Dépannez ISE et intégration de FirePOWER pour des gestions d'identité

Contenu

Introduction

Ce document décrit comment configurer et dépanner des stratégies averties de TrustSec sur le système de prévention des intrusions de nouvelle génération de Cisco (NGIPS). La version 6.0 NGIPS prend en charge l'intégration avec le Cisco Identity Services Engine (ISE) laissant établir des stratégies averties basées par identité.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration du VPN de l'appliance de sécurité adaptable Cisco (ASA)
- Configuration de Client à mobilité sécurisé Cisco AnyConnect
- Configuration de base de centre de Gestion de Cisco FirePOWER
- Configuration de Cisco ISE
- Solutions de Cisco TrustSec

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Autorité de certification (CA) de Microsoft Windows 2012
- Version 9.3 de Cisco ASA
- Versions de logiciel 1.4 de Cisco ISE
- Versions 4.2 de Client à mobilité sécurisé Cisco AnyConnect
- Version 6.0 du centre de Gestion de Cisco FirePOWER (FMC)
- Version 6.0 de Cisco FirePOWER NGIPS

Configurez

Le centre de Gestion de FirePOWER (FMC) est la plate-forme d'administration pour FirePOWER. Il y a deux types de fonctionnalités liées à l'intégration ISE :

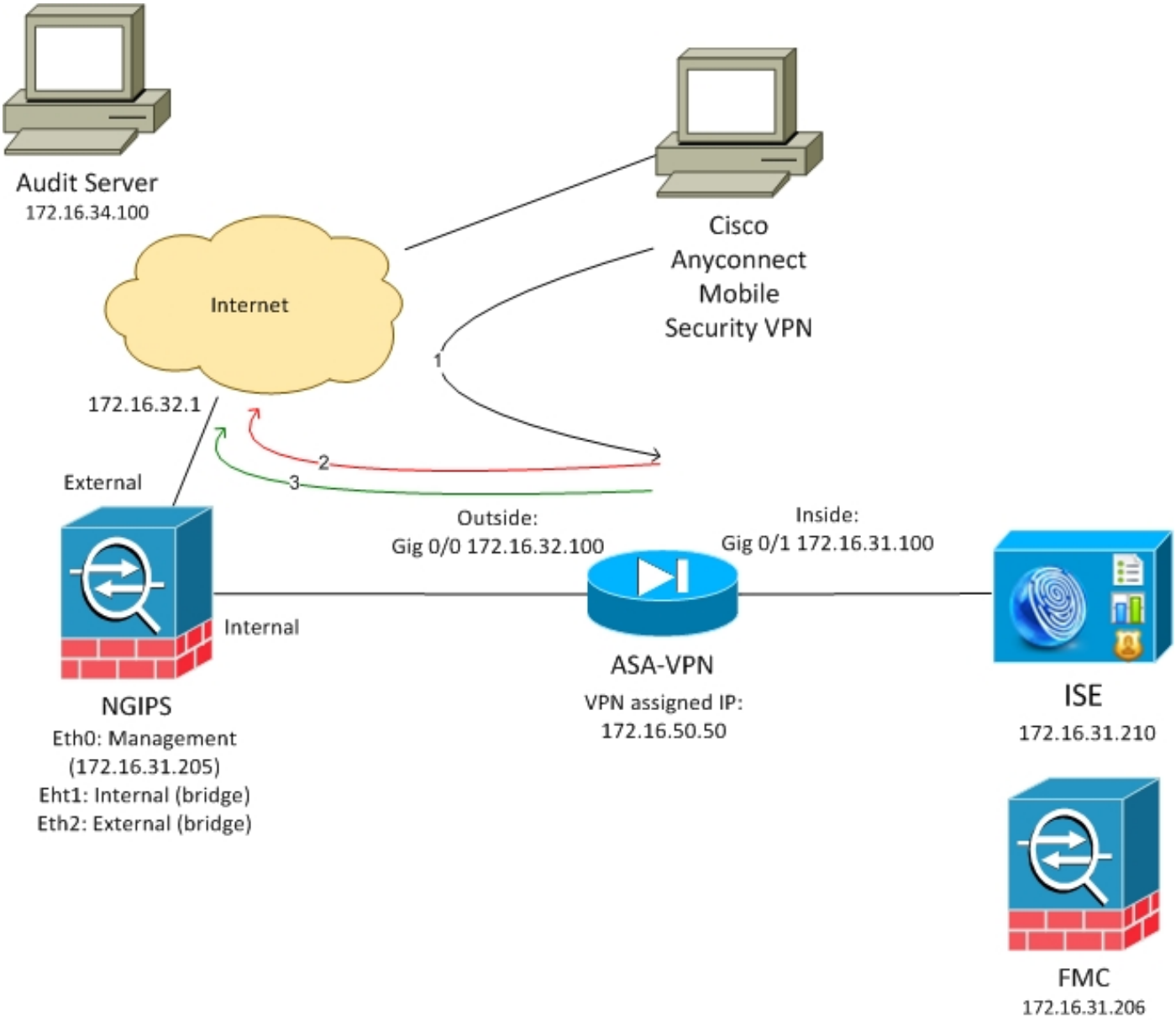
- Correction - permet à FMC pour mettre en quarantaine l'attaquant par l'intermédiaire d'ISE, qui est état d'autorisation changeant dynamiquement sur le périphérique d'accès fournissant l'accès au réseau limité. Il y a deux générations de cette solution :

1. Script existant Perl utilisant l'appel du service de protection de point final (ENV) API à ISE.
2. Un plus nouveau module utilisant l'appel de protocole de pxGrid à ISE (ce module est pris en charge seulement dans la version 5.4 - non prise en charge dans 6.0, prise en charge native prévue dans 6.1).

- Stratégie - permet à FMC pour configurer des stratégies basées sur les balises de groupe de sécurité de TrustSec (SGT).

Cet article se concentre sur la deuxième fonctionnalité. Pour la correction l'exemple a s'il vous plaît lu la section de références

Diagramme du réseau



FMC est configuré avec la stratégie de contrôle d'accès contenant deux règles :

- Refusez pour le trafic http avec URL de coutume (l'attaque-URL)
- Tenez compte du trafic http avec URL de coutume (attaque-URL) mais seulement si l'utilisateur est assigné pour apurer (9) la balise SGT par ISE

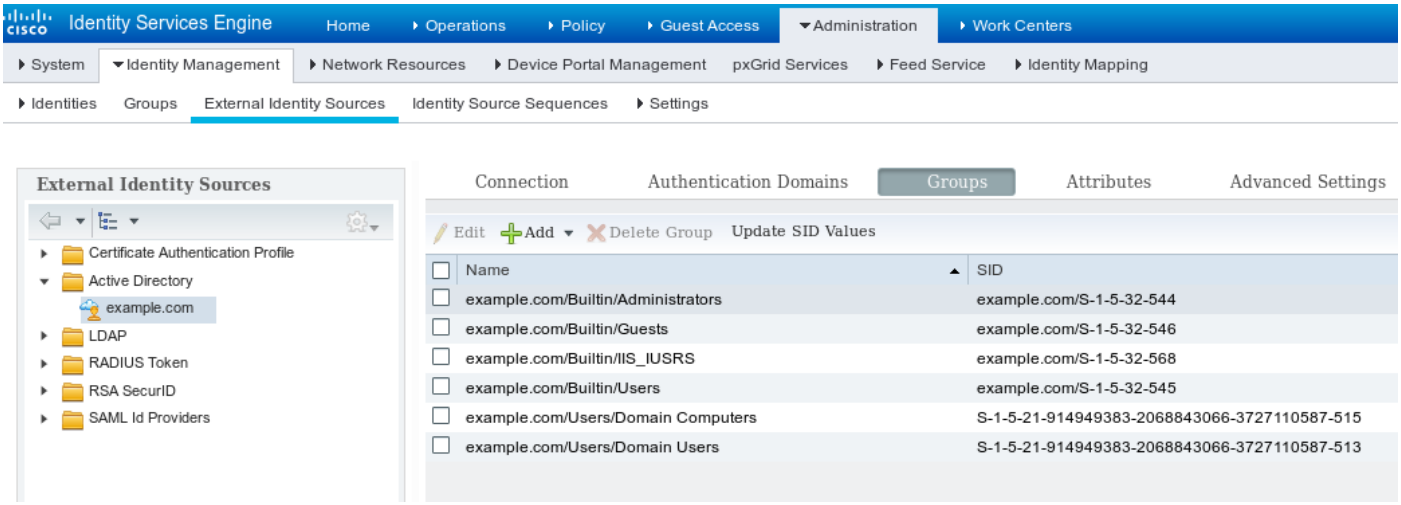
ISE décide d'assigner la balise d'audit à tous les utilisateurs de Répertoire actif qui appartient au groupe d'administrateur et utilise le périphérique ASA-VPN pour l'accès au réseau.

Réseau d'accès client par l'intermédiaire de la connexion VPN sur l'ASA. Les essais d'utilisateur puis à accéder à ont audité le serveur utilisant l'attaque-URL URL - mais échoue parce qu'il n'a pas été assigné pour apurer le groupe SGT. Une fois que cela est réparé, la connexion est réussie.

ISE

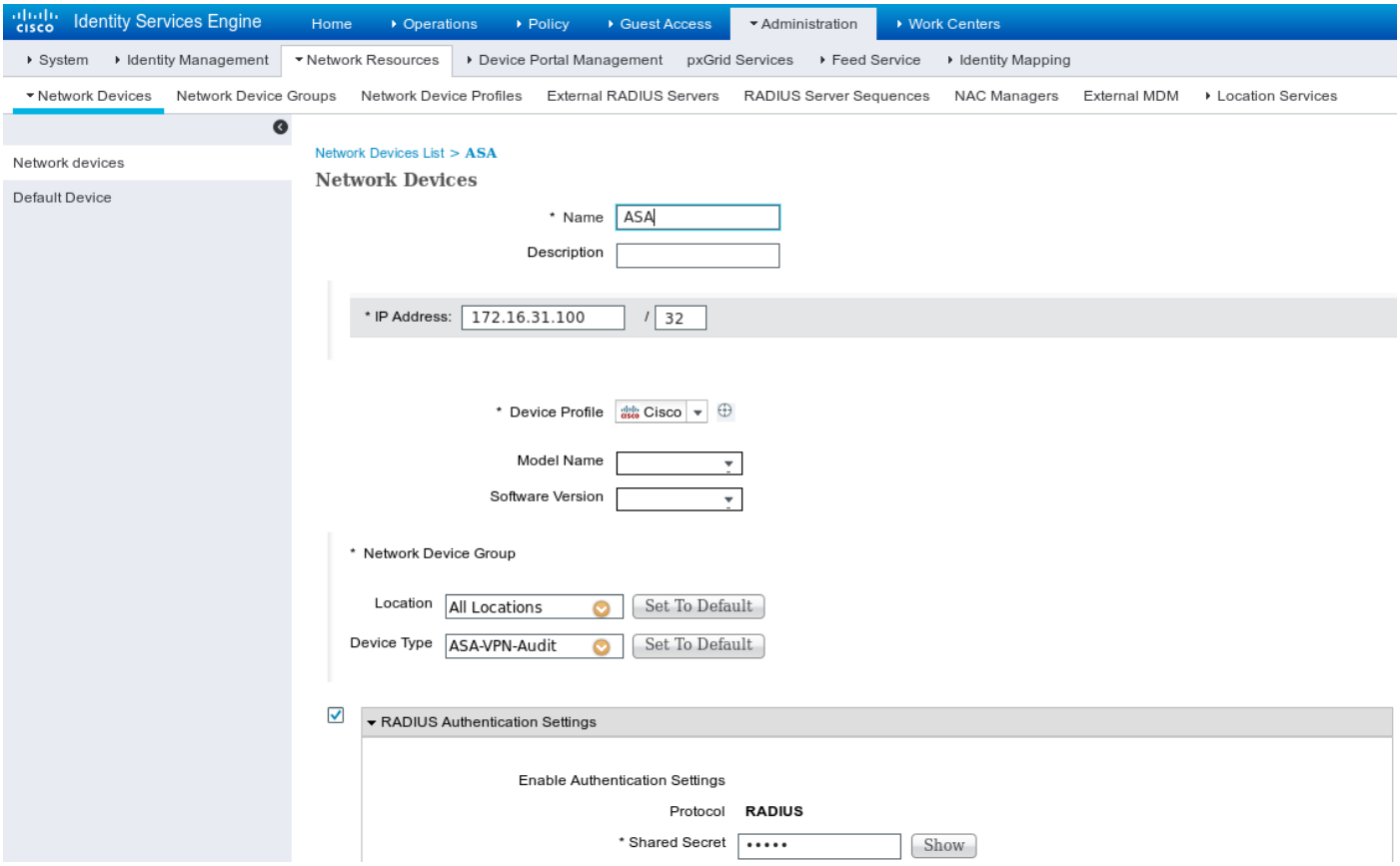
Active Directory

L'intégration d'AD doit être configurée et les groupes corrects doivent être cherchés (le groupe d'administrateurs est utilisé pour l'état de règle d'autorisation) :



