Troubleshooting ISE e integración de FirePOWER para los servicios de la identidad

Contenido

Introducción

Este documento describe cómo configurar y resolver problemas las directivas enteradas de TrustSec en el sistema de prevención de intrusiones de la última generación de Cisco (NGIPS). La versión 6.0 NGIPS soporta la integración con el Identity Services Engine (ISE) que permite construir las directivas enteradas basadas identidad.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración VPN adaptante del dispositivo de seguridad de Cisco (ASA)
- Configuración de Cliente de movilidad Cisco AnyConnect Secure
- Configuración básica del centro de administración de Cisco FirePOWER
- Configuración de Cisco ISE
- Soluciones de Cisco TrustSec

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Certificate Authority (CA) de Microsoft Windows 2012
- Versión de ASA 9.3 de Cisco
- Versiones de software 1.4 de Cisco ISE
- Versiones 4.2 del Cliente de movilidad Cisco AnyConnect Secure
- Versión 6.0 del centro de administración de Cisco FirePOWER (FMC)
- Versión 6.0 de Cisco FirePOWER NGIPS

Configurar

El centro de administración de FirePOWER (FMC) es la plataforma de administración para FirePOWER. Hay dos tipos de funciones relacionadas con la integración ISE:

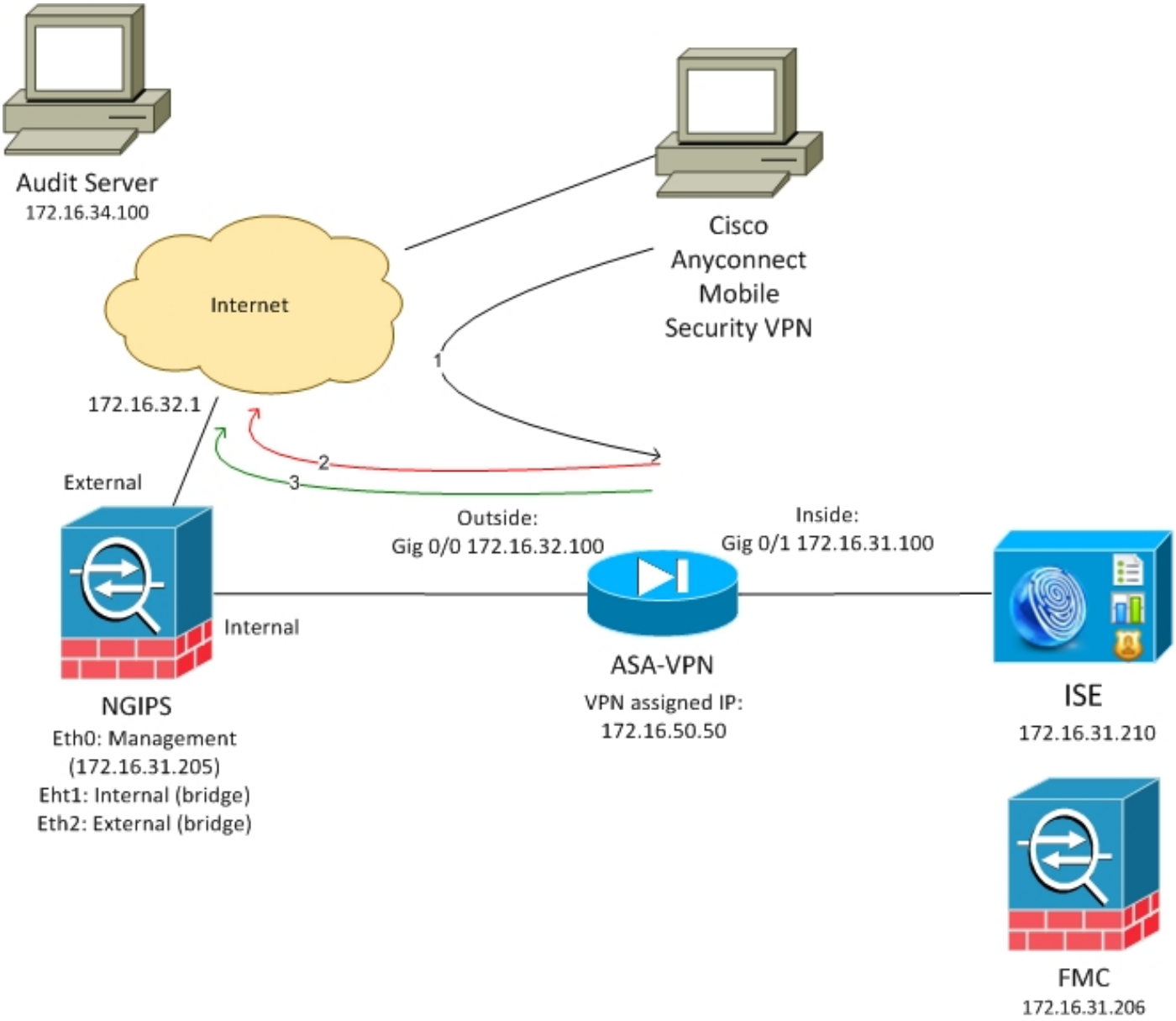
- Corrección - permite que FMC quarantine el atacante vía el ISE, que es estatus de autorización de intercambio dinámico en el dispositivo de acceso que proporciona al acceso a la red limitado. Hay dos generaciones de esta solución:

