Fehlerbehebung bei ISE- und FirePOWER-Integration für Identity Services

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von TrustSec-Richtlinien auf dem Cisco Next Generation Intrusion Prevention System (NGIPS) (NGIPS). NGIPS 6.0 unterstützt die Integration mit Identity Services Engine (ISE), sodass identitätsbasierte Richtlinien erstellt werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- VPN-Konfiguration der Cisco Adaptive Security Appliance (ASA)
- Konfiguration des Cisco AnyConnect Secure Mobility Client
- Grundkonfiguration des Cisco FirePower Management Center
- Cisco ISE-Konfiguration
- Cisco TrustSec-Lösungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Konfigurieren

FirePower Management Center (FMC) ist die Managementplattform für FirePower. Es gibt zwei Arten von Funktionen für die ISE-Integration:

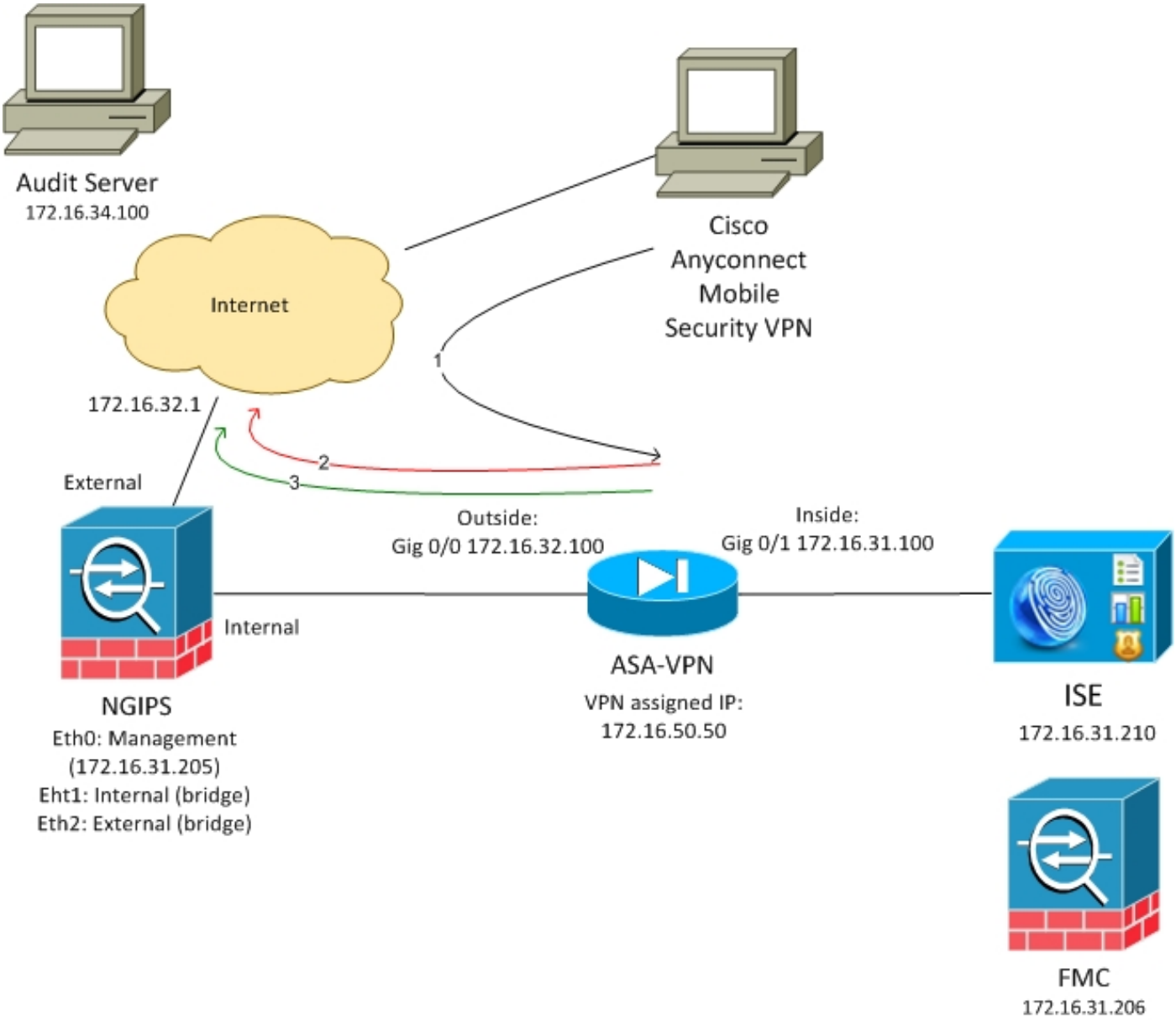
- Problembehebung - Ermöglicht FMC die Quarantäne des Angreifers über die ISE, die den Autorisierungsstatus auf dem Zugriffsgerät dynamisch ändert und einen begrenzten Netzwerkzugriff ermöglicht. Es gibt zwei Generationen dieser Lösung:

1. Legacy-Perl-Skript mit EPS-API-Aufruf (Endpoint Protection Service) für ISE.
2. Neueres Modul, das pxGrid-Protokoll-Aufruf für ISE (dieses Modul wird nur in Version 5.4 unterstützt - nicht in 6.0, native Unterstützung in 6.1 geplant).

- Richtlinie - Ermöglicht der FMC die Konfiguration von Richtlinien auf der Grundlage von TrustSec Security Group Tags (SGT).

Dieser Artikel konzentriert sich auf die zweite Funktionalität. Ein Beispiel zur Problembehebung finden Sie im Abschnitt zu Referenzen.

Netzwerkdiagramm



Das FMC wird mit einer Zugriffskontrollrichtlinie konfiguriert, die zwei Regeln enthält:

- Für HTTP-Datenverkehr mit benutzerdefinierter URL verweigern (Attach-URL)
- Zulassen von HTTP-Datenverkehr mit benutzerdefinierter URL (attack-url), jedoch nur, wenn der Benutzer dem Audit (9) SGT-Tag von der ISE zugewiesen wird

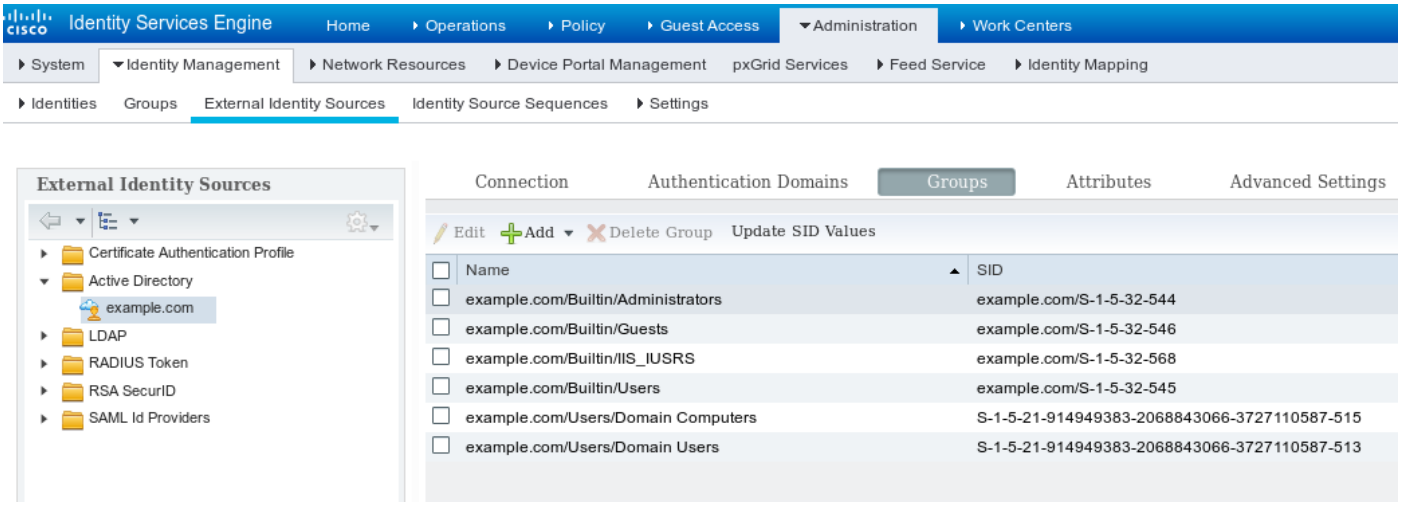
Die ISE beschließt, allen Active Directory-Benutzern, die der Administratorgruppe angehören, Audit-Tag zuzuweisen und verwendet das ASA-VPN-Gerät für den Netzwerkzugriff.

Der Benutzer greift über eine VPN-Verbindung auf das Netzwerk auf der ASA zu. Der Benutzer versucht dann, mithilfe von URL attack-url auf den überwachten Server zuzugreifen, schlägt aber fehl, weil er nicht der Audit SGT-Gruppe zugewiesen wurde. Sobald diese behoben ist, ist die Verbindung erfolgreich.

ISE

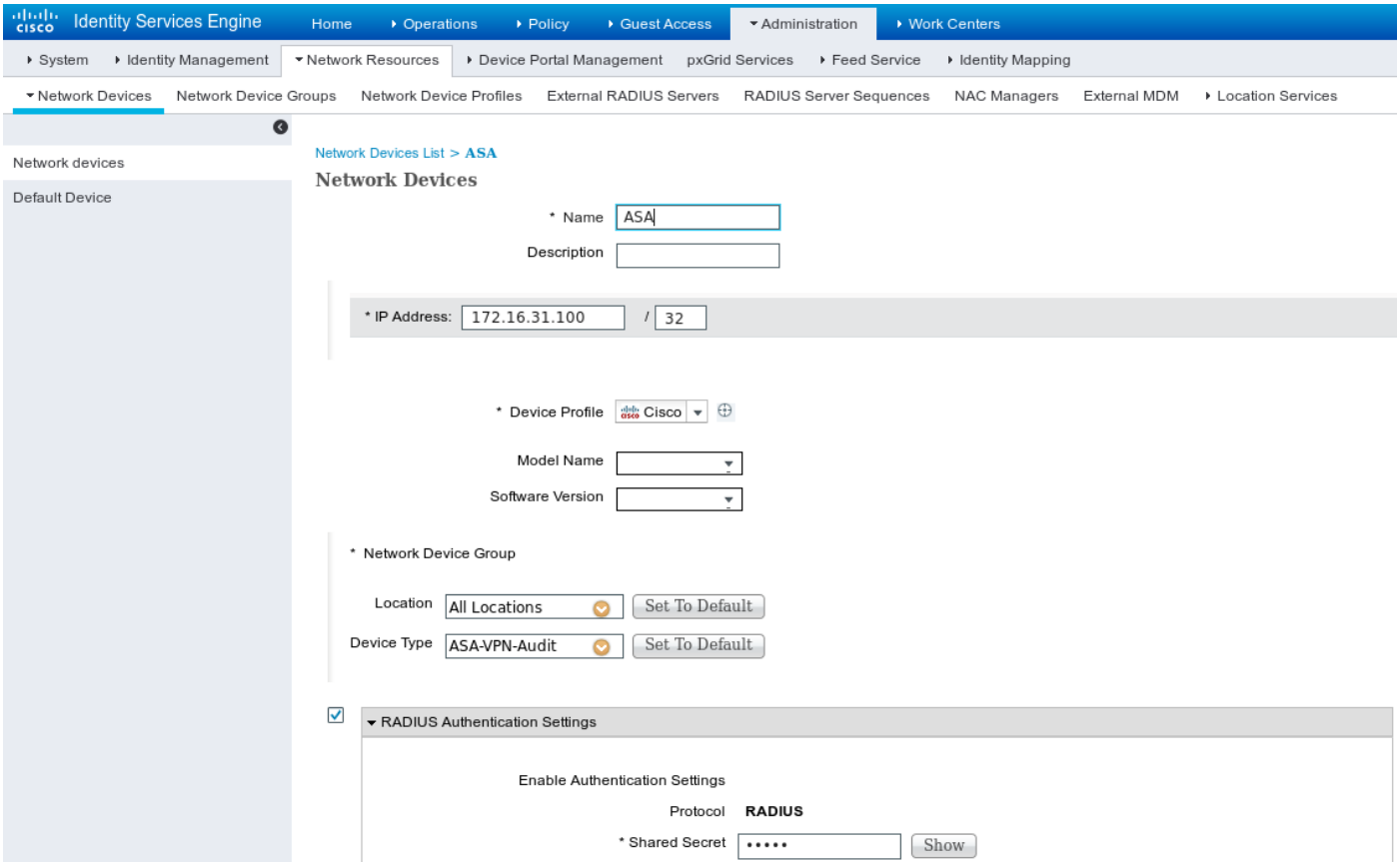
Active Directory

Die AD-Integration muss konfiguriert und die richtigen Gruppen abgerufen werden (für die Autorisierungsregel wird die Administratorgruppe verwendet):