Périphérique d'accès au réseau

L'ASA est ajoutée comme périphérique de réseau. L'ASA-VPN-audit fait sur commande de groupe est utilisé, suivant les indications de cette image :



Certificats pour le pxGrid et le MNT

FMC utilise les deux services sur ISE :

- pxGrid pour SGT et profiler la requête de données
- Surveillance et enregistrement (MNT) pour le téléchargement en vrac de session

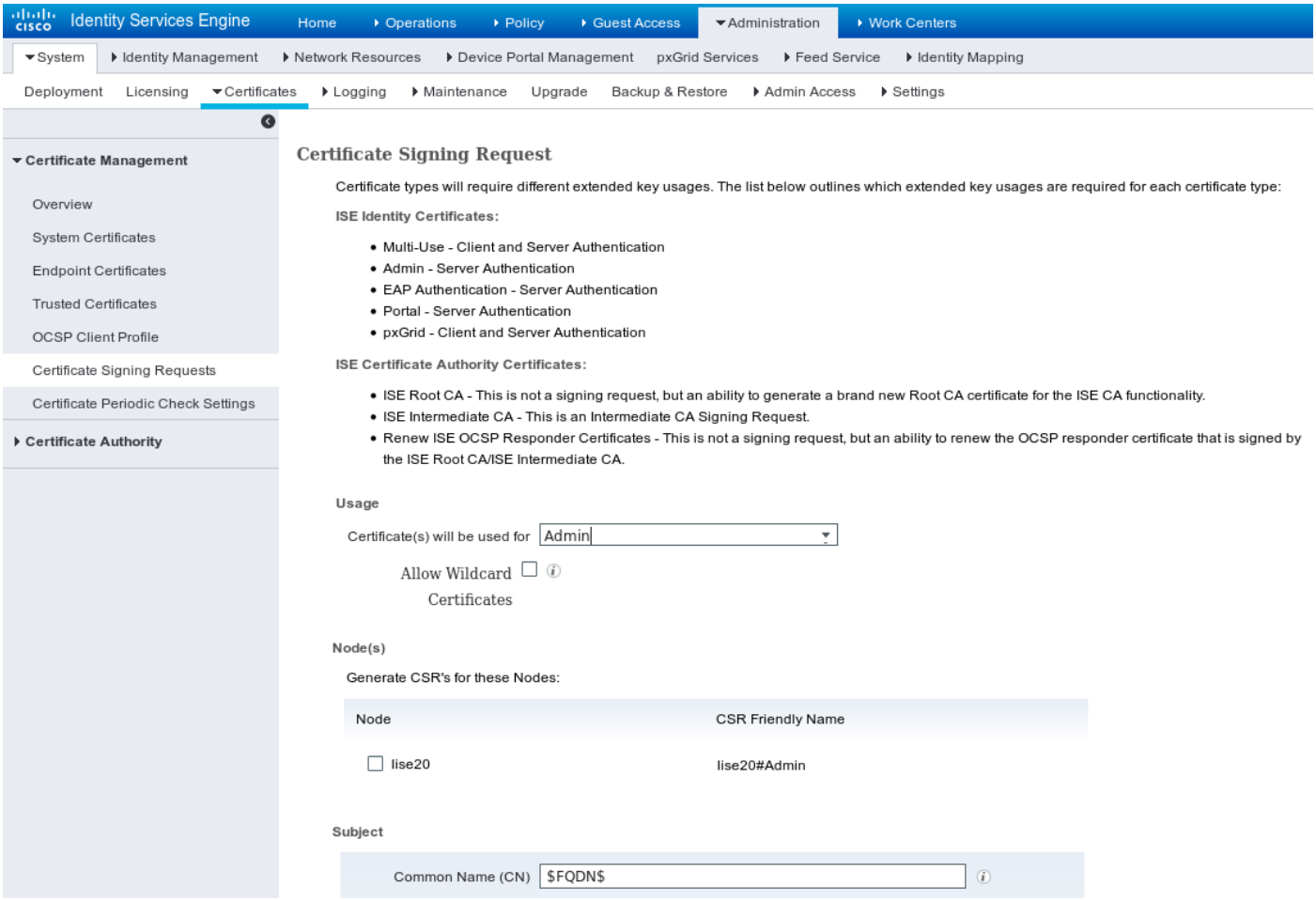
La Disponibilité MNT est très importante puisque de cette façon FMC est au courant ce qui est l'adresse IP de la session authentifiée, aussi son nom d'utilisateur et balise SGT. Basé sur cela, les stratégies correctes peuvent être appliquées. Notez s'il vous plaît que NGIPS ne prend en

charge pas à la façon des indigènes des balises SGT (en ligne étiquetant) comme l'ASA. Mais dans le contraire à l'ASA, il prend en charge des noms SGT au lieu des nombres seulement.

En raison de ces conditions requises ISE et FMC doit se faire confiance service (certificat). Le MNT utilise juste le certificat de côté serveur, pxGrid utilise les deux le certificat de côté de client et serveur.

Microsoft CA est utilisé pour signer tous les Certificats.

Pour MNT (rôle d'admin) ISE doit générer la demande de signature de certificat (CSR), suivant les indications de cette image :



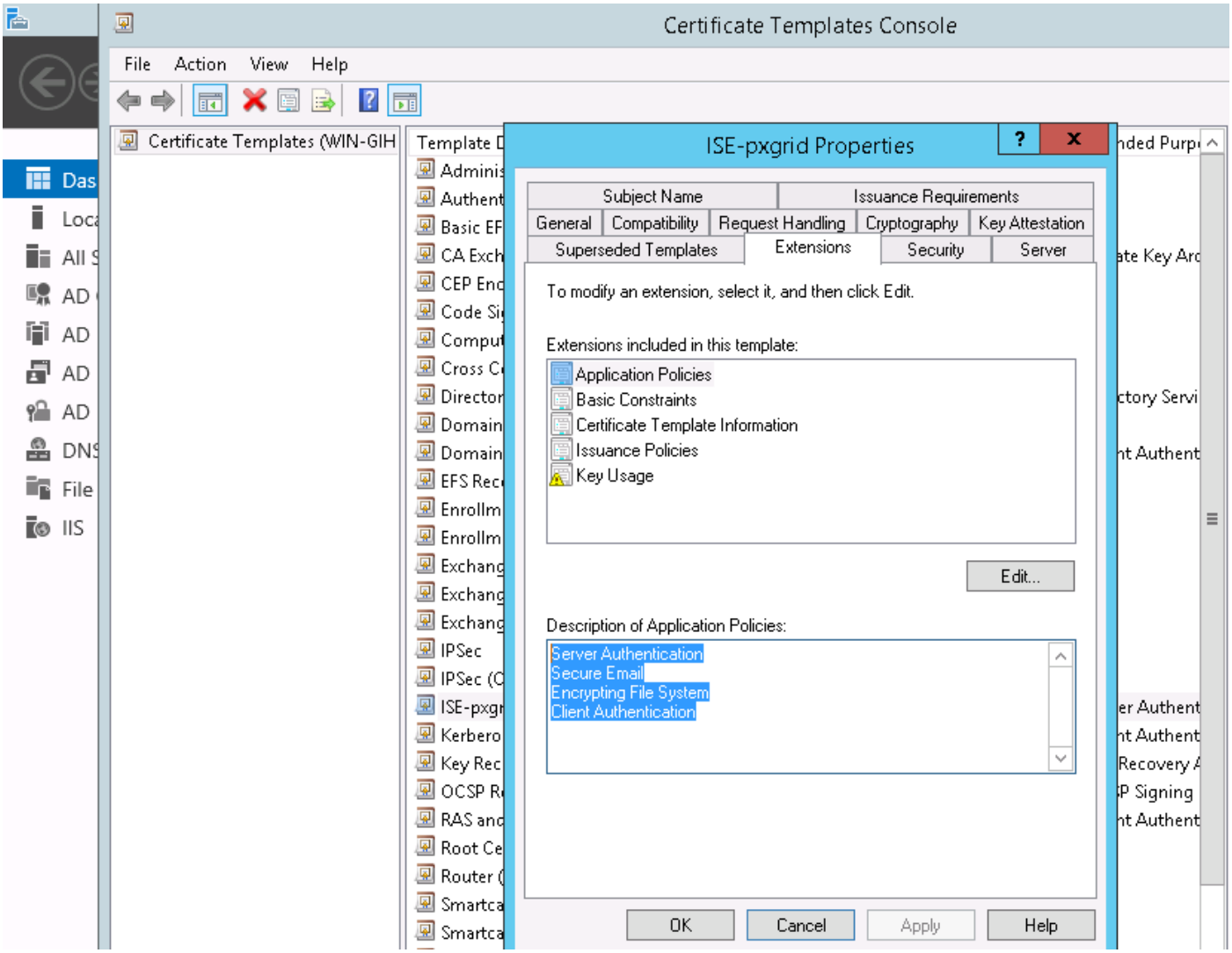
Après avoir été signé par Microsoft CA il doit être importé par l'intermédiaire de l'option de **certificat de grippage**.

Le processus semblable doit être suivi pour le service de pxGrid. **Des certificats seront utilisés pour l'**option doivent faire sélectionner le pxGrid.

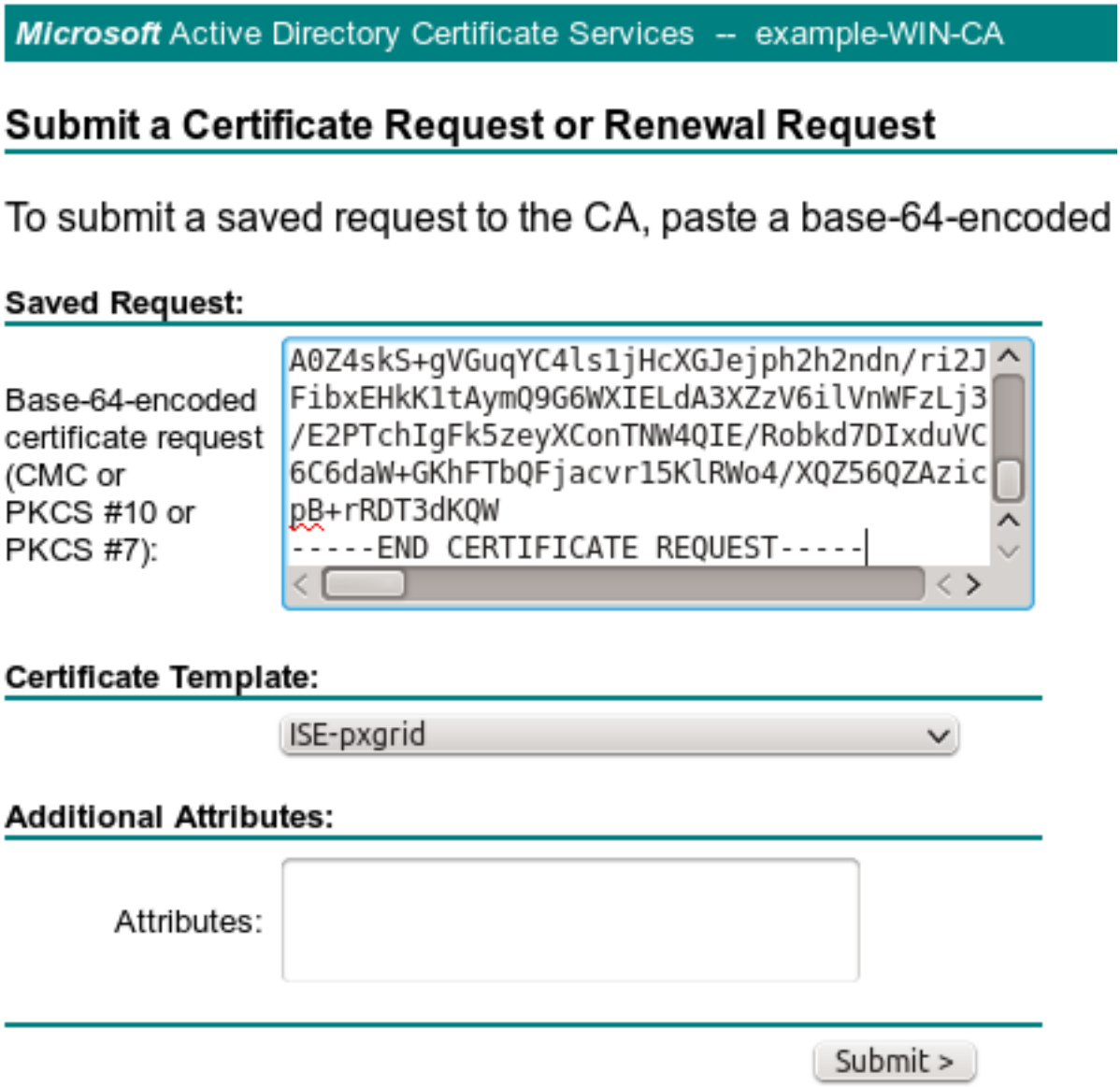
Puisqu'il ne peut pas y avoir deux Certificats avec le nom du sujet identique il est entièrement acceptable d'ajouter la valeur différente pour la section OU ou O (par exemple pxGrid).

