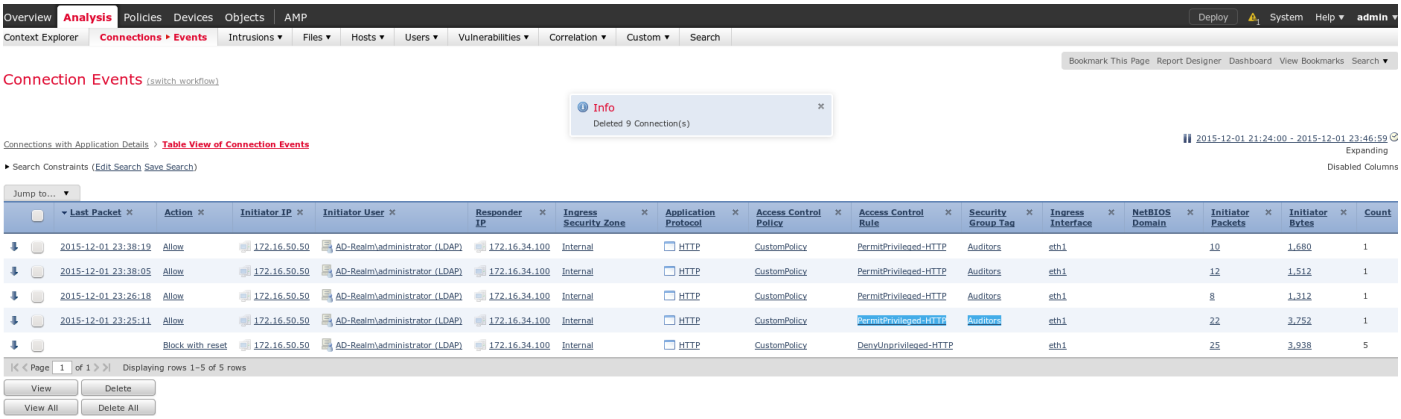


En de gebruiker kan de genoemde service benaderen:



FMC-logtoegang

Deze activiteit kan worden bevestigd door het verbindingsrapport:



Eerst had de gebruiker geen SGT-tag toegewezen en pakte hij de DenyUnbevoorrechte-HTTP-regel in. Zodra de tag van de auditor door ISE (en opgehaald door FMC) is toegewezen, wordt PermitPrivileged-HTTP gebruikt en is toegang toegestaan.

Merk ook op dat om de weergave te hebben, meerdere kolommen zijn verwijderd omdat normaal gesproken toegangscontroleregel en beveiligingsgroepmarkering worden weergegeven als een van de laatste kolommen (en er moet een horizontale schuifbalk worden gebruikt). Deze aangepaste weergave kan in de toekomst worden opgeslagen en opnieuw worden gebruikt.

Problemen oplossen

FMC-uiteinden

U kunt de loggen van de adi-component die verantwoordelijk is voor de identiteitsdiensten, als volgt controleren:

```
[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
```

Om gedetailleerdere uitwerpselen te krijgen is het mogelijk om adi-proces te doden (van wortel na eind) en het te draaien met debug argument:

```
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.......>
```