Netzwerkzugriffsgerät

ASA wird als Netzwerkgerät hinzugefügt. Die benutzerdefinierte Gruppe ASA-VPN-Audit wird verwendet, wie in diesem Bild gezeigt:



Zertifikate für pxGrid und MnT

FMC nutzt beide Services auf der ISE:

- pxGrid für SGT und Profiling-Datenabfrage
- Überwachung und Reporting (MnT) für den Download von Massensitzungen

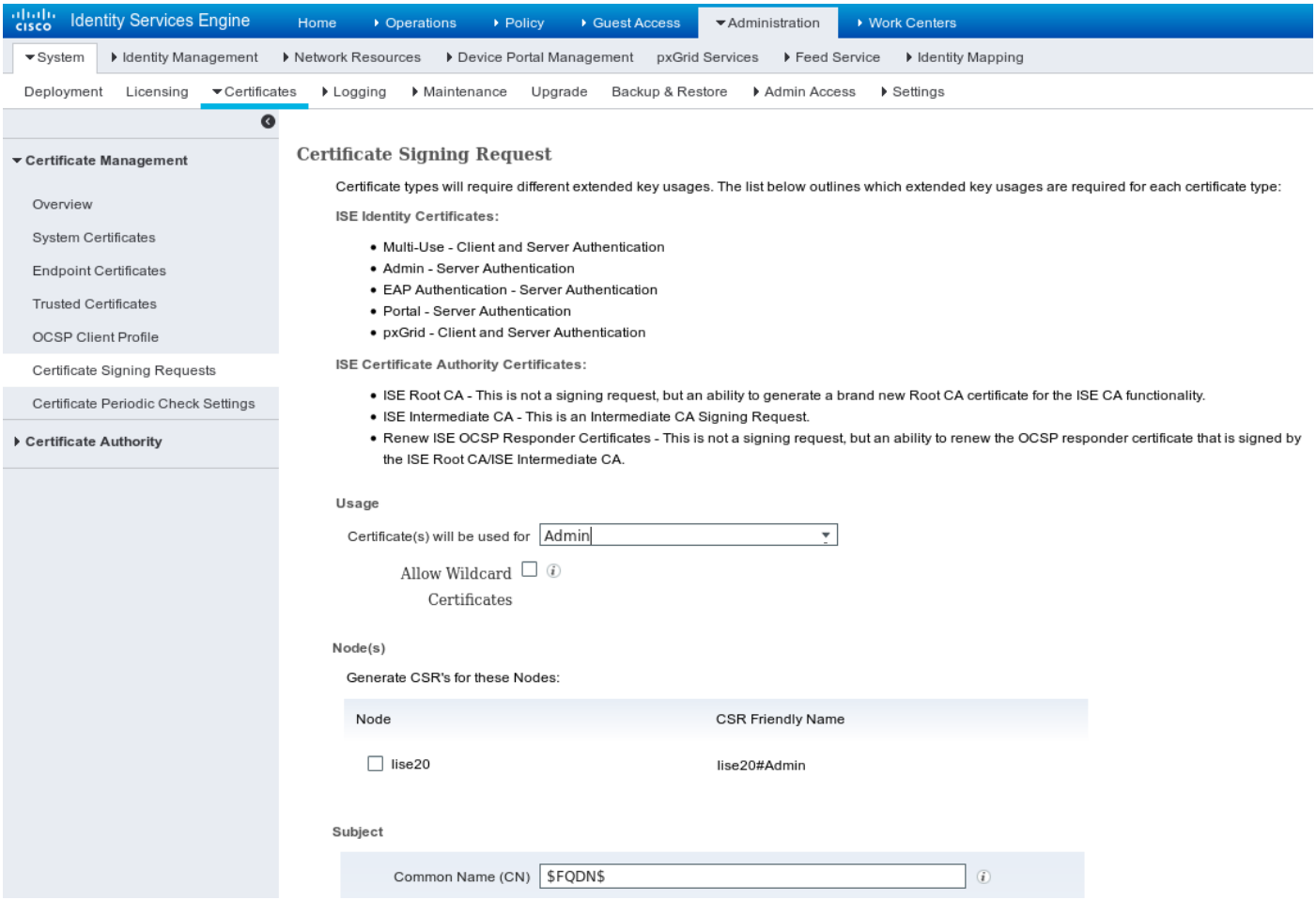
Die MnT-Verfügbarkeit ist sehr wichtig, da FMC auf diese Weise über die IP-Adresse der authentifizierten Sitzung informiert wird, auch über den Benutzernamen und das SGT-Tag. Auf dieser Grundlage können die richtigen Richtlinien angewendet werden. Bitte beachten Sie, dass

NGIPS keine nativen SGT-Tags (Inline-Tagging) wie die ASA unterstützt. Im Gegensatz zur ASA unterstützt sie jedoch nur SGT-Namen statt Zahlen.

Aufgrund dieser Anforderungen müssen sowohl ISE als auch FMC einander vertrauen (Zertifikat). MnT verwendet nur serverseitiges Zertifikat, pxGrid verwendet sowohl das clientseitige als auch das serverseitige Zertifikat.

Microsoft CA wird zum Signieren aller Zertifikate verwendet.

Für MnT (Admin-Rolle) muss die ISE, wie in diesem Bild gezeigt, eine Zertifikatssignierungsanfrage (CSR) generieren:



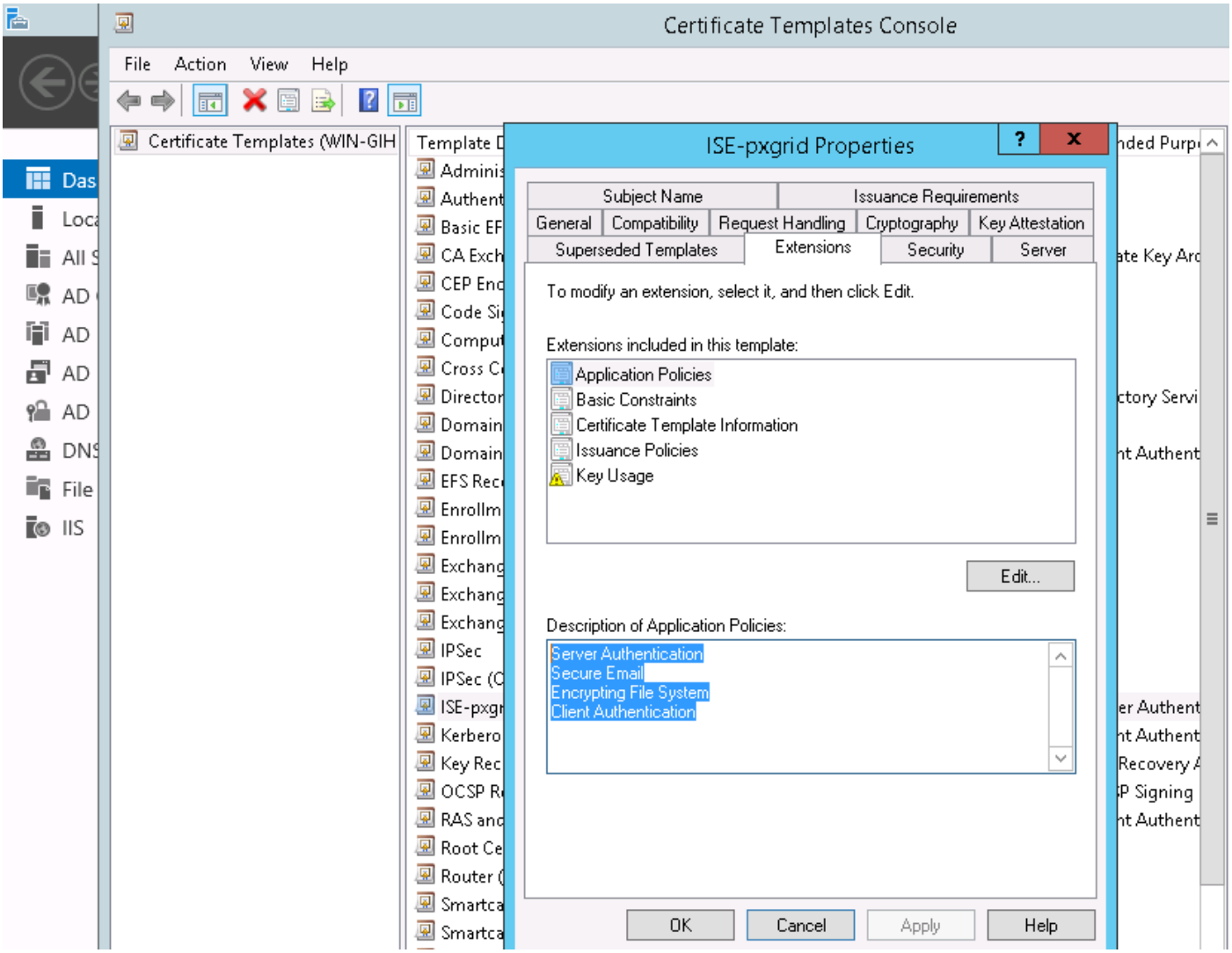
Nach der Signierung durch Microsoft CA muss der Import über die Option **Bind Certificate** erfolgen.

Ein ähnlicher Prozess muss für den pxGrid-Dienst befolgt werden. **Für die** Option **werden Zertifikate verwendet,** muss pxGrid ausgewählt sein.

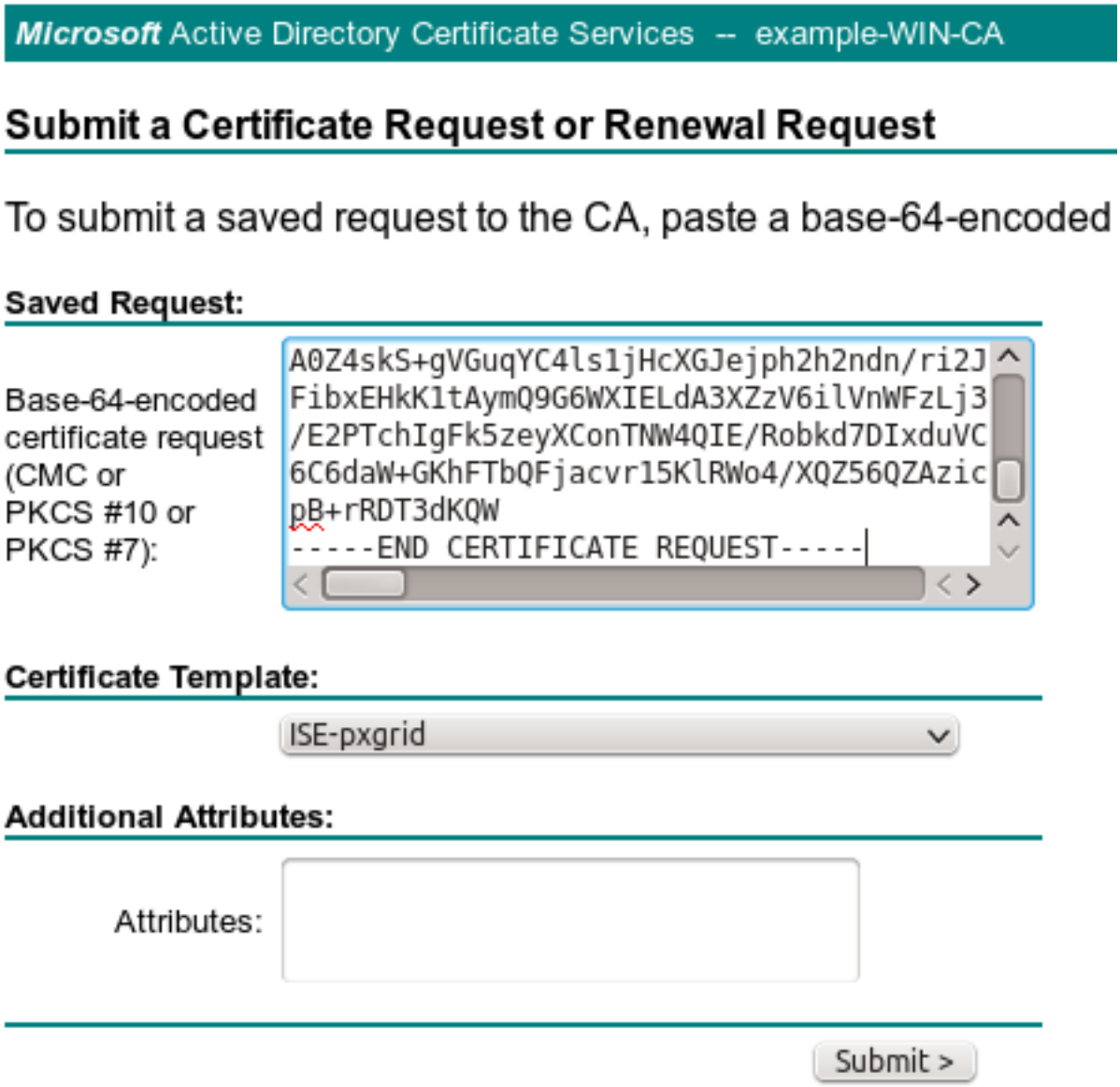
Da es nicht zwei Zertifikate mit identischem Betreffnamen geben kann, kann für den OU- oder O-Abschnitt (z. B. pxGrid) ein anderer Wert hinzugefügt werden.