> **Note**: Veuillez s'assurer que pour chaque nom de domaine complet (FQDN) pour ISE et FMC, l'enregistrement DNS correct est configuré sur le serveur DNS.

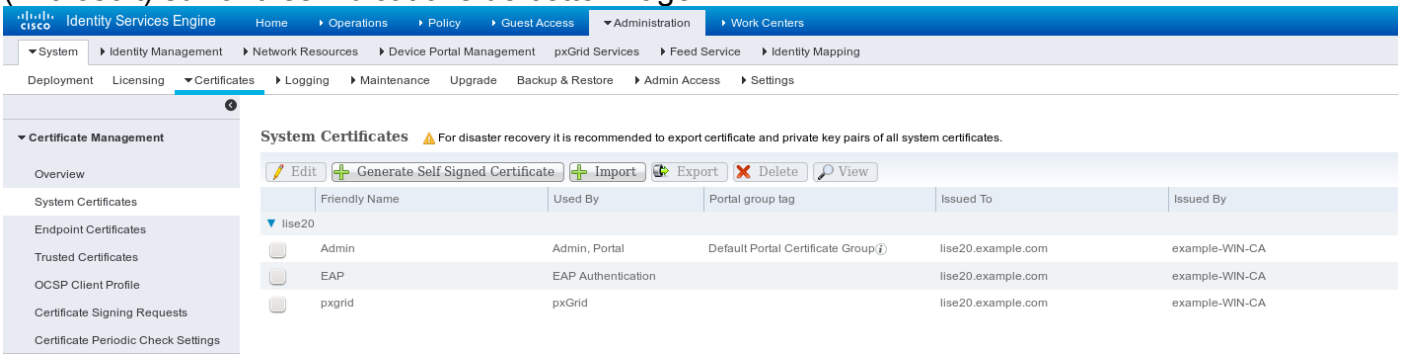
La seule différence entre l'admin et le certificat de pxGrid est avec le processus de signature. Puisque les Certificats de pxGrid doivent avoir étendu des options d'utilisation principale pour des les deux modèle personnalisé d'authentification de client et serveur sur Microsoft CA peuvent être utilisées pour cela :



Comment utiliser le service Web de Microsoft pour signer le CSR de pxGrid est affiché dans cette image :

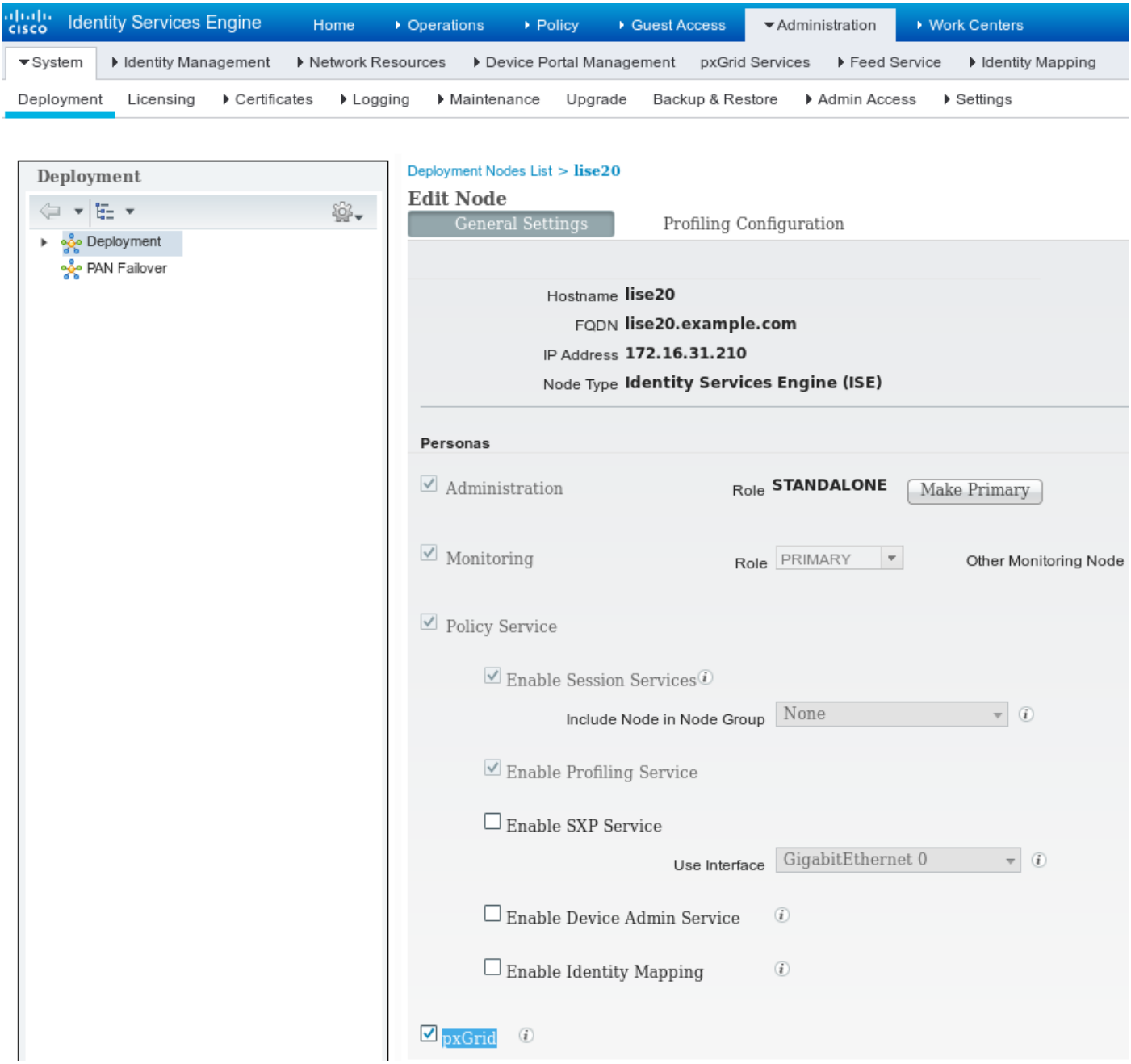


À l'extrémité ISE doit avoir des Certificats d'admin et de pxGrid signés par le CA de confiance (Microsoft) suivant les indications de cette image :

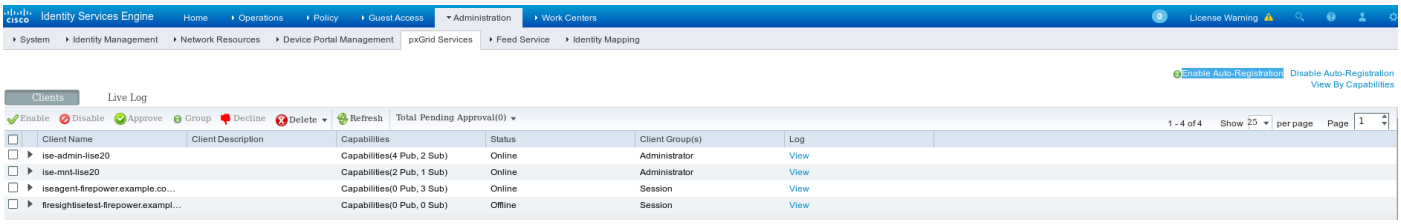


service de pxGrid

Avec les Certificats corrects le rôle de pxGrid pour le noeud spécifique doit être activé, suivant les indications de cette image :



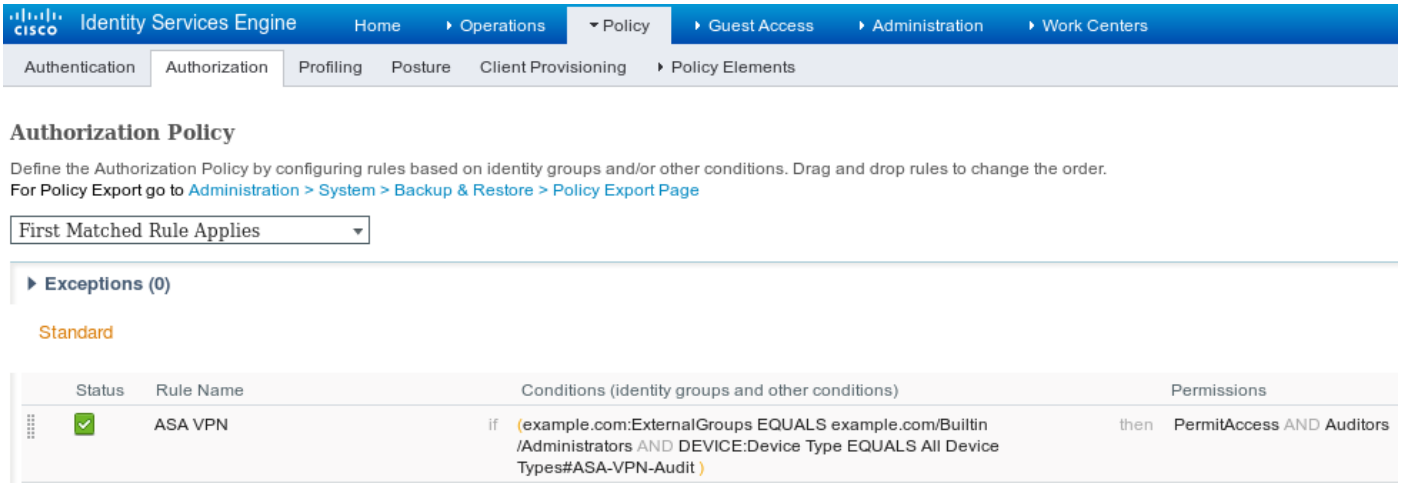
Et l'approbation automatique doit être placée à activer :



Stratégie d'autorisation

La stratégie d'authentification par défaut est utilisée (la consultation d'AD est exécutée si l'utilisateur local n'est pas trouvé).