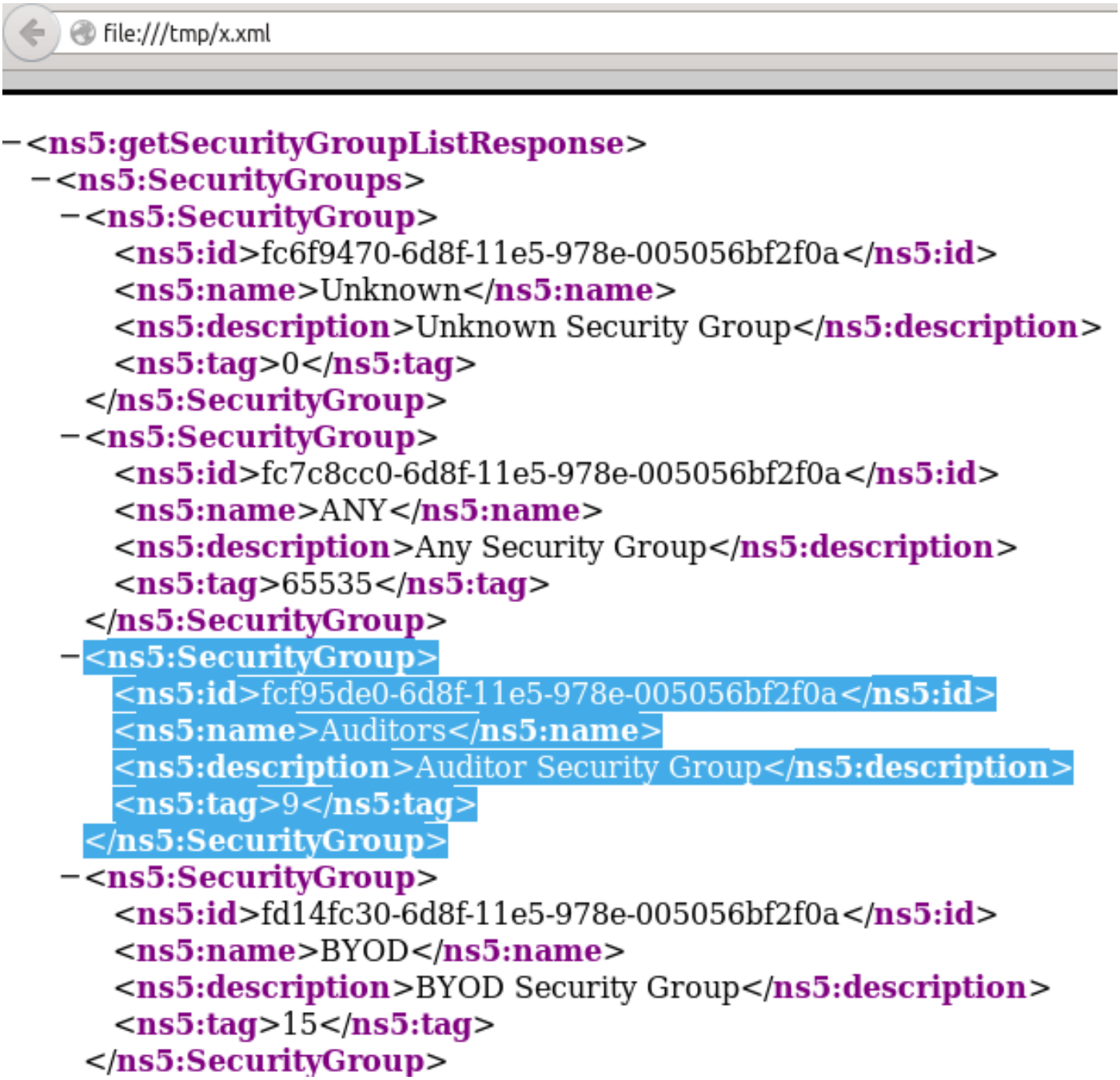
SGT query via pxGrid

De bewerking wordt uitgevoerd wanneer op de **Test**-knop wordt gedrukt in **ISE Integration** sectie of wanneer de SGT-lijst wordt ververst, terwijl regels in Access Control Policy worden toegevoegd.

```
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>fe2d22f0-6d8f-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>fe487320-6d8f-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>fe62d8f0-6d8f-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>fe7d3ec0-6d8f-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>fe99c770-6d8f-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:getSecurityGroupListResponse>]

Voor een beter beeld kunt u de inhoud van xml uit dat logbestand kopiëren naar xml-bestand en openen door een webbrowser. U kunt bevestigen dat specifieke SGT (audit) wordt ontvangen evenals alle andere SGT die op ISE is gedefinieerd:



Session query via REST API voor MnT

Dat is ook een onderdeel van Test operation (noteer dat MnT hostname en poort via pxGrid wordt doorgegeven). Downloadsessie:

```
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>
```

En ontkoppeld resultaat (1 actieve sessie ontvangen):

```
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}
```

In die fase probeert NGIPS die gebruikersnaam (en domein) te correleren met Realm-AD-gebruikersnaam:

```
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
```

LDAP wordt gebruikt om een gebruiker- en groepslidmaatschap te vinden:

```
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-debugs

Nadat u TRACE level-debug voor pxGrid-component hebt ingeschakeld, kan deze elke handeling controleren (maar zonder payload/data zoals op FMC).

Voorbeeld met SGT-tagophalen:

```
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
```

Bugs

CSCuv3295 - ISE kan domeininformatie in gebruikersnaam-velden verzenden

CSCus53796 - Kan geen FQDN van host voor REST-bulkquery krijgen

CSCuv43145 - PXGRID & Identity mapping Service opnieuw opstarten, importeren/verwijderen van een trustwinkel

Referenties

- Remediatieservices met ISE en FirePower-integratie configureren
- PxGrid configureren in een gedistribueerde ISE-omgeving
- Hoe u certificaten kunt implementeren met Cisco PxGrid: De configuratie van CA-Ondertekende ISE PxGrid-knooppunt en CA-ondertekende PxGrid-client
- ISE versie 1.3 pxGrid-integratie met IPS PxLog toepassing
- Administrator-gids voor Cisco Identity Services Engine, release 2.0
- Referentiegids voor Cisco Identity Services Engine API, release 1.2 - Inleiding naar extern RESTful S...
- Referentiegids voor Cisco Identity Services Engine API, release 1.2 - Inleiding over de bewaking van SRE...
- Administrator-gids voor Cisco Identity Services Engine, release 1.3
- Technische ondersteuning en documentatie - Cisco-systemen