> **Hinweis**: Stellen Sie sicher, dass für jeden vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) für ISE und FMC der richtige DNS-Datensatz auf dem DNS-Server konfiguriert wird.

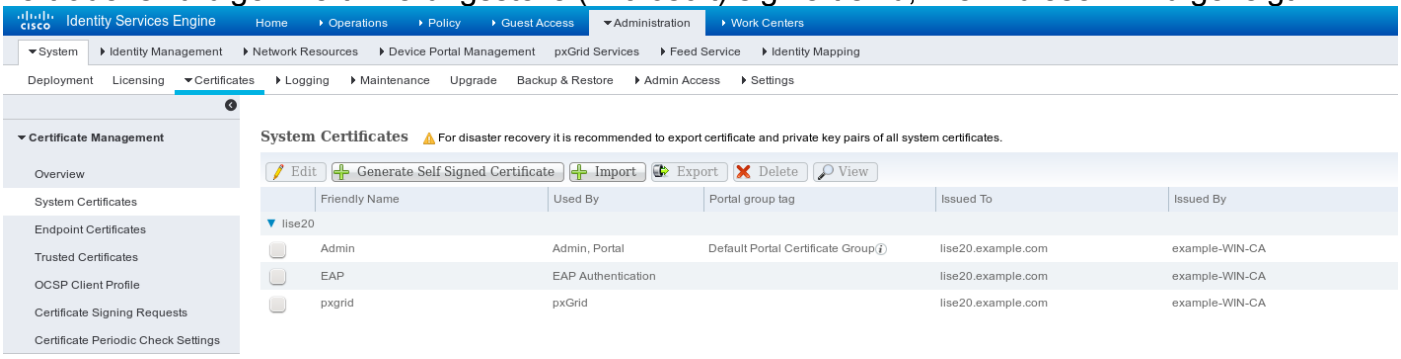
Der einzige Unterschied zwischen dem Admin- und dem pxGrid-Zertifikat besteht im Signierungsprozess. Da pxGrid-Zertifikate über Extended Key Usage-Optionen für die benutzerdefinierte Client- und Serverauthentifizierung in Microsoft CA verfügen müssen, können folgende Aufgaben durchgeführt werden:



In diesem Bild wird gezeigt, wie der Microsoft-Webdienst zum Signieren von pxGrid CSR verwendet wird:

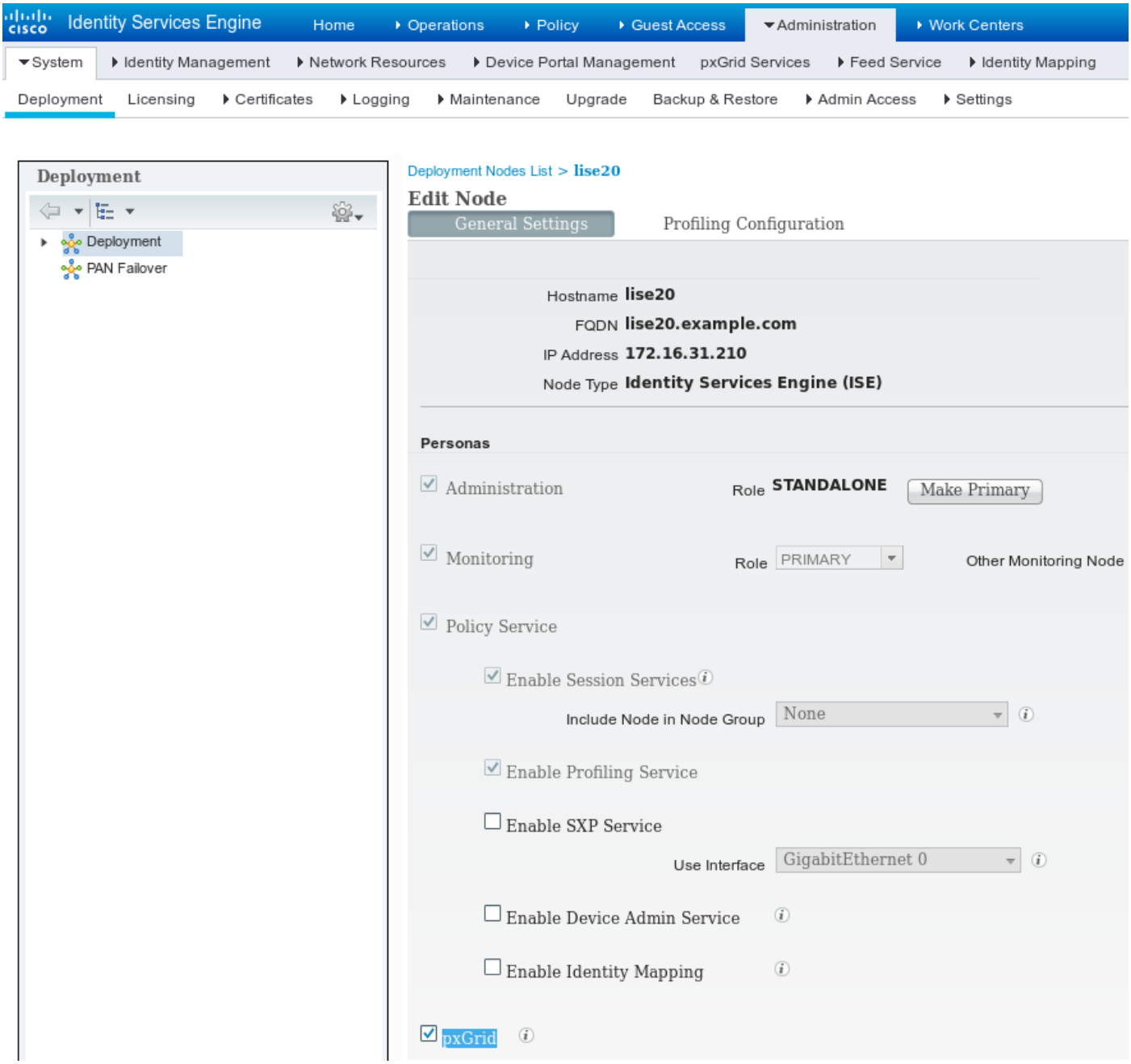


Am Ende muss die ISE über Admin- und pxGrid-Zertifikate verfügen, die von der vertrauenswürdigen Zertifizierungsstelle (Microsoft) signiert sind, wie in diesem Bild gezeigt:

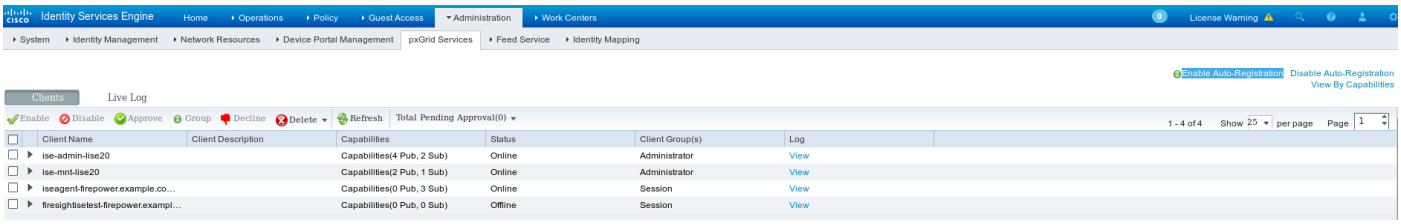


pxGrid-Service

Mit den richtigen Zertifikaten muss die pxGrid-Rolle für einen bestimmten Knoten aktiviert werden, wie in diesem Bild gezeigt:



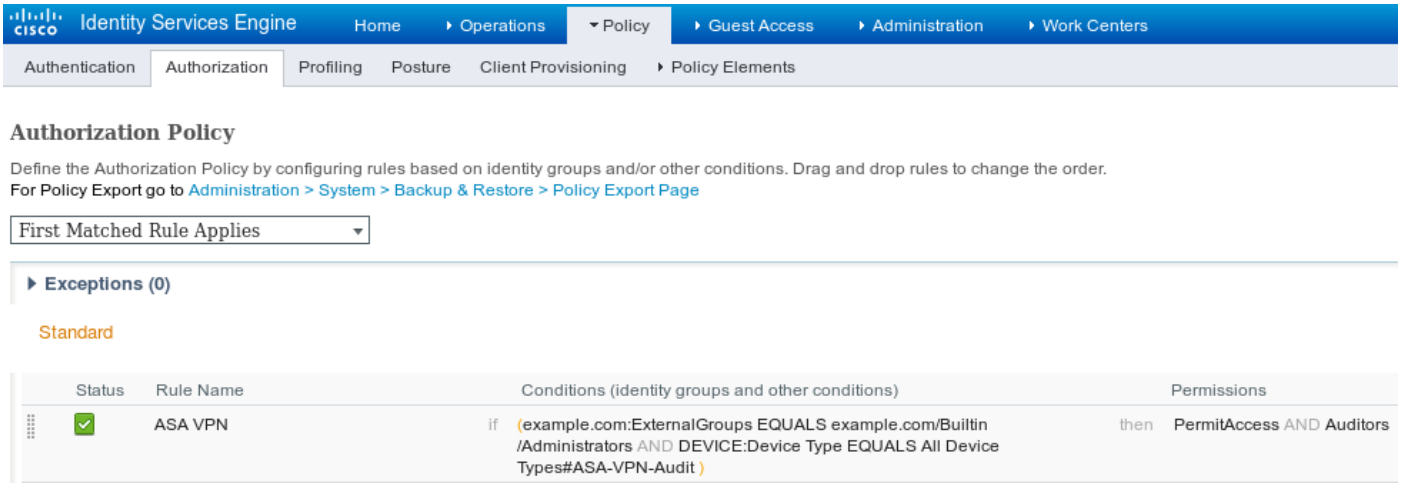
Die automatische Genehmigung muss aktiviert sein:



Autorisierungsrichtlinie

Die Standardauthentifizierungsrichtlinie wird verwendet (AD-Suche wird durchgeführt, wenn kein lokaler Benutzer gefunden wird).