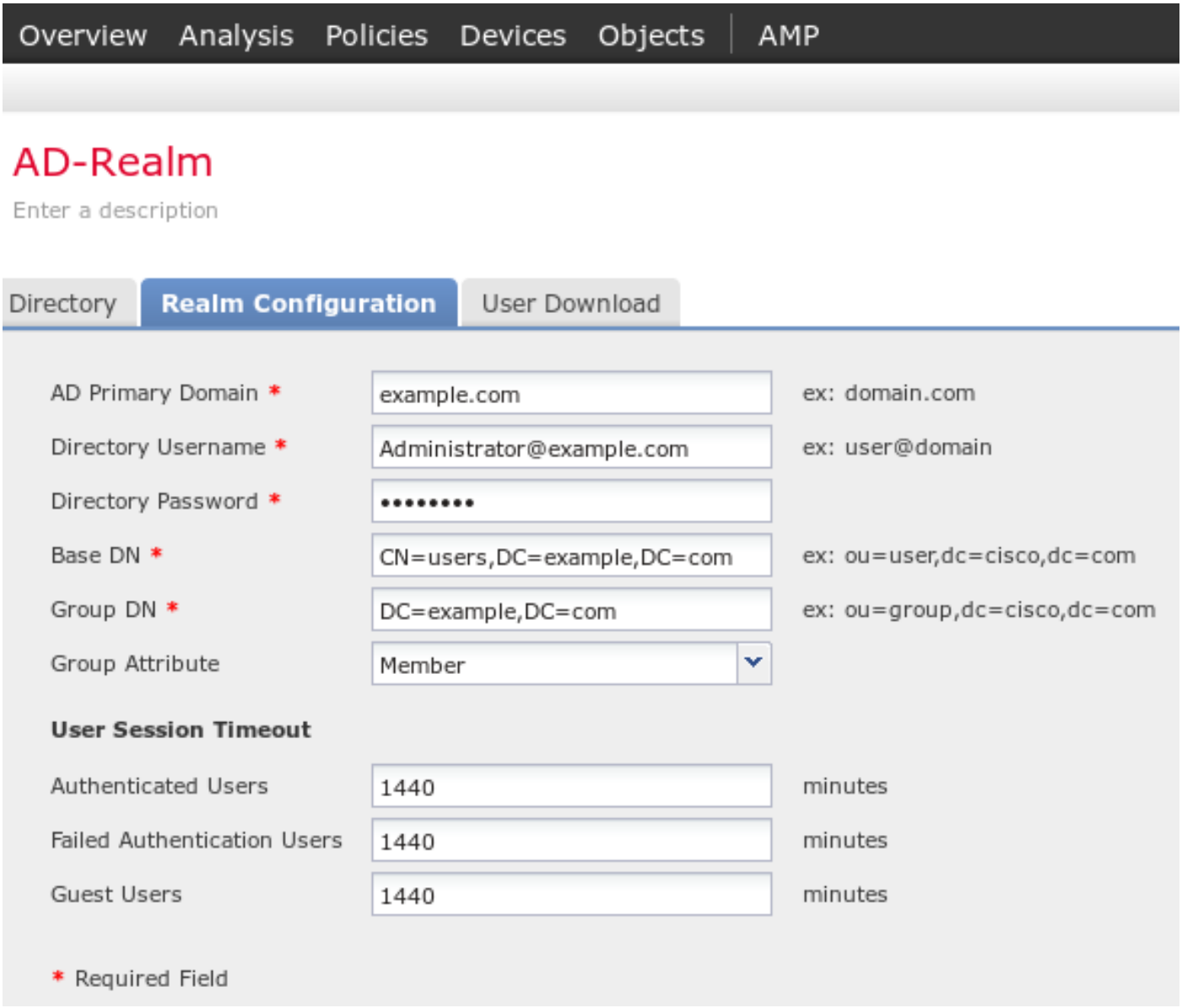
La stratégie d'autorisation a été configurée pour fournir le plein accès au réseau (autorisation : PermitAccess) pour des utilisateurs authentifiant par l'intermédiaire d'ASA-VPN et appartenant aux administrateurs de groupe de Répertoire actif - pour ces auditeurs de balise des utilisateurs SGT est retourné :



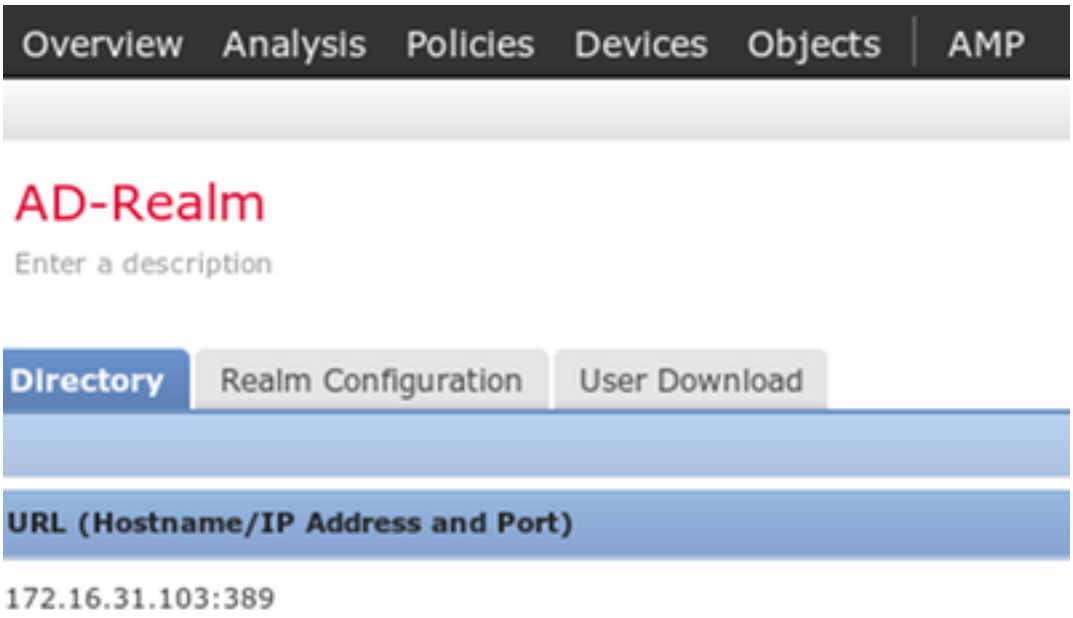
FMC

Royaume de Répertoire actif

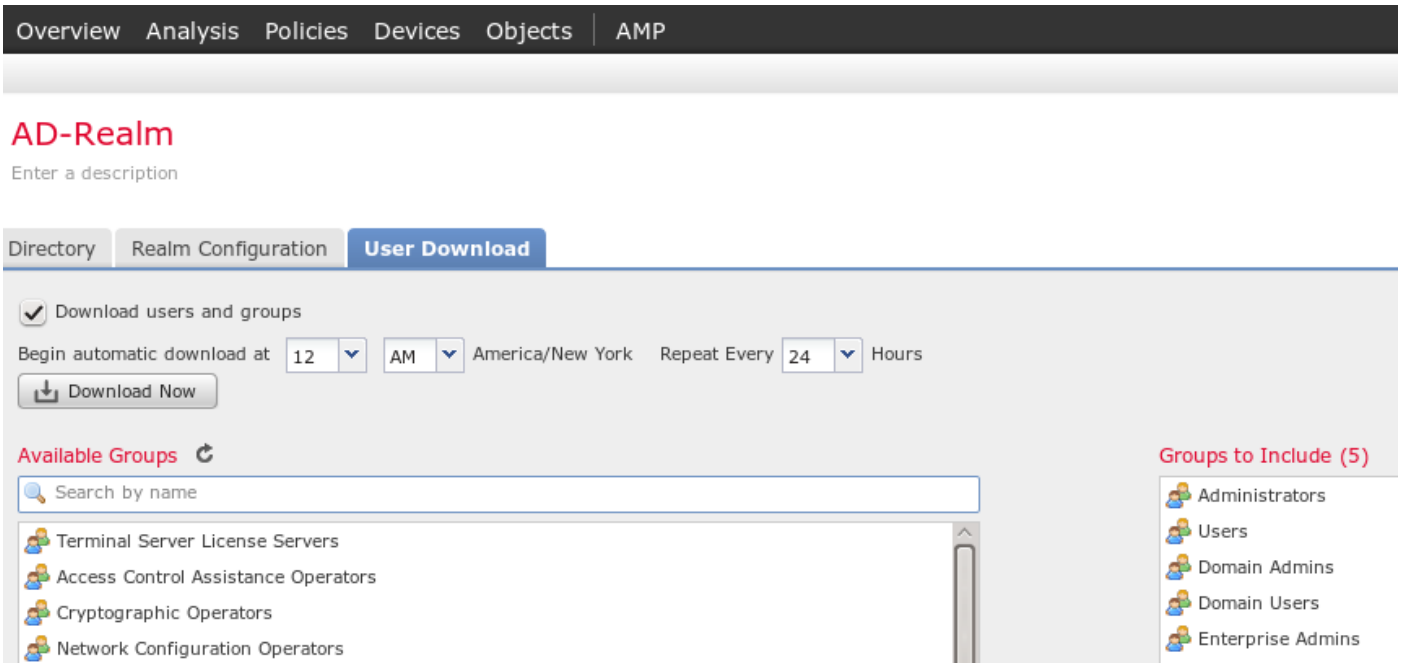
La configuration de royaume est exigée afin de fonctionner avec l'intégration ISE (pour utiliser des stratégies d'identité et récupérer l'adhésion à des associations pour les utilisateurs passivement authentifiés). Le royaume peut être configuré pour le Répertoire actif ou le Protocole LDAP (Lightweight Directory Access Protocol). Dans cet exemple l'AD est utilisé. **Du système > de l'intégration > du royaume** :



Des configurations standard de répertoire sont utilisées :

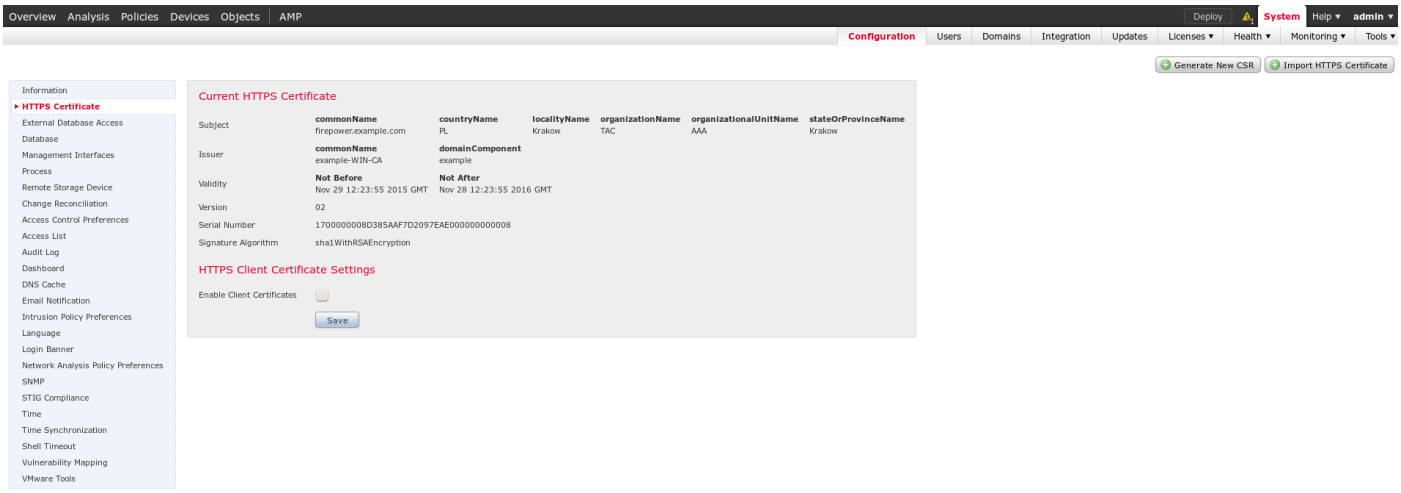


Et certains des groupes d'AD sont récupérés (être utilisé comme l'état supplémentaire dans le contrôle d'accès ordonne) :