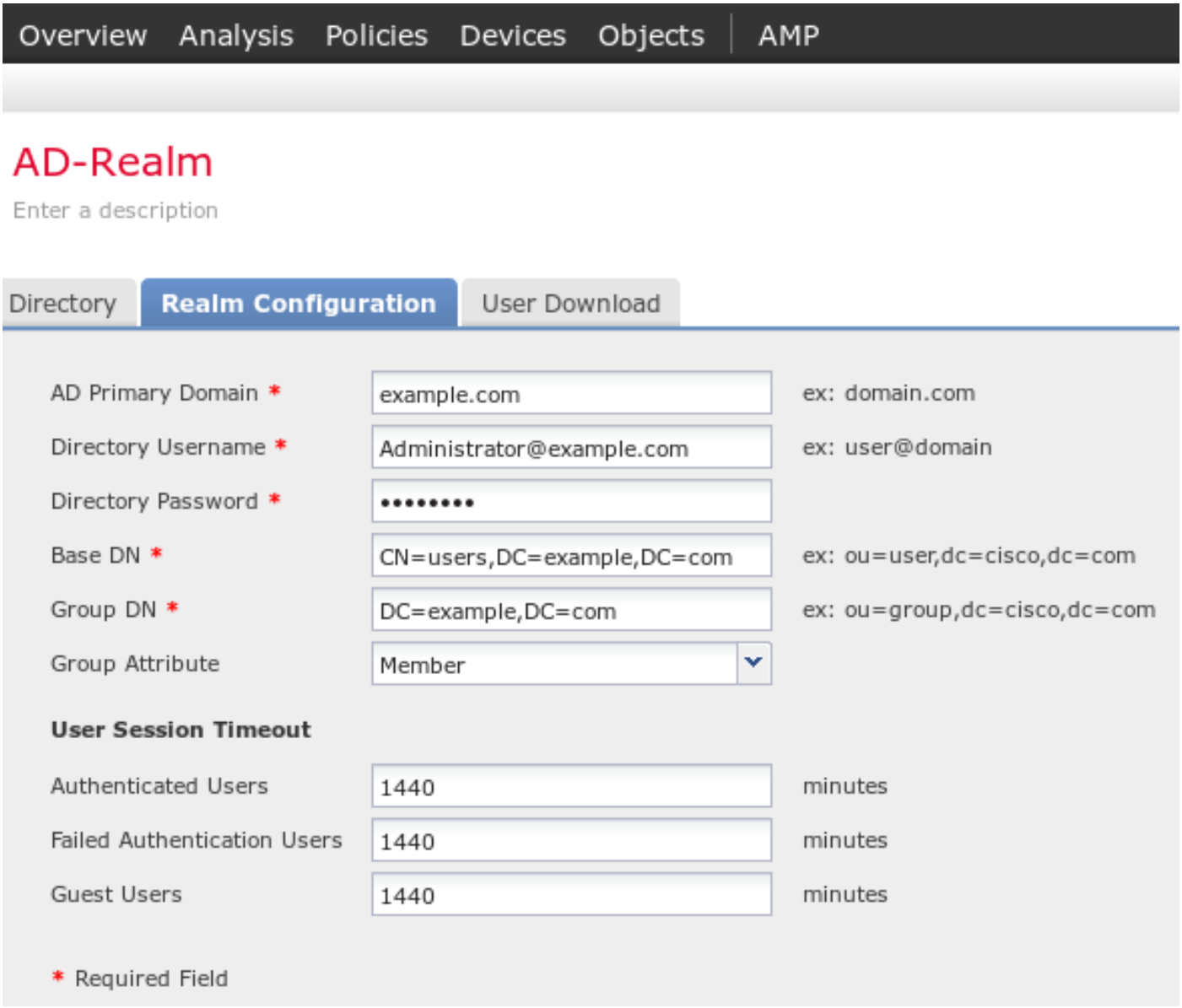
Die Autorisierungsrichtlinie wurde so konfiguriert, dass sie vollständigen Netzwerkzugriff bereitstellt (Berechtigung: PermitAccess) für Benutzer, die sich über ASA-VPN authentifizieren und zu Active Directory-Gruppenadministratoren gehören - für diese Benutzer werden SGT-Tag-Auditoren zurückgegeben:



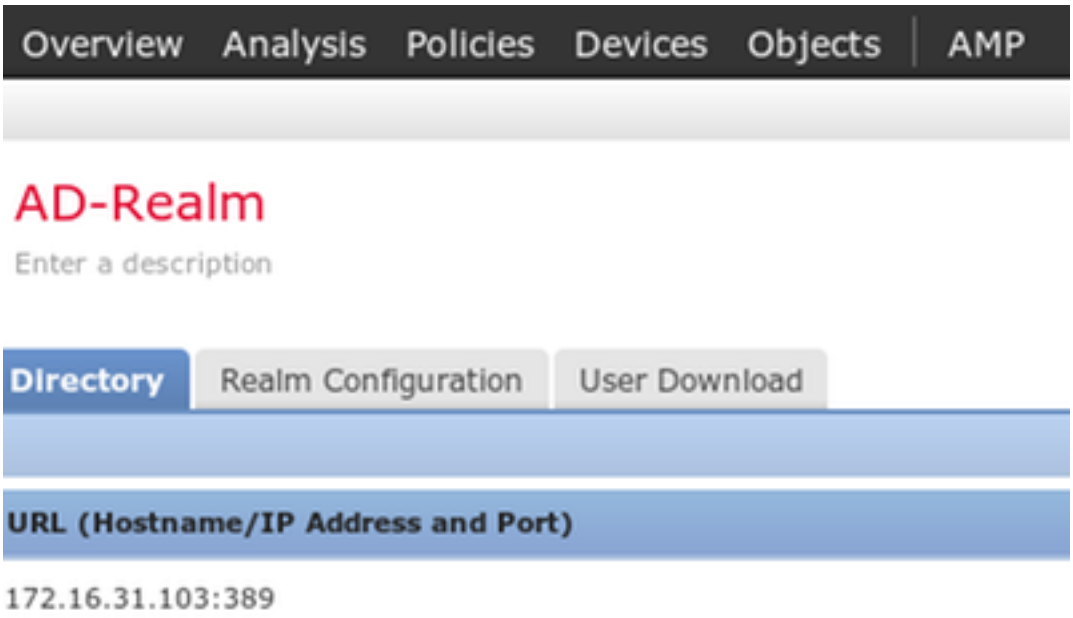
FMC

Active Directory-Bereich

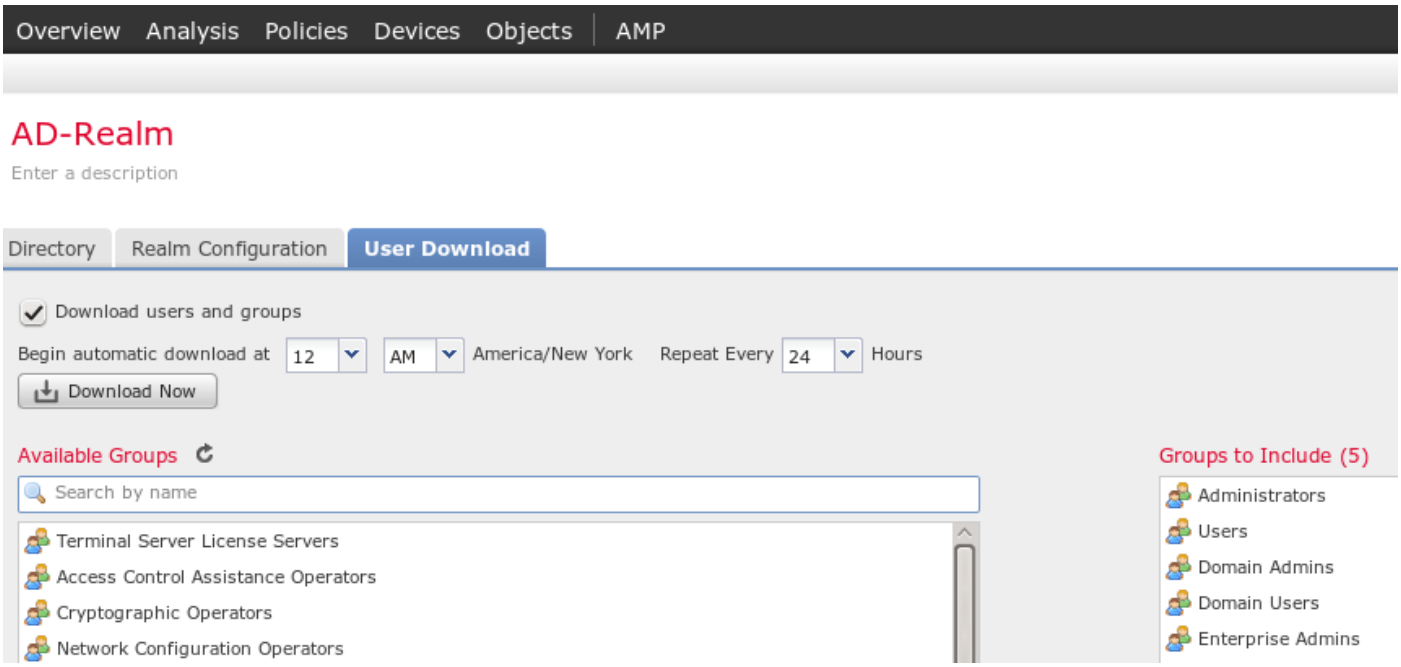
Für die ISE-Integration ist eine Bereichskonfiguration erforderlich (um Identitätsrichtlinien zu verwenden und die Gruppenmitgliedschaft für passiv authentifizierte Benutzer abzurufen). Der Bereich kann für Active Directory oder Lightweight Directory Access Protocol (LDAP) konfiguriert werden. In diesem Beispiel wird AD verwendet. Von **System > Integration > Bereich**:



Es werden folgende Standardverzeichniseinstellungen verwendet:

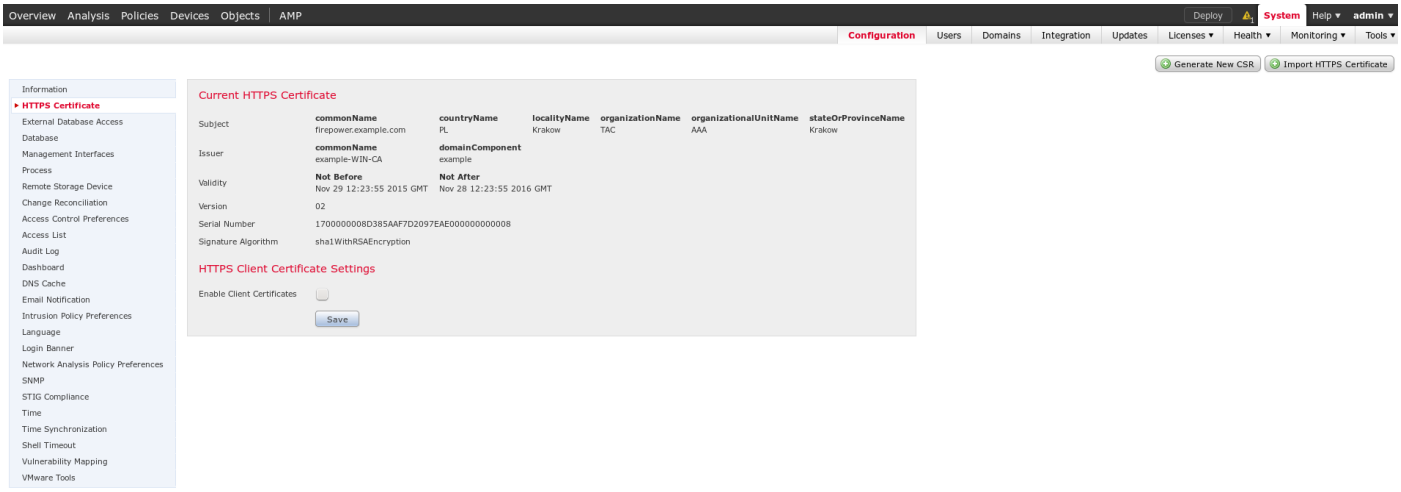


Einige AD-Gruppen werden abgerufen (als zusätzliche Bedingung in Zugriffskontrollregeln zu verwenden):

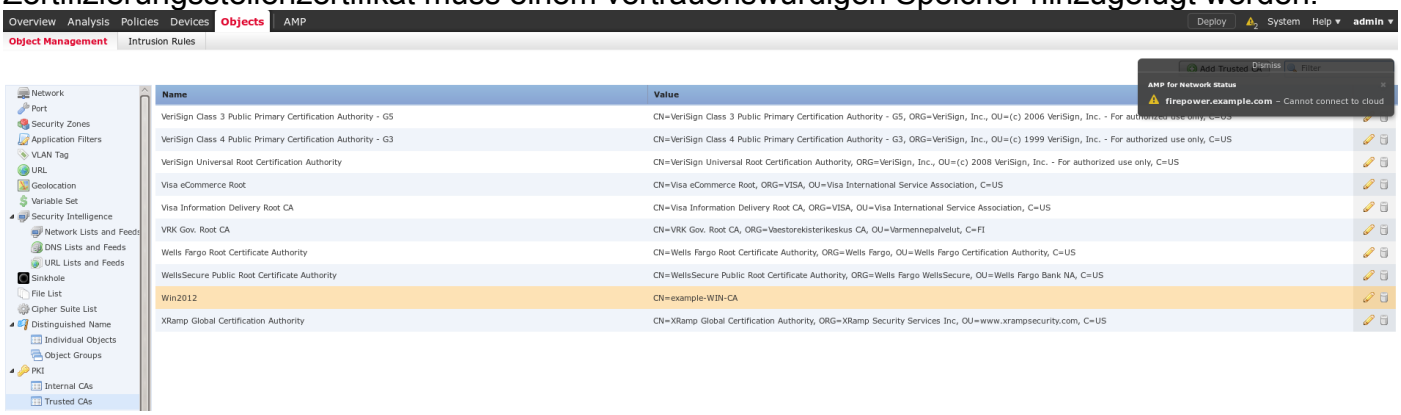


Zertifikate für Admin und pxGrid

Obwohl dies nicht erforderlich ist, empfiehlt es sich, CSR für den Administratorzugriff zu erstellen. Signieren Sie diese CSR-Anfrage mit vertrauenswürdigem AD, und importieren Sie das signierte Zertifikat zurück, wie in diesem Bild gezeigt:



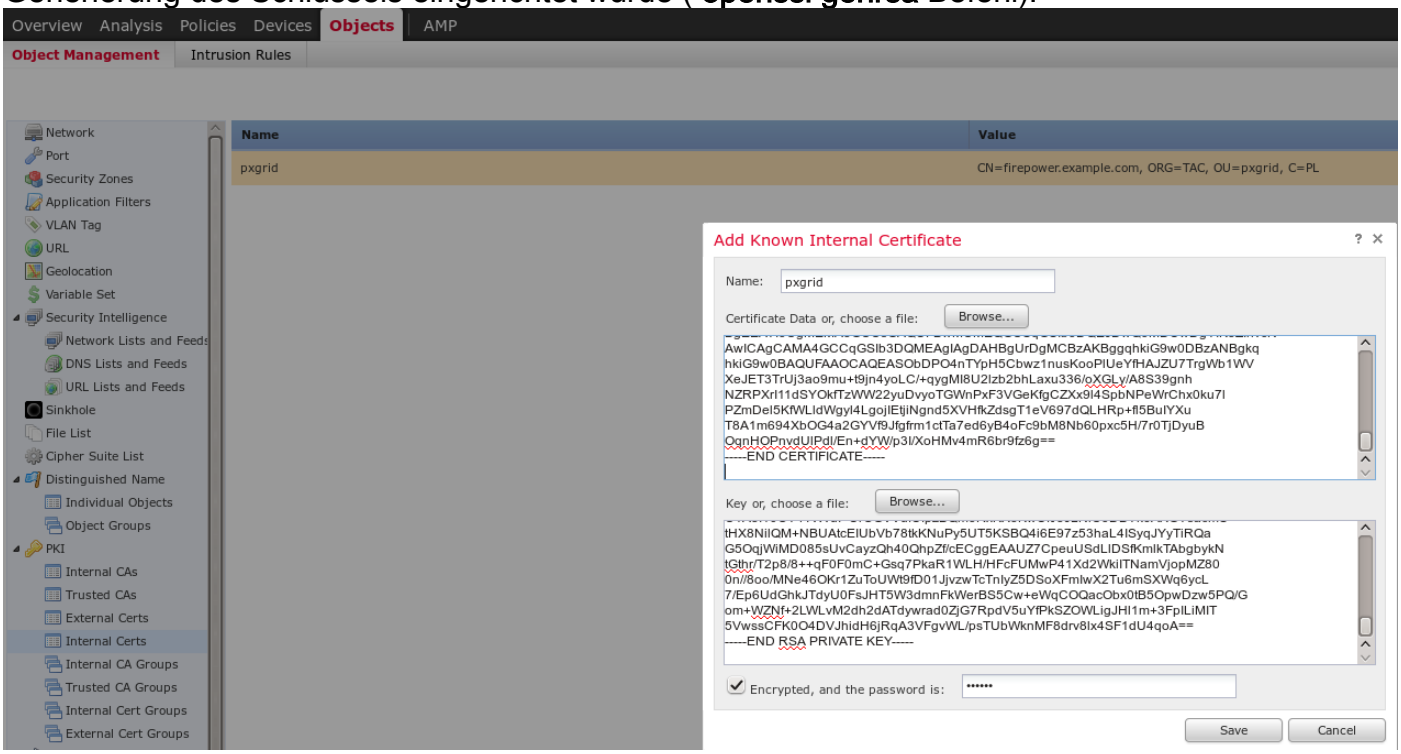
Zertifizierungsstellenzertifikat muss einem vertrauenswürdigen Speicher hinzugefügt werden:



Der letzte Schritt besteht in der Generierung des pxGrid-Zertifikats, das vom FMC zur Autorisierung für den ISE pxGrid-Service verwendet wird. Zur Generierung von CSR CLI muss verwendet werden (oder ein anderes externes System mit openssl-Tool).

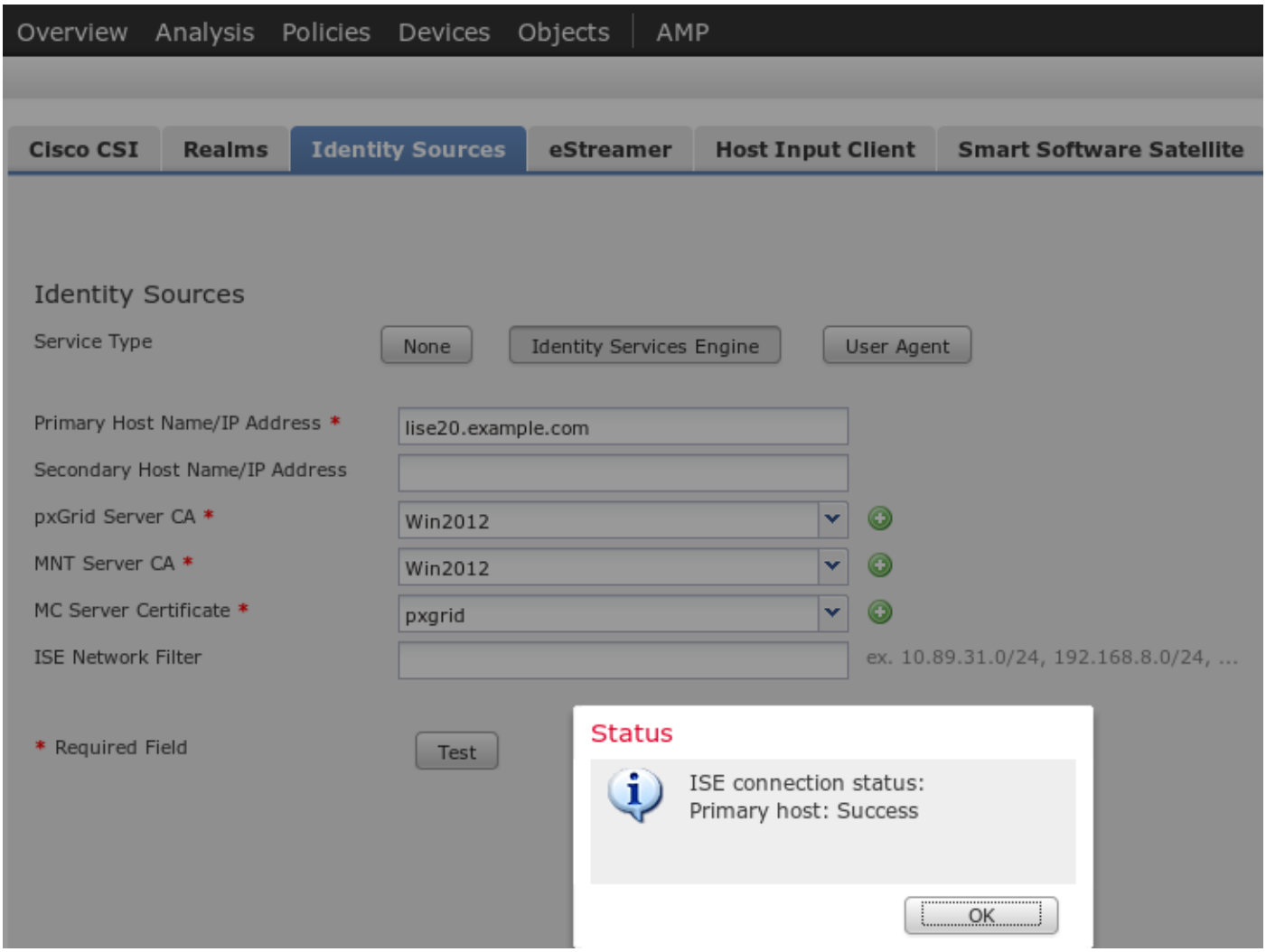
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#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

Nachdem fire.csr erstellt wurde, signieren Sie es mit Microsoft CA (pxGrid-Vorlage). Importieren Sie privaten Schlüssel (fire.key) und signiertes Zertifikat (fire.pem) in den internen Zertifikatsspeicher von FMC. Verwenden Sie für private Schlüssel das Kennwort, das während der Generierung des Schlüssels eingerichtet wurde (**openssl genrsa** Befehl):



ISE-Integration

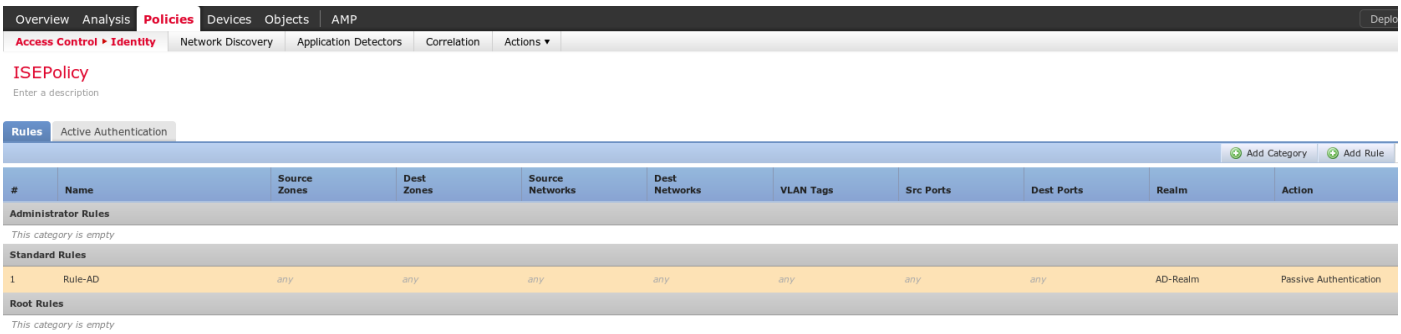
Nachdem alle Zertifikate installiert wurden, konfigurieren Sie die ISE-Integration von **System > Integration**:



Verwenden Sie die importierte CA für die Validierung von pxGrid- und MnT-Dienstzertifikaten. Für die Management Console (MC) wird das interne Zertifikat verwendet, das für pxGrid generiert wurde.