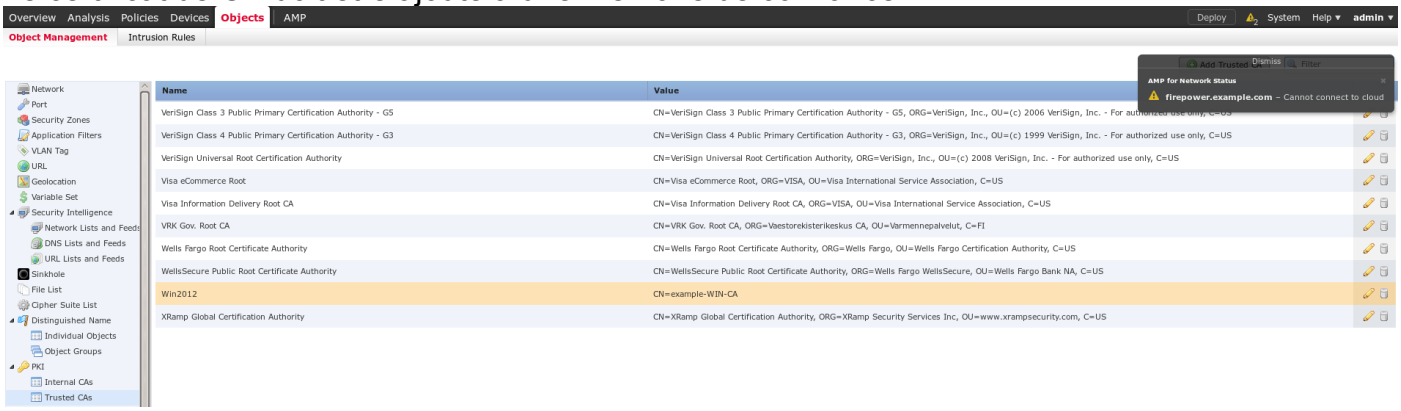


Certificats pour l'admin et le pxGrid

Bien que non requis, son une bonne pratique de générer le CSR pour l'accès d'admin. Signez ce CSR utilisant l'AD de confiance, importation de retour le certificat signé, suivant les indications de cette image :



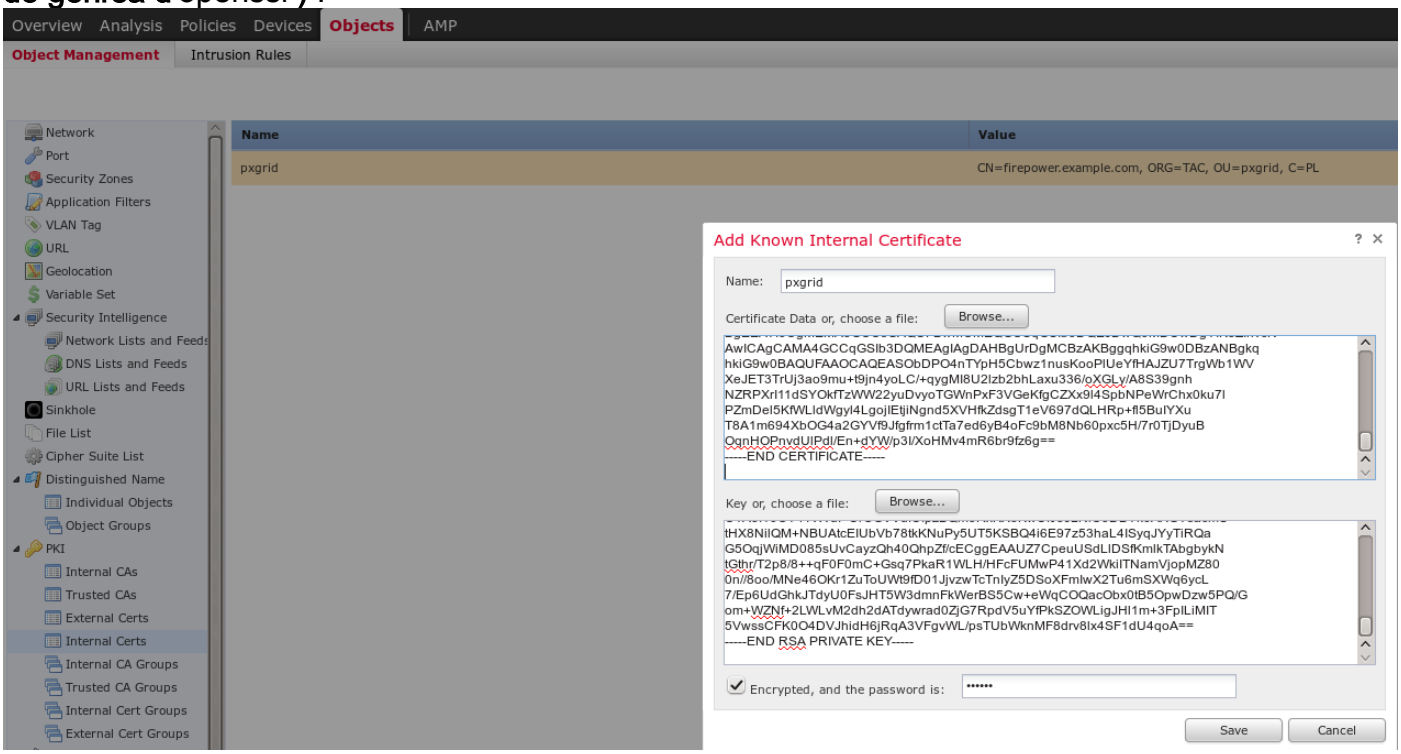
Le certificat de CA doit être ajouté à une mémoire de confiance :



La dernière étape est de générer le certificat de pxGrid utilisé par FMC pour autoriser au service de pxGrid ISE. Pour générer CSR CLI doit être utilisé (ou tout autre ordinateur externe avec l'outil d'openssl).

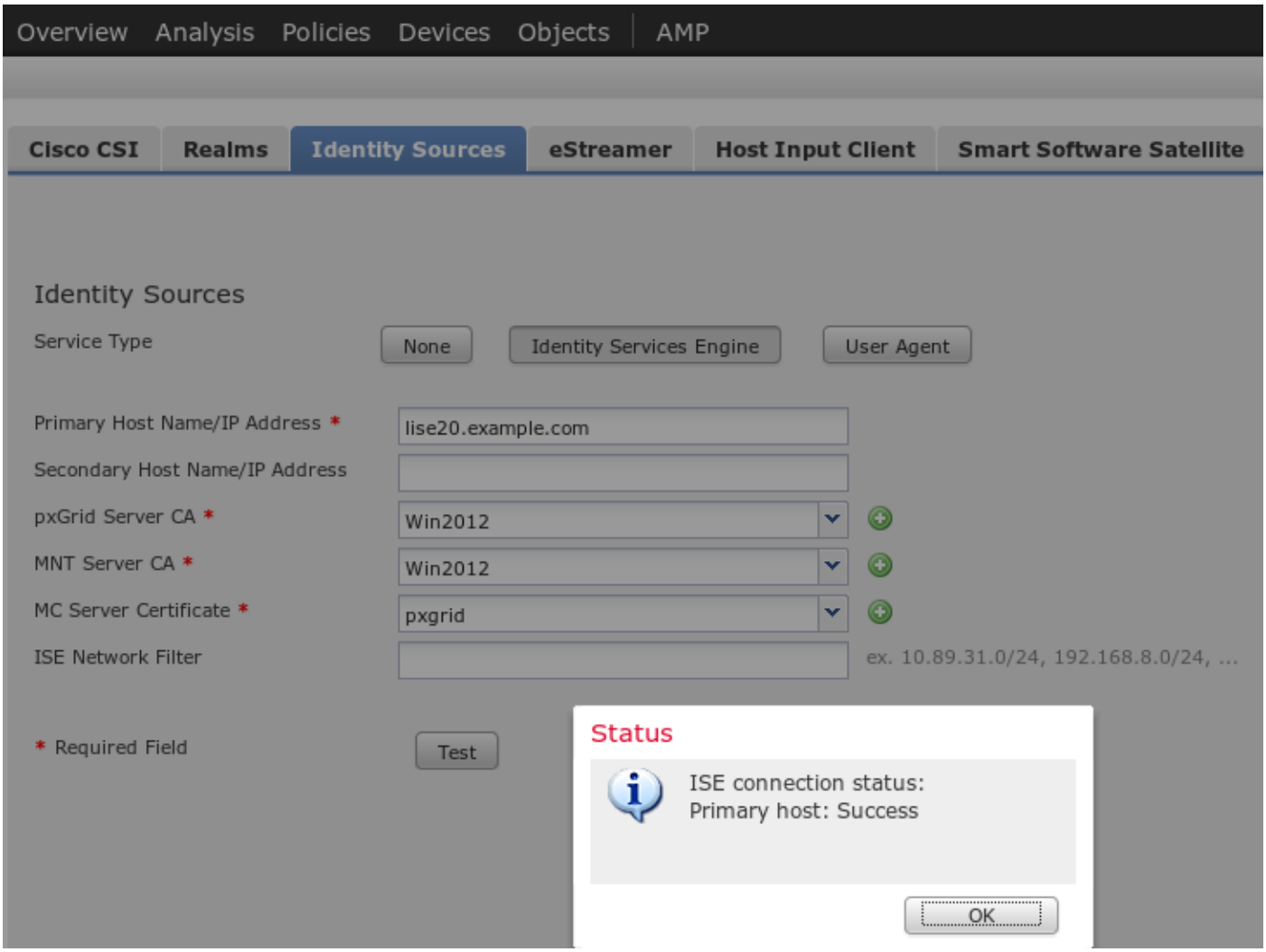
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#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

Une fois que généré fire.csr, le signent utilisant Microsoft CA (modèle de pxGrid). Importez de retour la clé privée (fire.key) et le certificat signé (fire.pem) à la mémoire interne de certificat FMC. Pour l'usage de clé privée le mot de passe a installé pendant la génération de la clé (**commande de genrsa d'**openssl) :



Intégration ISE

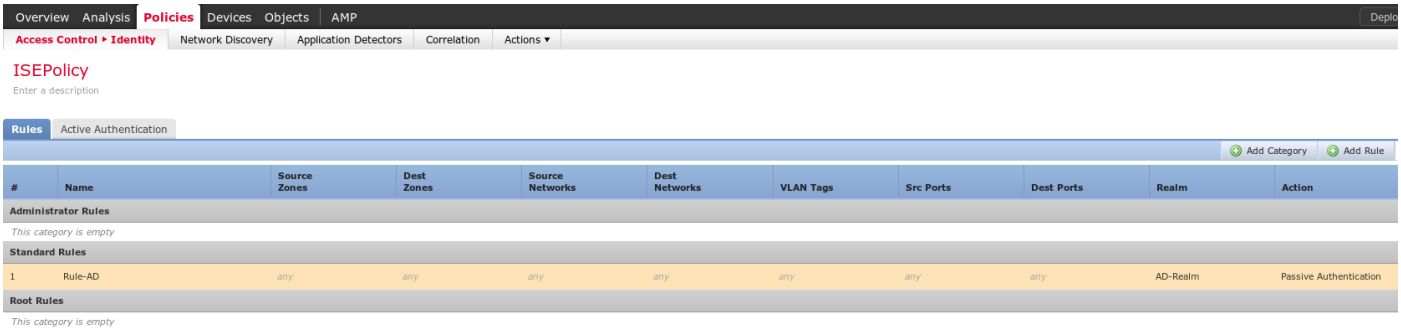
Une fois que tous les Certificats sont installés configurez l'intégration ISE du **système > de l'intégration** :



Utilisez le CA importé pour la validation de Certificats de pxGrid et de services MNT. Pour le certificat interne d'utilisation de console de gestion (MC) généré pour le pxGrid.

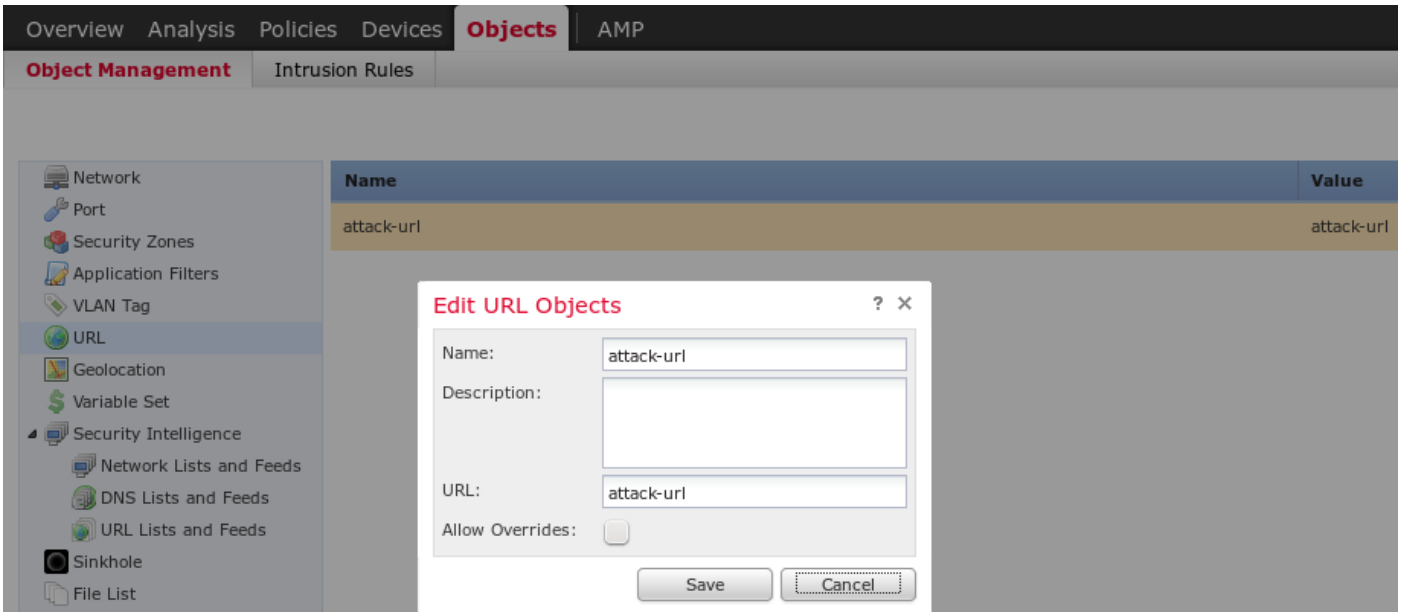
Stratégie d'identité

Configurez la stratégie d'identité qui utilise le royaume précédemment configuré d'AD pour l'authentification passive :

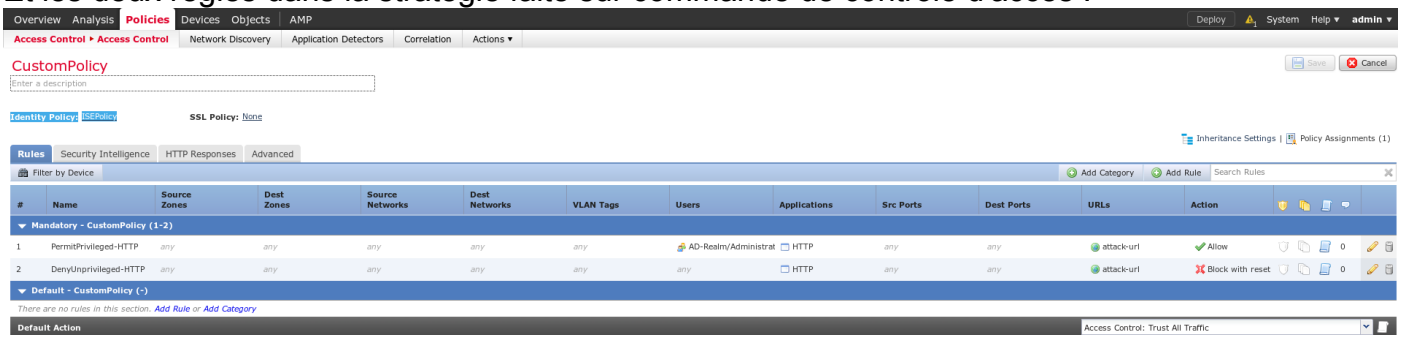


Stratégie de contrôle d'accès

Pour cet exemple l'URL de coutume a été créé :



Et les deux règles dans la stratégie faite sur commande de contrôle d'accès :

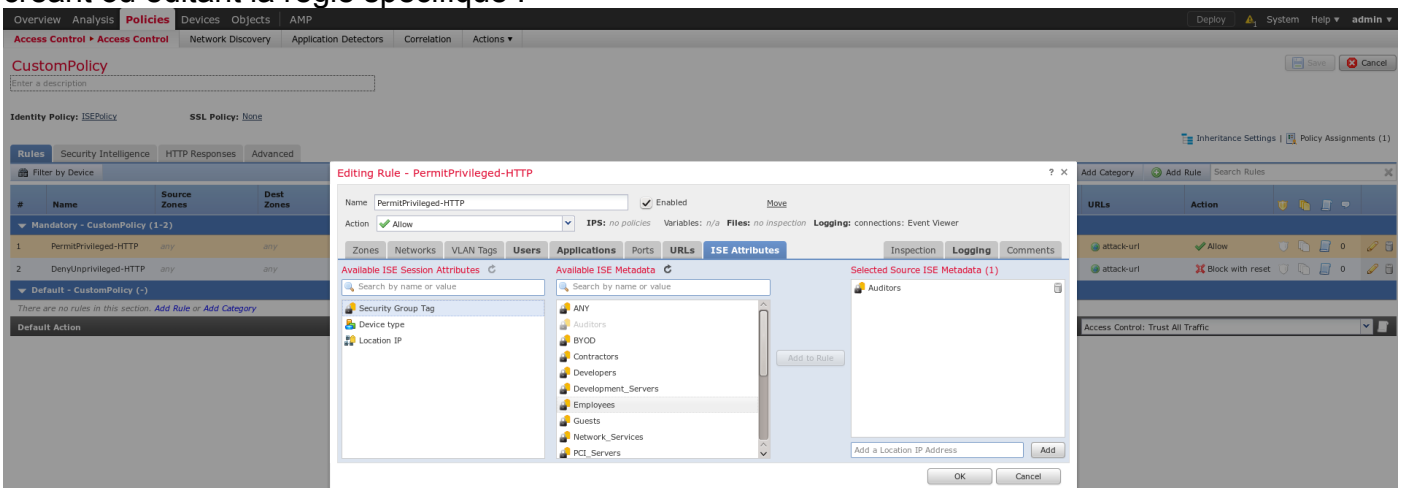


La règle de PermitPrivileged-HTTP permet tous les utilisateurs appartenant au groupe d'administrateurs d'AD qui ont été assignés la balise SGT. Auditeurs pour exécuter l'attaque de HTTP sur toutes les cibles.

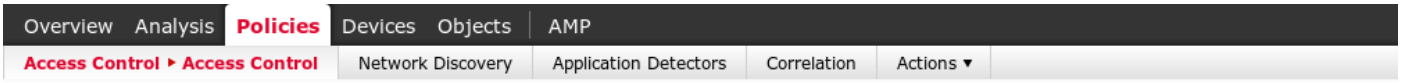
Le DenyUnprivileged-HTTP refuse cette action à tous autres utilisateurs.

Notez également que la stratégie d'identité précédemment créée a été assignée à cette stratégie de contrôle d'accès.

Sur cet onglet ses non possibles de voir des balises SGT, mais sur ceux sont visibles tout en créant ou éditant la règle spécifique :

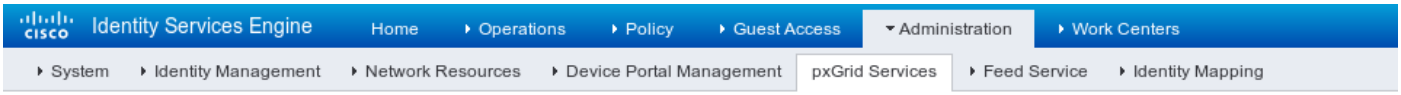


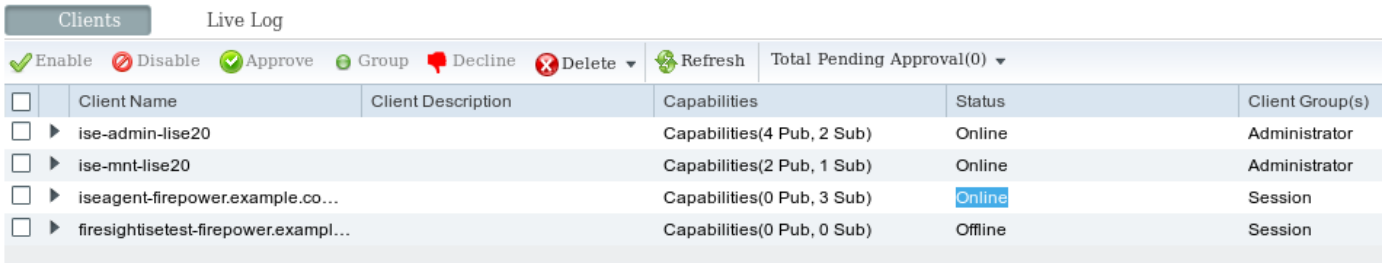
Assurez-vous que la stratégie est assignée au NGIPS et toutes les modifications sont déployées :



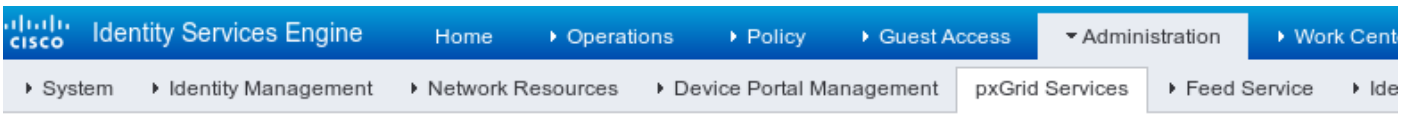
Vérifiez

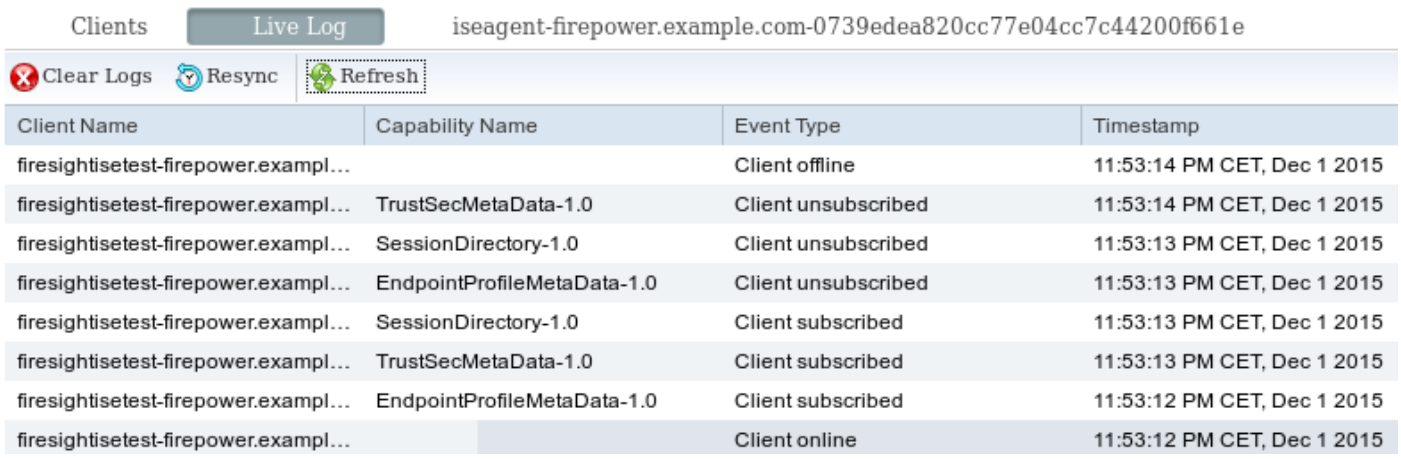
Après que tout soit configuré correctement ISE devrait voir le client de pxGrid s'abonner pour un service de session (état en ligne).





Des logs vous pouvez également confirmer que FMC s'est abonné pour le service de TrustSecMetaData (balises SGT) - ont obtenu toutes les balises et se sont désabonnés.