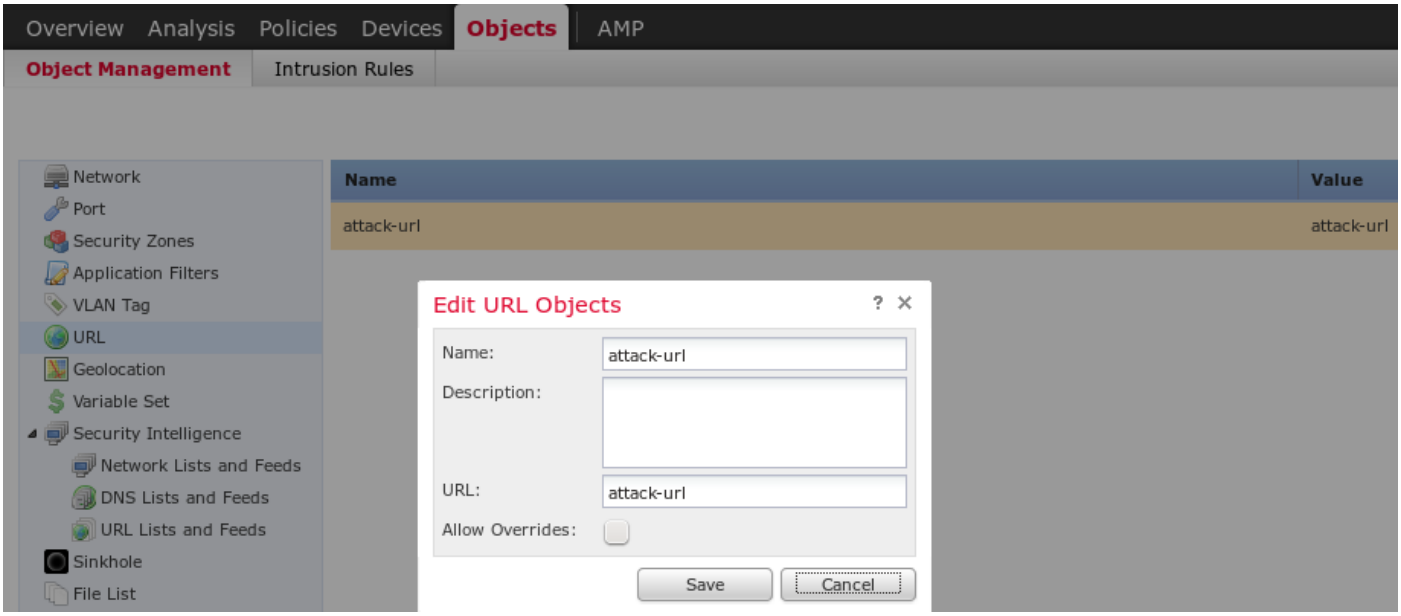
Identitätsrichtlinie

Konfigurieren Sie die Identitätsrichtlinie, die den zuvor konfigurierten AD-Bereich für die passive Authentifizierung verwendet:

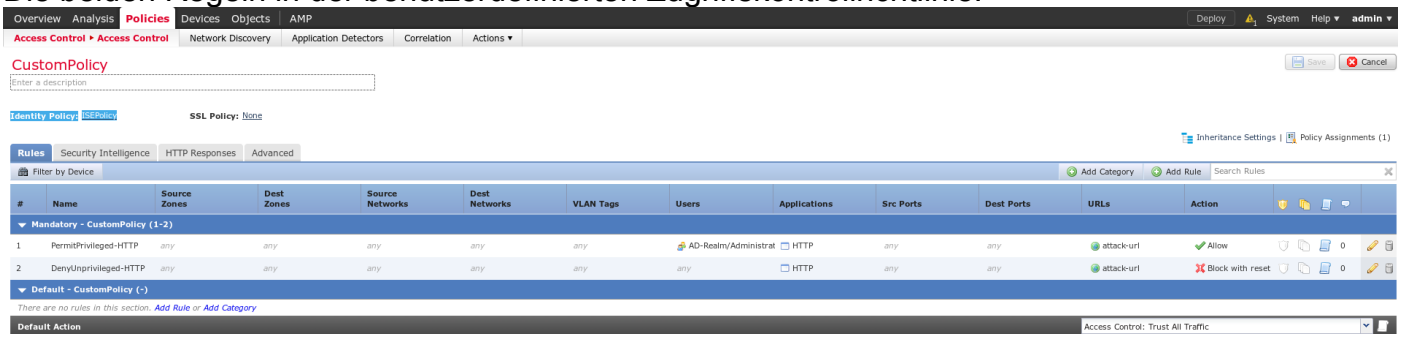


Zugriffskontrollrichtlinie

Für dieses Beispiel wurde die benutzerdefinierte URL erstellt:



Die beiden Regeln in der benutzerdefinierten Zugriffskontrollrichtlinie:

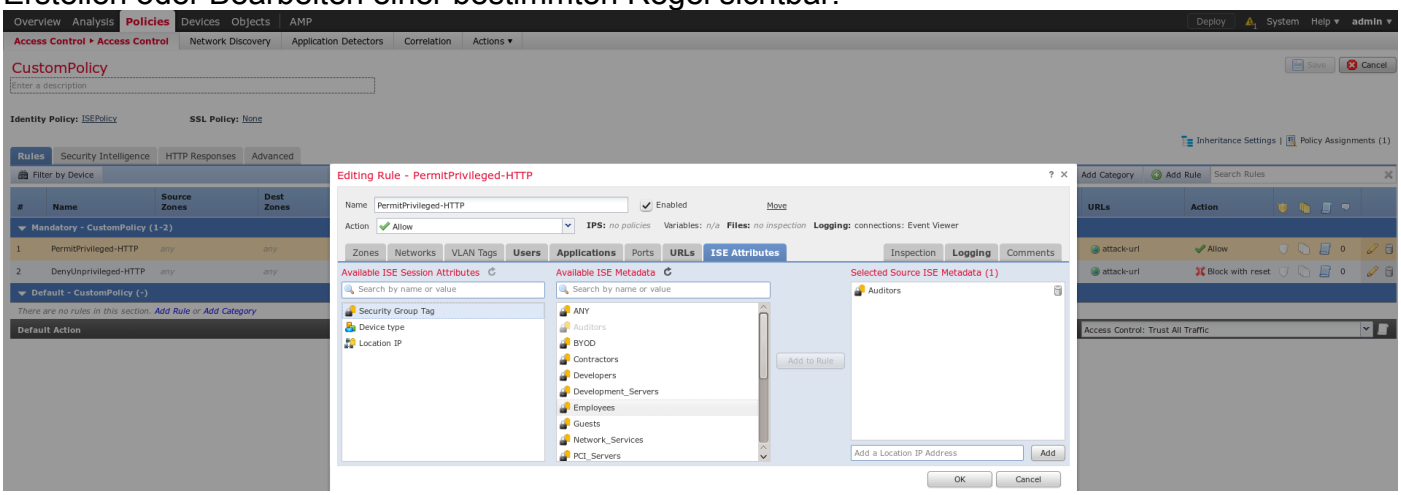


PermitPrivileged-HTTP-Regel ermöglicht allen Benutzern der Gruppe AD-Administratoren, denen das SGT-Tag zugewiesen wurde. Auditoren führen HTTP-Angriffe auf alle Ziele aus.

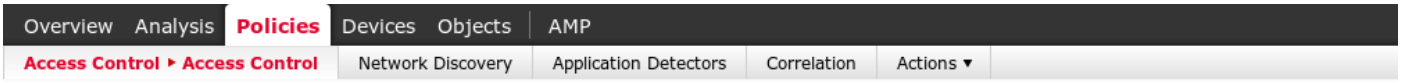
DenyUnprivileged-HTTP verweigert diese Aktion allen anderen Benutzern.

Beachten Sie außerdem, dass zuvor erstellte Identitätsrichtlinien dieser Zugriffskontrollrichtlinie zugewiesen wurden.

Auf dieser Registerkarte können keine SGT-Tags angezeigt werden, diese sind jedoch beim Erstellen oder Bearbeiten einer bestimmten Regel sichtbar:

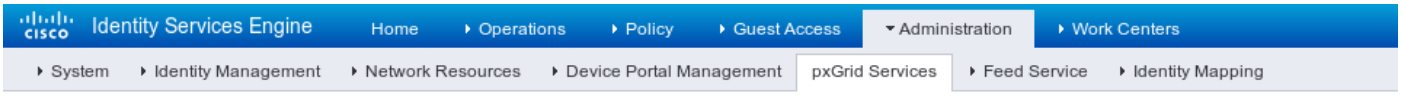


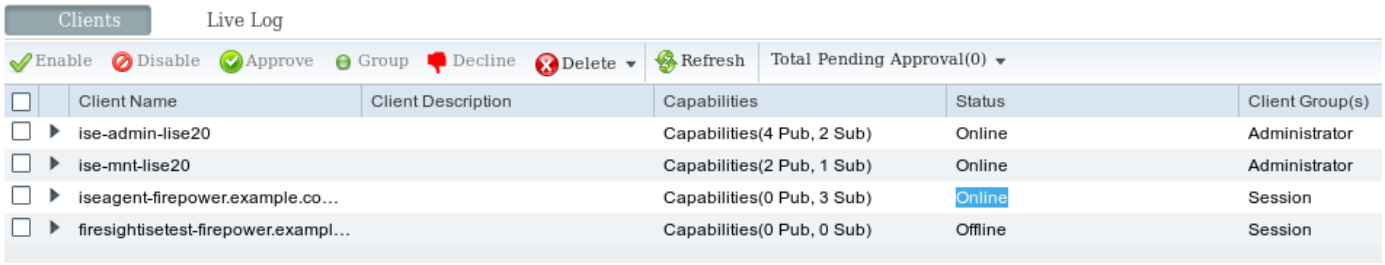
Stellen Sie sicher, dass die Richtlinie dem NGIPS zugewiesen und alle Änderungen bereitgestellt werden:



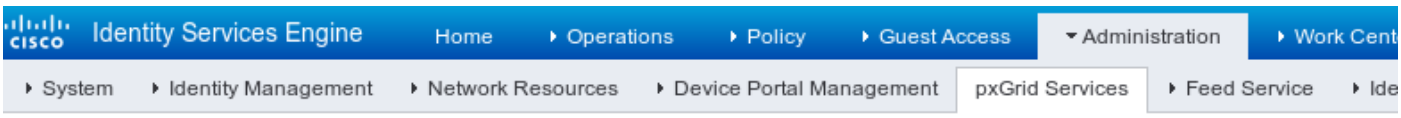
Überprüfen

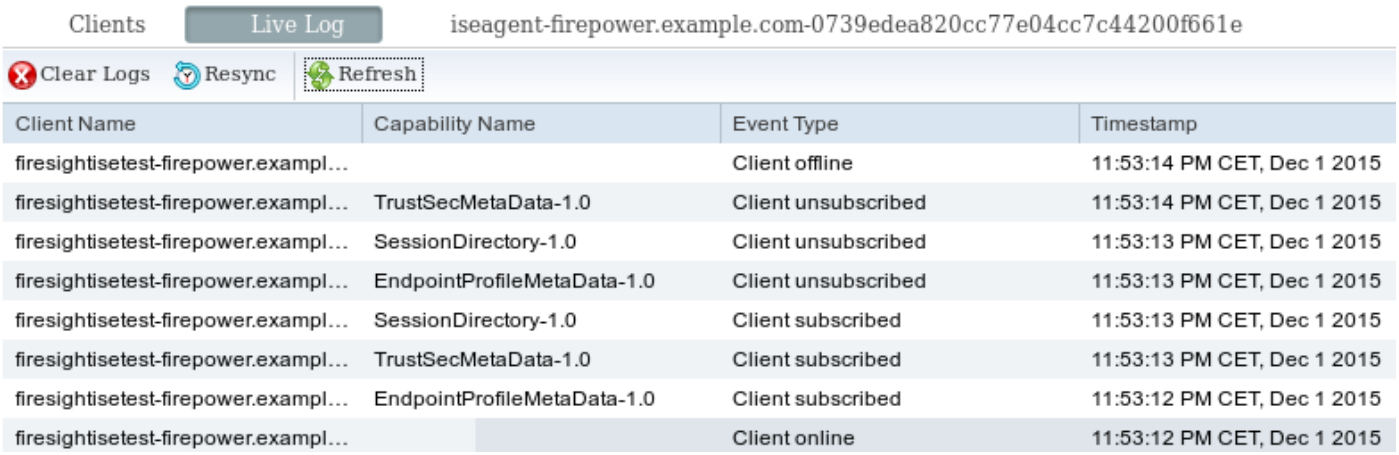
Nachdem alles korrekt konfiguriert wurde, sollte die ISE pxGrid-Client-Abonnement für einen Session-Service (Status Online) sehen.





Aus den Protokollen können Sie auch bestätigen, dass FMC den TrustSecMetaData-Dienst (SGT-Tags) abonniert hat - alle Tags erhalten und abbestellt hat.