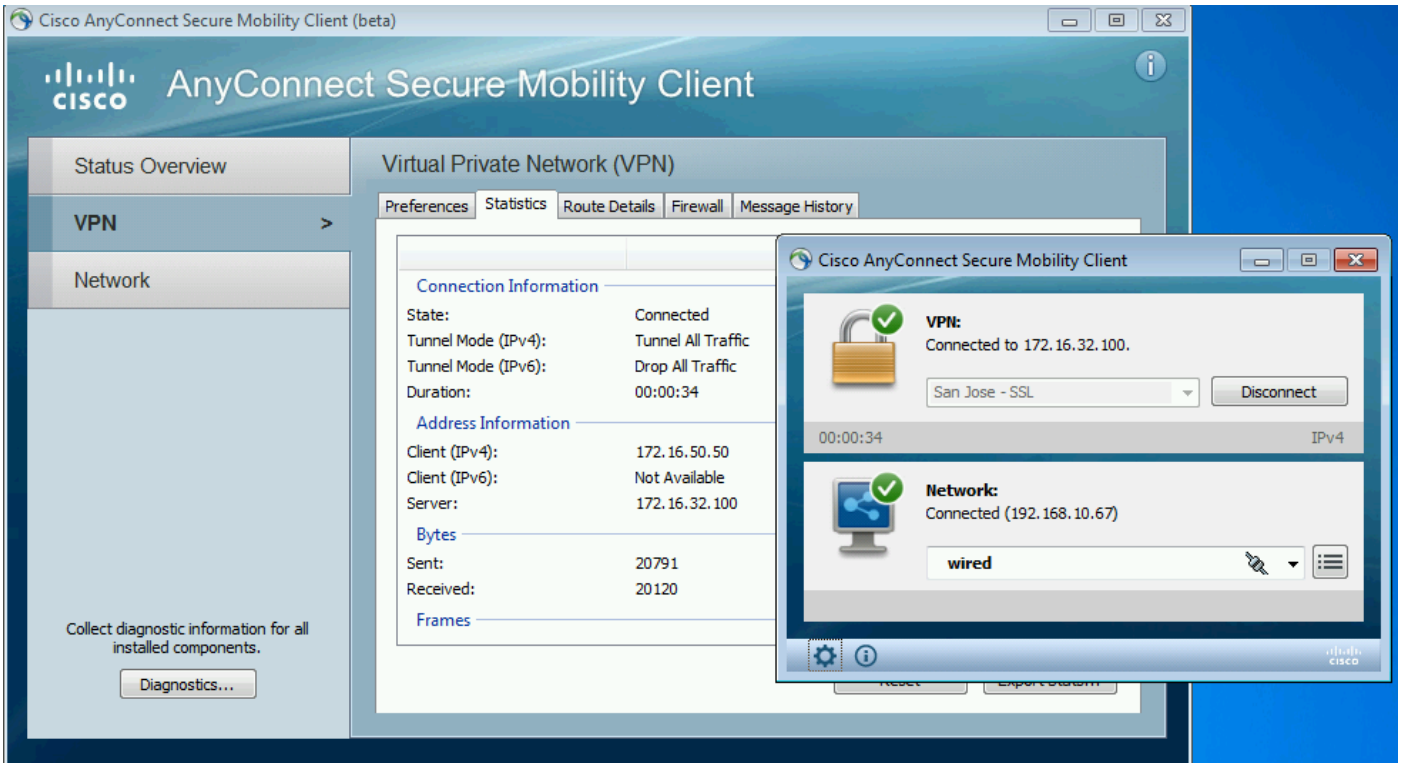




Établissement de session VPN

Le premier essai est réalisé pour un scénario quand l'autorisation sur ISE ne renvoie pas la balise correcte SGT (NGIPS ne tient pas compte des tests de contrôle).

Une fois que la session VPN est EN HAUSSE l'interface utilisateur d'AnyConnect (UI) peut fournir plus de détails :



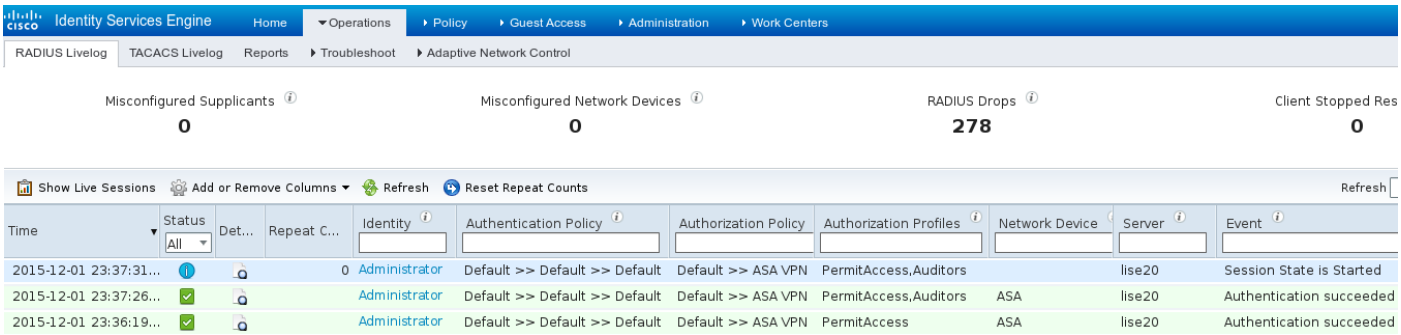
L'ASA peut confirmer la session est établie :

```
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
```

Veuillez noter que l'ASA voit n'importe quelle balise SGT retournée pour cette authentification. L'ASA n'est pas configurée pour TrustSec - de sorte que les informations soient ignorées de toute façon.

ISE est également signalant l'autorisation réussie (le log à 23:36:19) - aucune balise SGT retournée :



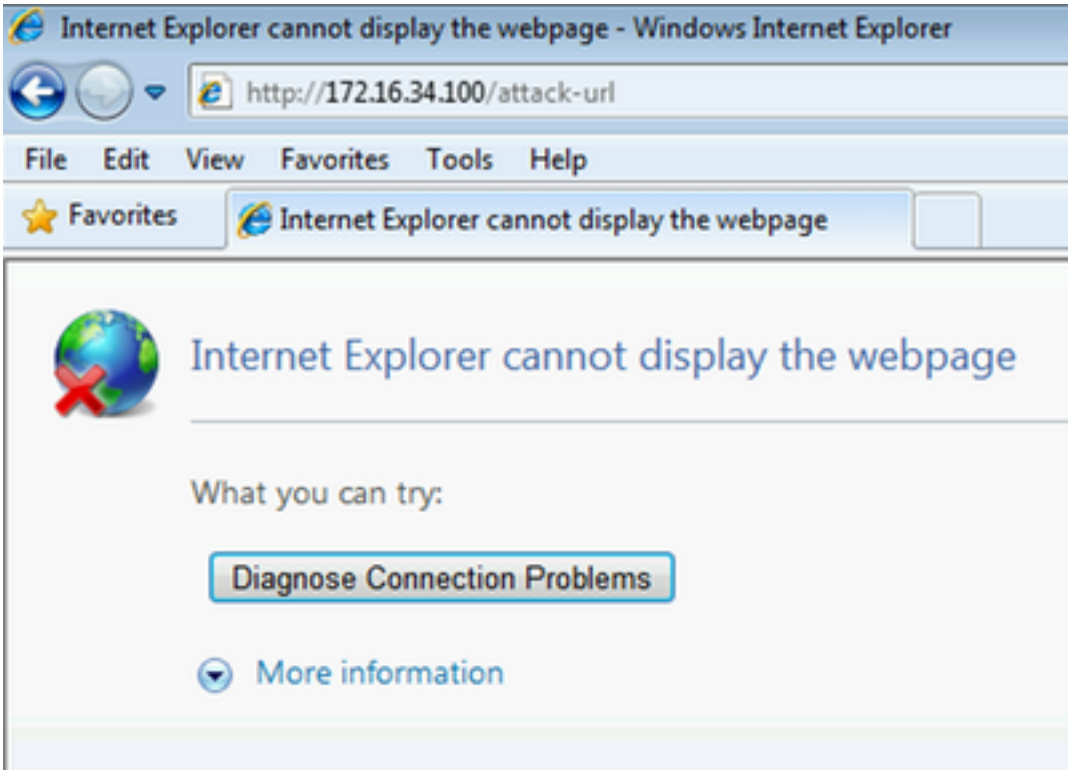
FMC obtenant des données de session de MNT

Àcette étape FMC dans /var/log/messages signale une nouvelle session (reçue en tant qu'abonné pour le service de pxGrid) pour le nom d'utilisateur d'administrateur et la consultation d'AD de peform pour l'adhésion à des associations :

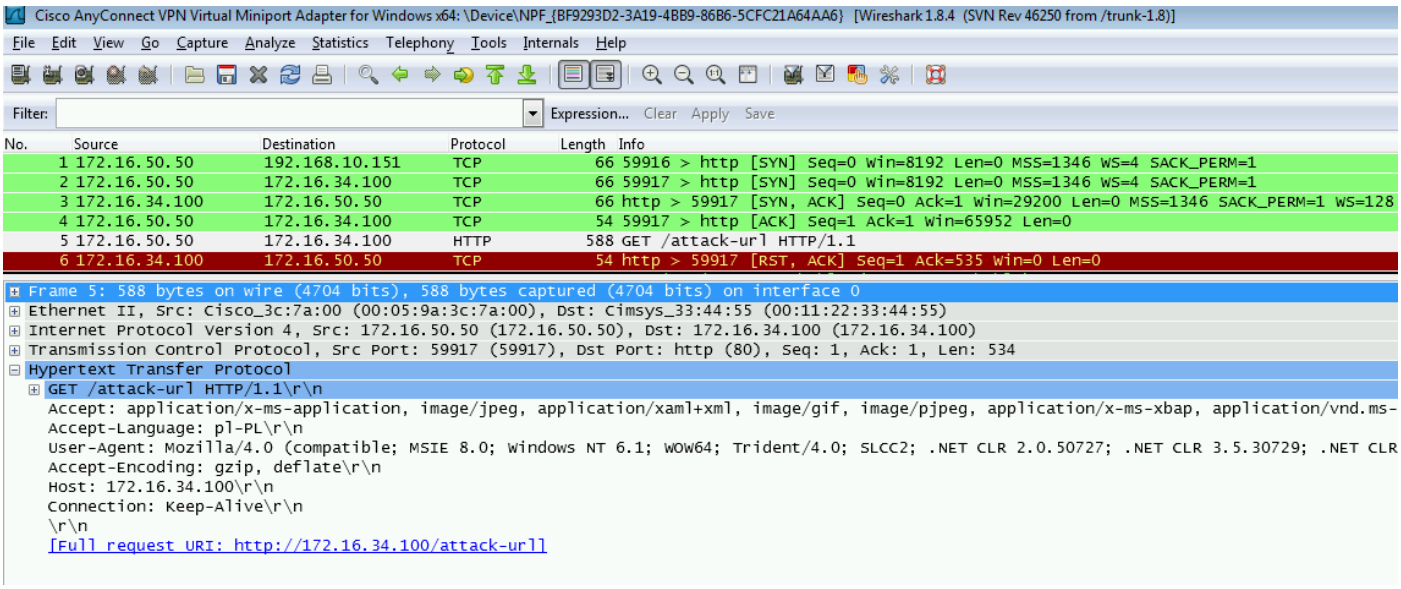
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

Accès au réseau non privilégié et privilégié

Quand aux essais de cet utilisateur d'étape pour ouvrir le navigateur Web et à l'accéder à a audité le serveur, la connexion sera terminée :



Il peut être confirmé par les captures de paquet prises du client (le TCP RST envoient selon la configuration FMC) :

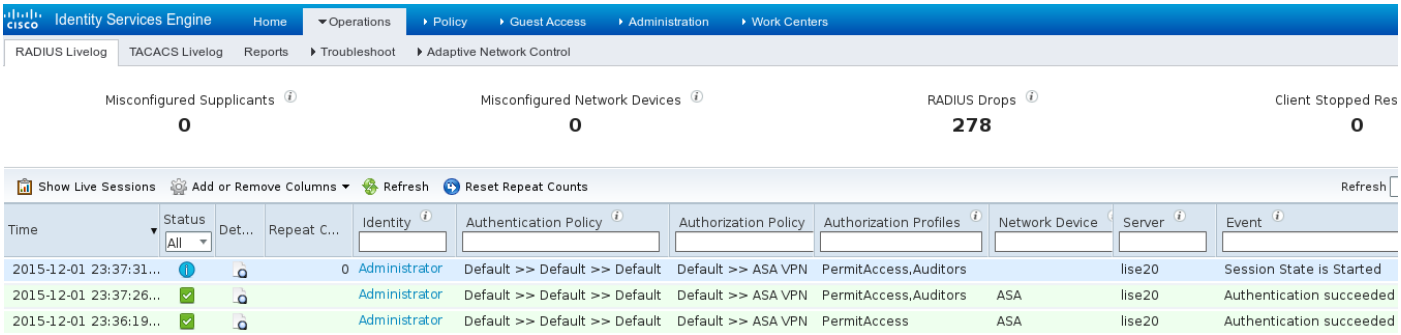


Une fois qu'ISE est configuré pour retourner, la session de la balise ASA d'audit signale :

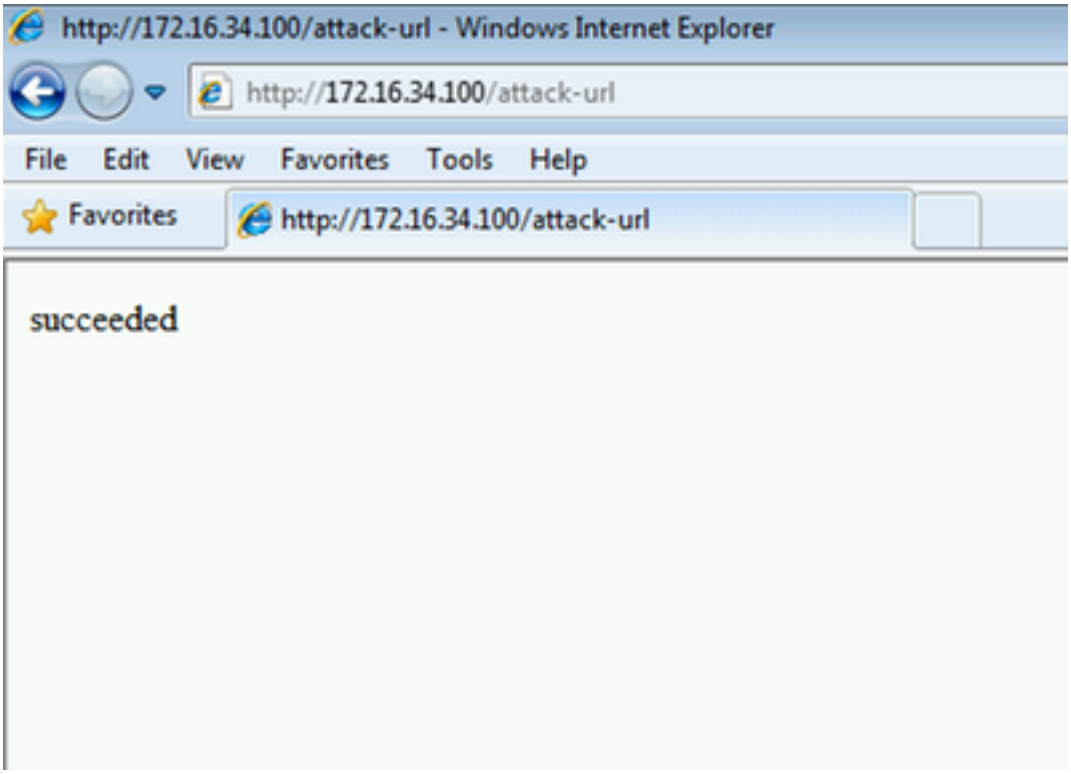
```
asav# show vpn-sessiondb anyconnect

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 est signale également un auditeur réussi de balise de l'autorisation (le log à 23:37:26) - SGT est retourné :

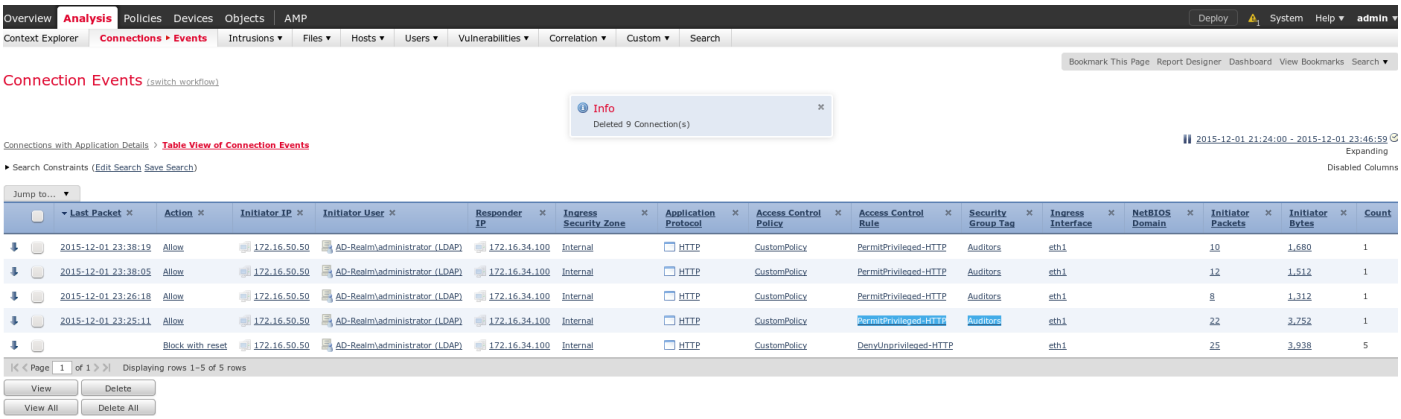


Et l'utilisateur peut accéder au service mentionné :



FMC se connectant l'accès

Cette activité peut être confirmée par état d'événement de connexion :



D'abord, l'utilisateur n'a fait assigner aucune balise SGT et frappait la règle de DenyUnprivileged-HTTP. Une fois que la balise de l'auditeur a été assignée par règle ISE (et récupérée par FMC), le PermitPrivileged-HTTP est utilisé et l'accès est permis.

Notez également cela pour avoir l'affichage, de plusieurs colonnes ont été retirées parce que normalement la balise de règle et de groupe de sécurité de contrôle d'accès sont affichées en tant qu'une des dernières colonnes (et de la barre de défilement horizontale doit être utilisé). Que la vue personnalisée peut être enregistrée et réutilisée à l'avenir.

Dépannez

FMC met au point

Pour vérifier les logs du composant ADI responsables du contrôle /var/log/messages de gestions d'identité classent :

```
[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
```

Pour obtenir plus détaillé le met au point est possible pour détruire le processus ADI (de la racine après sudo) et l'exécuter avec mettent au point l'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.......>
```

Requête SGT par l'intermédiaire de pxGrid

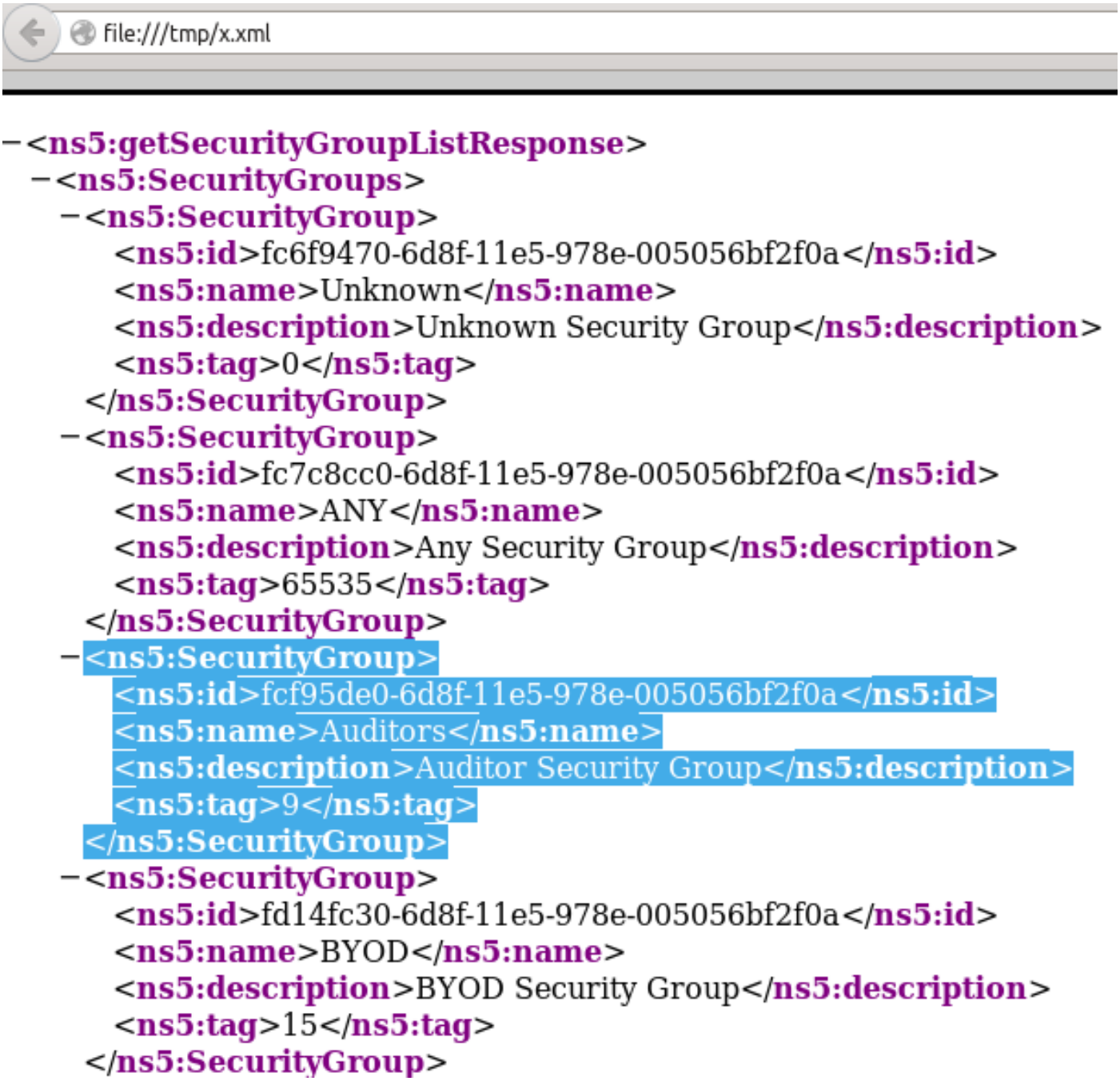
L'exécution est exécutée quand la touche "TEST" est cliquée sur dans la section d'**intégration ISE**

ou quand la liste SGT est régénérée, tout en ajoutant la règle dans la stratégie de contrôle d'accès.

```
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>]

Pour un meilleur xml de vue un contenu de ce log peut être copié sur le fichier de xml et être ouvert par un navigateur Web. Vous pouvez confirmer que la particularité SGT (audit) est reçue aussi bien que tout autre SGT est défini sur ISE :



Requête de session par l'intermédiaire du REPOS API au MNT

C'est également une partie d'exécution de test (notez s'il vous plaît que cette adresse Internet et port MNT est passé par l'intermédiaire du pxGrid). Le téléchargement en vrac de session est utilisé :

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>fc6f9470-6d8f-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>fc7c8cc0-6d8f-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>fcf95de0-6d8f-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>fd14fc30-6d8f-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>fd2fb020-6d8f-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>fd4e34a0-6d8f-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>fd6d2e50-6d8f-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>fda10f90-6d8f-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>fdbcd4f0-6d8f-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>fdd9abc0-6d8f-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>fdf4d4e0-6d8f-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>fe11abb0-6d8f-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>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>]
```

Et résultat analysé (1 session active reçue) :

```
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}
```

Àcette étape NGIPS est des essais pour corréler ce nom d'utilisateur (et domaine) avec le nom d'utilisateur de Royaume-AD :

```
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
```

Le LDAP est utilisé pour trouver un utilisateur et une adhésion à des associations :

```
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 met au point

Après l'activation du niveau de SUIVI mettez au point pour le composant de pxGrid son possible de vérifier chaque exécution (mais sans charge utile/données comme sur FMC).

Exemple avec la récupération de balise SGT :

```
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
```

Bogues

CSCuv32295 - ISE peut envoyer l'information de domaines dans des domaines de nom d'utilisateur

CSCus53796 - Incapable d'obtenir le FQDN de l'hôte pour la requête en vrac de REPOS

CSCuv43145 - PXGRID et reprise de service de mappage d'identité, importation/effacement de mémoire de confiance

Références

- Configurez les services de correction avec l'intégration ISE et de FirePOWER
- Configurer le pxGrid dans un environnement distribué ISE
- Comment-Faire déployant des Certificats avec le pxGrid de Cisco : Configurer le noeud Ca-signé de pxGrid ISE et le client Ca-signé de pxGrid
- Intégration de pxGrid de version 1.3 ISE avec l'application de pxLog IPS
- Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 2.0
- Guide de référence du Logiciel Cisco Identity Services Engine API, version 1.2 – Introduction à S reposant externe…
- Guide de référence du Logiciel Cisco Identity Services Engine API, version 1.2 – Introduction à la recherche de surveillance…
- Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 1.3
- Support et documentation techniques - Cisco Systems