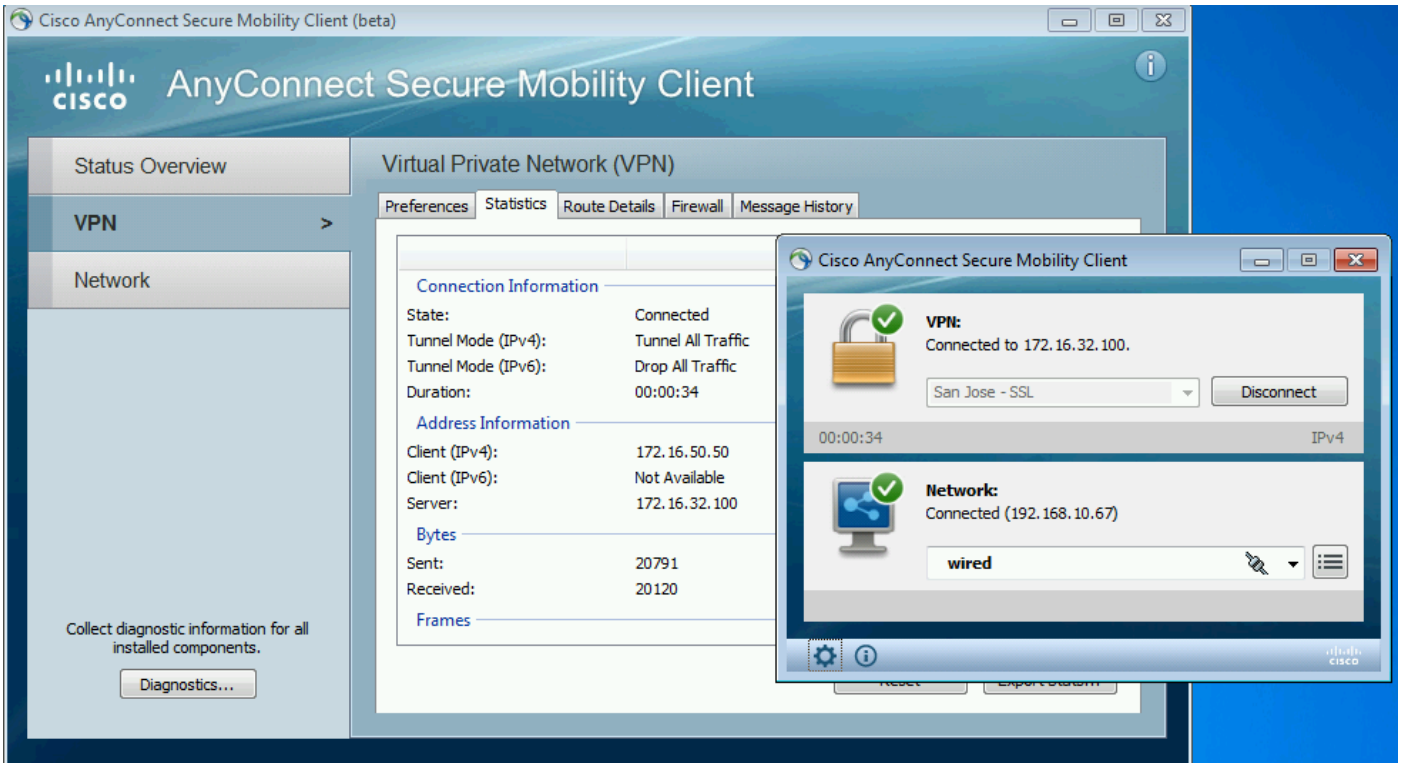




Einrichtung von VPN-Sitzungen

Der erste Test wird für ein Szenario durchgeführt, in dem die Autorisierung für die ISE nicht das richtige SGT-Tag zurückgibt (NGIPS lässt keine Audit-Tests zu).

Sobald die VPN-Sitzung die UP AnyConnect-Benutzeroberfläche (UI) ist, können weitere Details bereitgestellt werden:



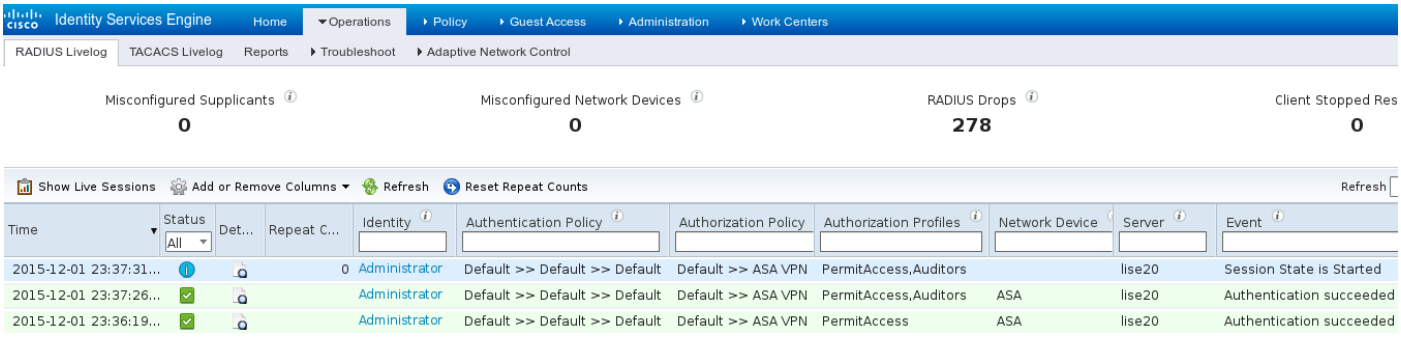
ASA kann bestätigen, dass die Sitzung eingerichtet wurde:

```
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
```

Beachten Sie, dass ASA kein SGT-Tag für diese Authentifizierung zurückgibt. ASA ist nicht für TrustSec konfiguriert, sodass Informationen sowieso übersprungen werden.

Die ISE meldet ebenfalls eine erfolgreiche Autorisierung (Protokoll um 23:36:19) - kein SGT-Tag wurde zurückgegeben:



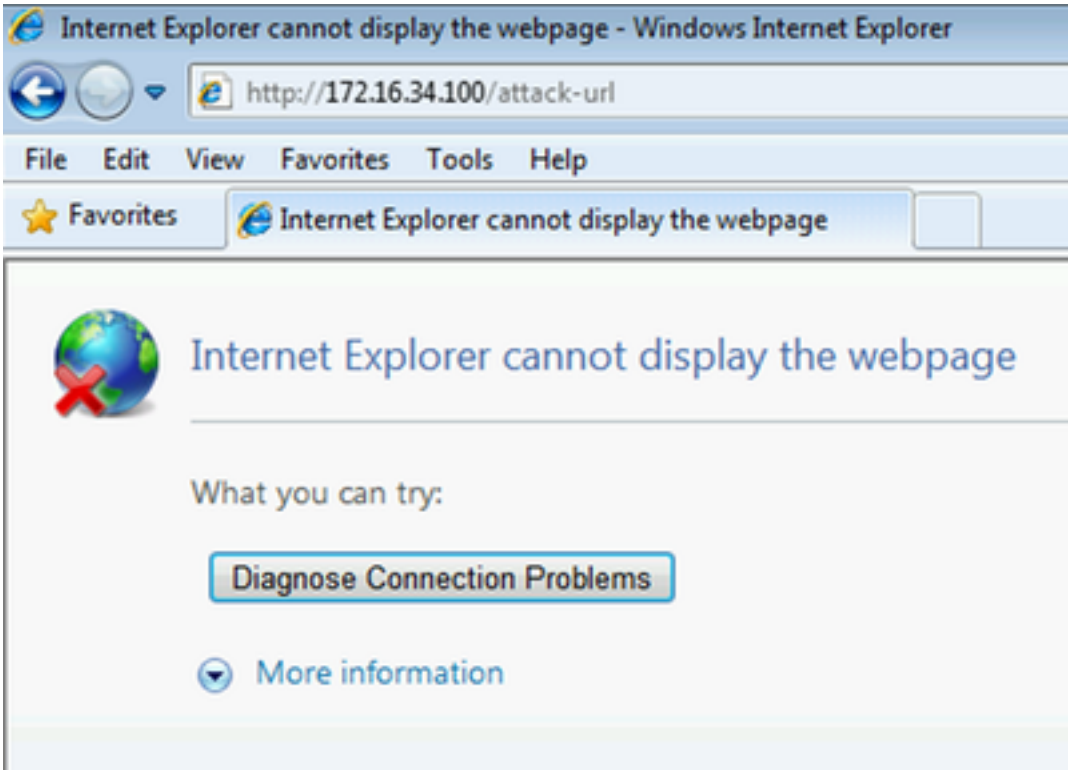
FMC empfängt Sitzungsdaten von MnT

In dieser Phase meldet das FMC in /var/log/messages eine neue Sitzung (die als Teilnehmer für den pxGrid-Dienst empfangen wurde) für den Administratorbenutzernamen und führt eine AD-Suche für die Gruppenmitgliedschaft durch:

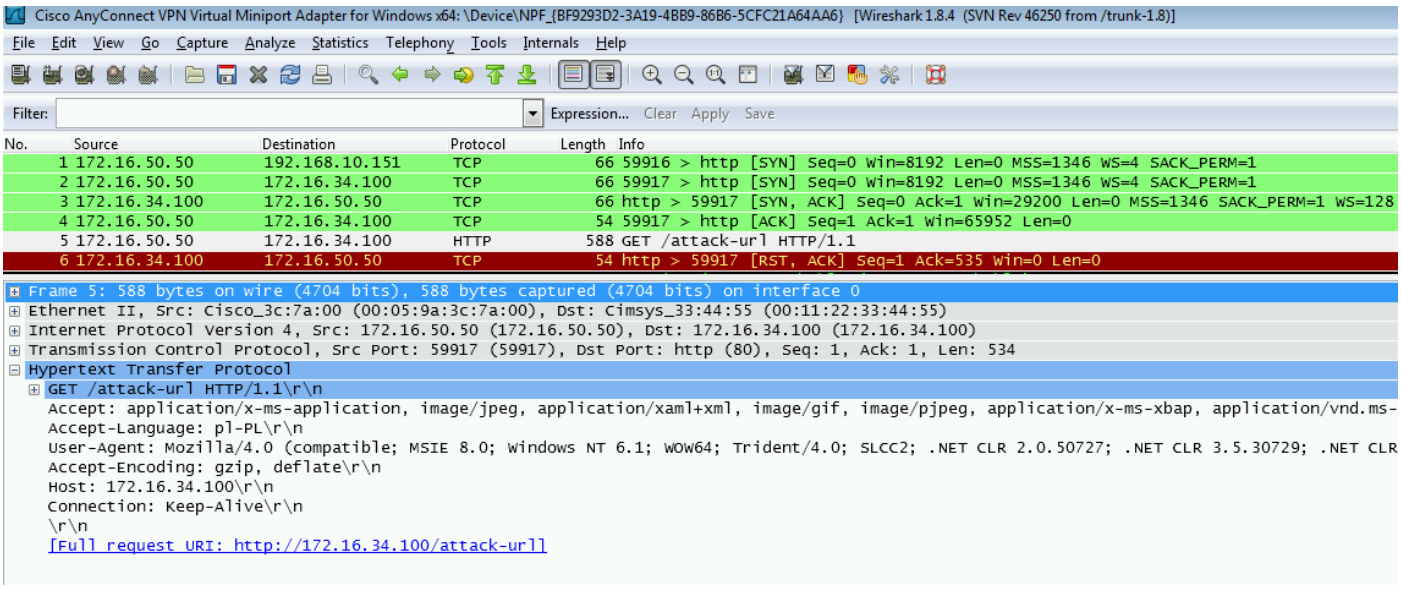
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

Unprivilegierter und privilegierter Netzwerkzugriff

Wenn der Benutzer zu diesem Zeitpunkt versucht, einen Webbrowser zu öffnen und auf einen überwachten Server zuzugreifen, wird die Verbindung beendet:



Dies kann durch die Paketerfassungen vom Client bestätigt werden (TCP RST-Senden gemäß FMC-Konfiguration):

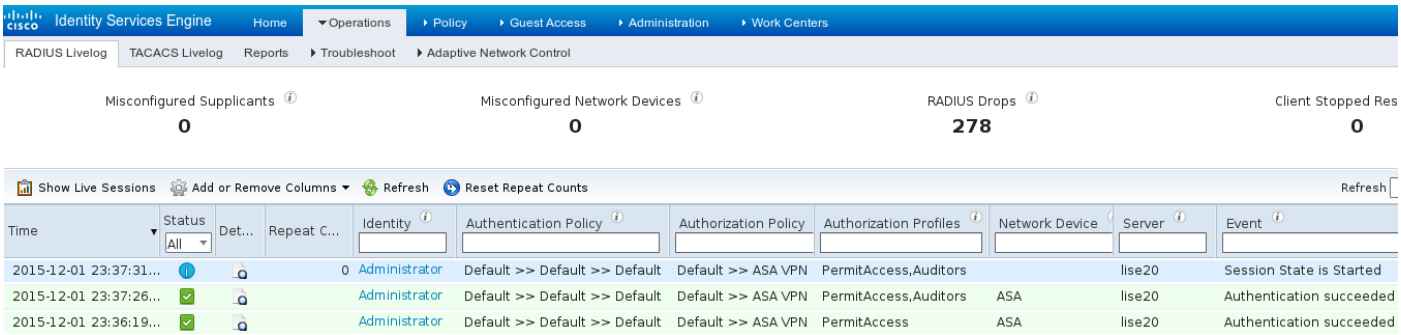


Sobald die ISE für die Rückgabe konfiguriert ist, werden folgende Berichte über die Audit-Tag-ASA-Sitzung angezeigt:

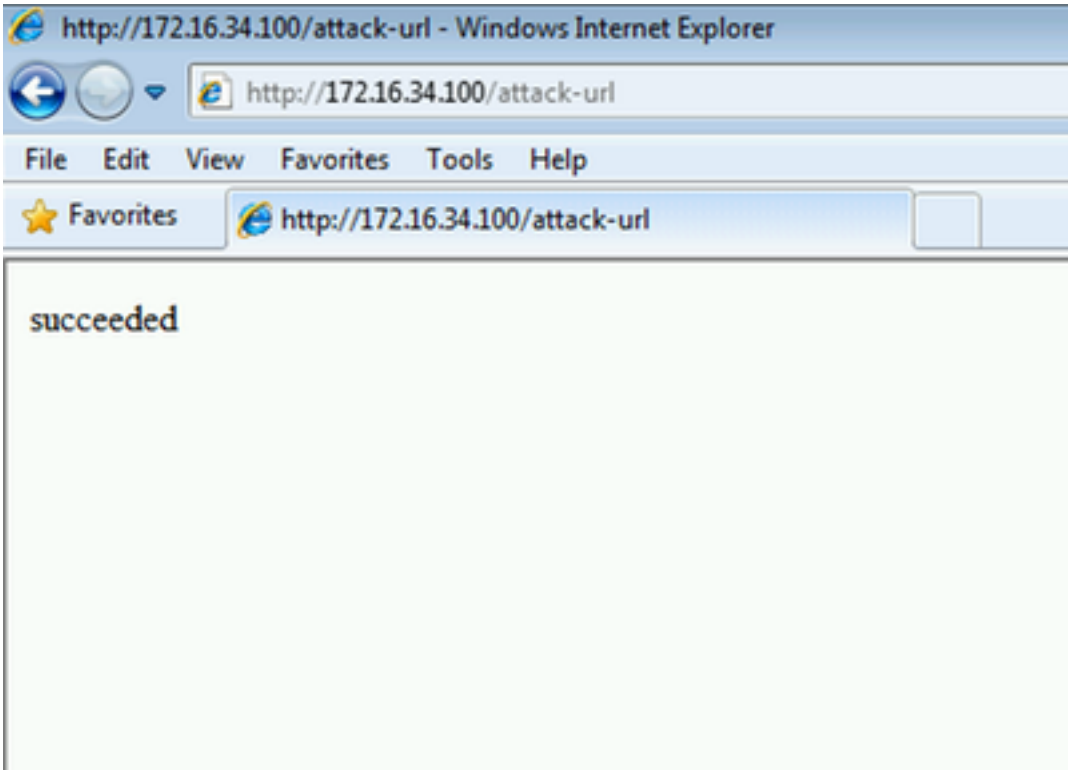
```
asav# show vpn-sessiondb anyconnect

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
```

Die ISE meldet auch eine erfolgreiche Autorisierung (das Protokoll wird um 23:37:26 Uhr gesendet) - der SGT-Tag-Auditor wird zurückgegeben:

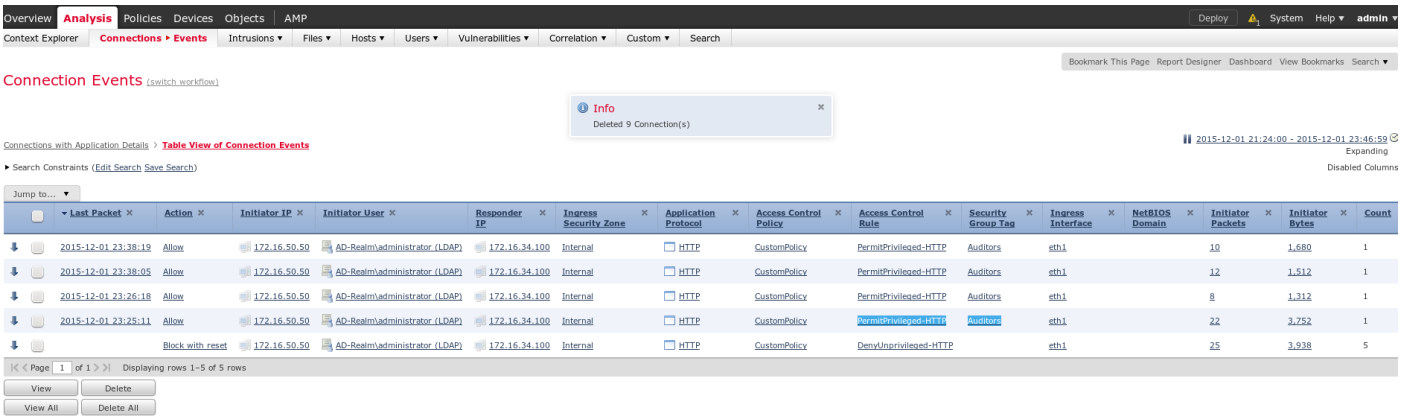


Der Benutzer kann auf den genannten Service zugreifen:



Zugriff auf FMC-Protokollierung

Diese Aktivität kann im Connection Event-Bericht bestätigt werden:



Zuerst hatte der Benutzer kein SGT-Tag zugewiesen und hatte die DenyUnprivileged-HTTP-Regel erreicht. Nachdem der Prüfer-Tag der ISE-Regel zugewiesen (und von der FMC-Regel abgerufen) wurde, wird PermitPrivileged-HTTP verwendet, und der Zugriff ist zulässig.

Beachten Sie außerdem, dass mehrere Spalten entfernt wurden, um die Anzeige zu erhalten, da normalerweise die Zugriffskontrollregel und die Sicherheitsgruppen-Tag-Nummer als eine der letzten Spalten angezeigt werden (und eine horizontale Bildlaufleiste verwendet werden muss). Diese benutzerdefinierte Ansicht kann gespeichert und später wiederverwendet werden.

Fehlerbehebung

FMC-Debugger

So überprüfen Sie die Protokolle der adi-Komponente, die für Identitätsdienste zuständig ist: /var/log/messages file:

```
[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
```

Um detailliertere Debuggen zu erhalten, ist es möglich, adi-Prozess (von root nach sudo) zu beenden und mit debug argument auszuführen:

```
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-Abfrage über pxGrid

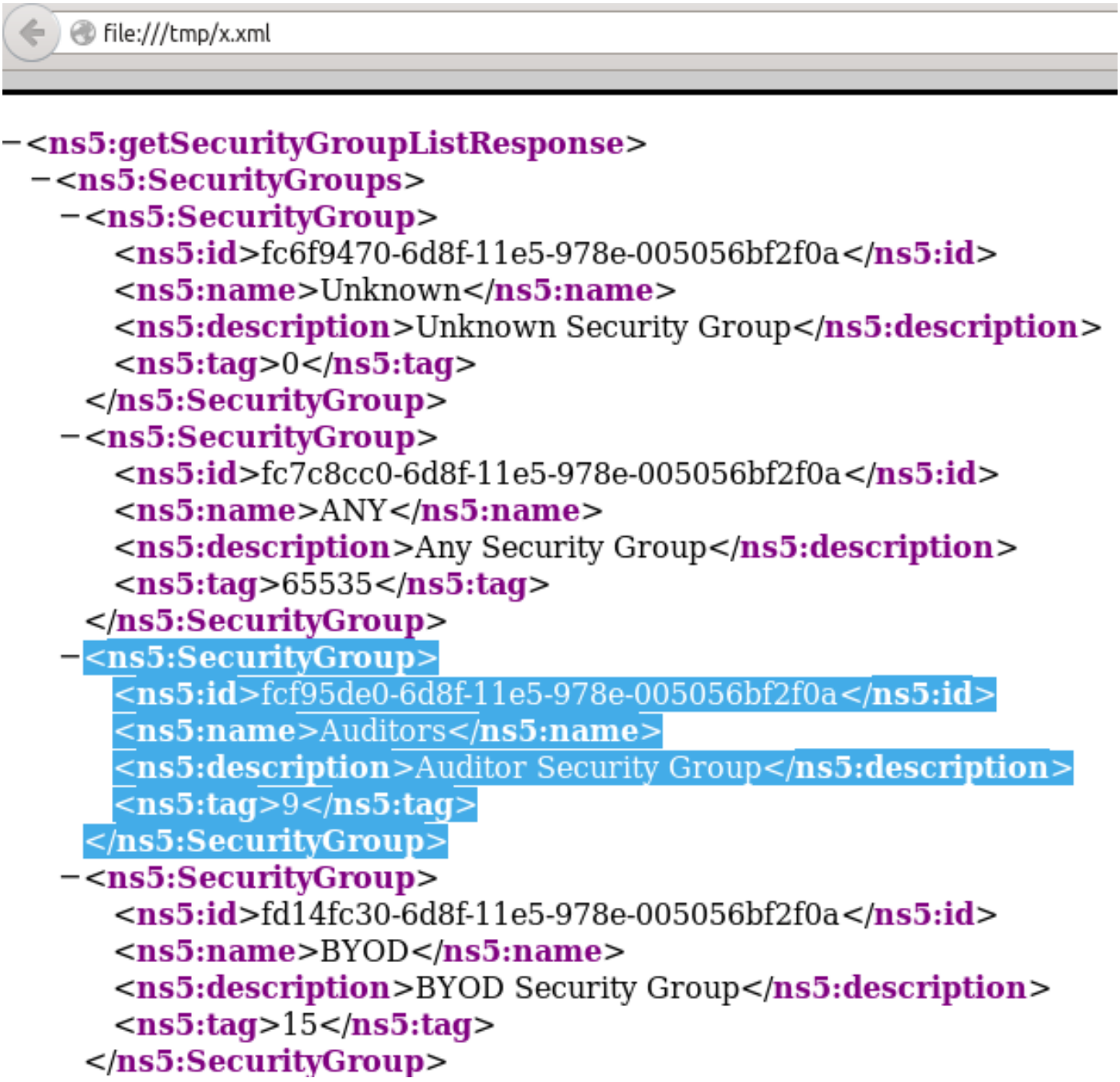
Der Vorgang wird ausgeführt, wenn auf die **Test-**Schaltfläche im Abschnitt **ISE-Integration** geklickt

wird oder wenn die SGT-Liste aktualisiert wird, während die Regel in der Zugriffskontrollrichtlinie hinzugefügt wird.

```
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>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>]

Für eine bessere Ansicht können XML-Inhalte aus diesem Protokoll in XML-Dateien kopiert und von einem Webbrowser geöffnet werden. Sie können bestätigen, dass sowohl ein bestimmtes SGT (Audit) als auch alle anderen auf der ISE definierten SGT empfangen werden:



Sitzungsabfrage über REST-API zu MnT

Dies ist auch Teil des Test-Vorgangs (beachten Sie, dass der MnT-Hostname und der Port über pxGrid übergeben werden). Massensitzungsdownload wird verwendet:

```
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>
```

Analysiertes Ergebnis (1 aktive Sitzung erhalten):

```
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 dieser Phase versucht NGIPS, diesen Benutzernamen (und die Domäne) mit dem Benutzernamen für das Realm-AD zu korrelieren:

```
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 wird verwendet, um einen Benutzer und eine Gruppenmitgliedschaft zu finden:

```
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-Debugging

Nach Aktivierung des TRACE-Level-Debug für die pxGrid-Komponente ist es möglich, jeden Vorgang zu überprüfen (aber ohne Payload/Daten wie auf FMC).

Beispiel für den Abruf von SGT-Tags:

```
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
```

Bug

CSCuv32295 - ISE kann Domäneninformationen in Benutzernamenfeldern senden

CSCus53796 - FQDN des Hosts kann für REST-Massenabfrage nicht abgerufen werden

CSCuv43145 - PXGRID & Identity Mapping Service Restart, Import/Löschen von Trust Store

Referenzen

- Konfigurieren von Problembehebungsservices mit ISE- und FirePower-Integration
- Konfigurieren von pxGrid in einer verteilten ISE-Umgebung
- So stellen Sie Zertifikate mit Cisco pxGrid bereit: Konfigurieren der CA-signierten ISE pxGrid Node und des CA-signierten pxGrid Clients
- ISE Version 1.3 pxGrid-Integration mit IPS pxLog-Anwendung
- Administratoranleitung für Cisco Identity Services Engine, Version 2.0
- Cisco Identity Services Engine API Referenzhandbuch, Version 1.2 - Einführung in External RESTful S...
- Cisco Identity Services Engine API-Referenzhandbuch, Version 1.2 - Einführung in das Monitoring RES ...
- Administratoranleitung für Cisco Identity Services Engine, Version 1.3
- Technischer Support und Dokumentation - Cisco Systems