1. Script Perl de la herencia usando la llamada del servicio de protección del punto final (EP) API al ISE.
2. Un módulo más nuevo usando la llamada del protocolo del pxGrid al ISE (este módulo se soporta solamente en la versión 5.4 - no soportada en 6.0, soporte nativo previsto en 6.1).

- Directiva - permite que FMC configure las directivas basadas en las etiquetas del grupo de seguridad de TrustSec (SGT).

Este artículo se centra en las segundas funciones. Para la corrección el ejemplo leyó por favor la sección de referencias

Diagrama de la red



FMC se configura con la directiva del control de acceso que contiene dos reglas:

- Niegue para el tráfico HTTP con la aduana URL (el ataque-URL)
- Tenga en cuenta el tráfico HTTP con la aduana URL (ataque-URL) pero solamente si el ISE asigna el usuario para auditoría (9) la etiqueta SGT

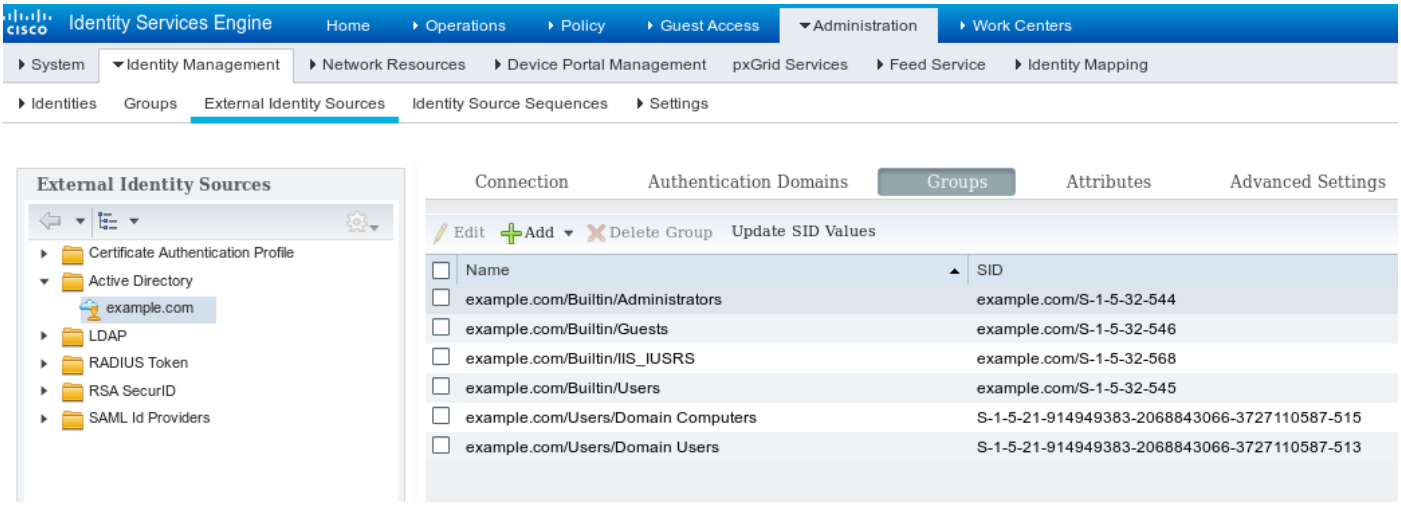
El ISE decide a asignar la etiqueta de la auditoría a todos los usuarios de Active Directory que pertenece al Grupo del administrador y utiliza el dispositivo ASA-VPN para el acceso a la red.

Red de los accesos del usuario vía la conexión VPN en el ASA. El usuario entonces intenta acceder el servidor auditoría usando URL ataque-URL - pero falla porque le no han asignado para auditoría al grupo SGT. Una vez que se repara eso, la conexión es acertada.

ISE

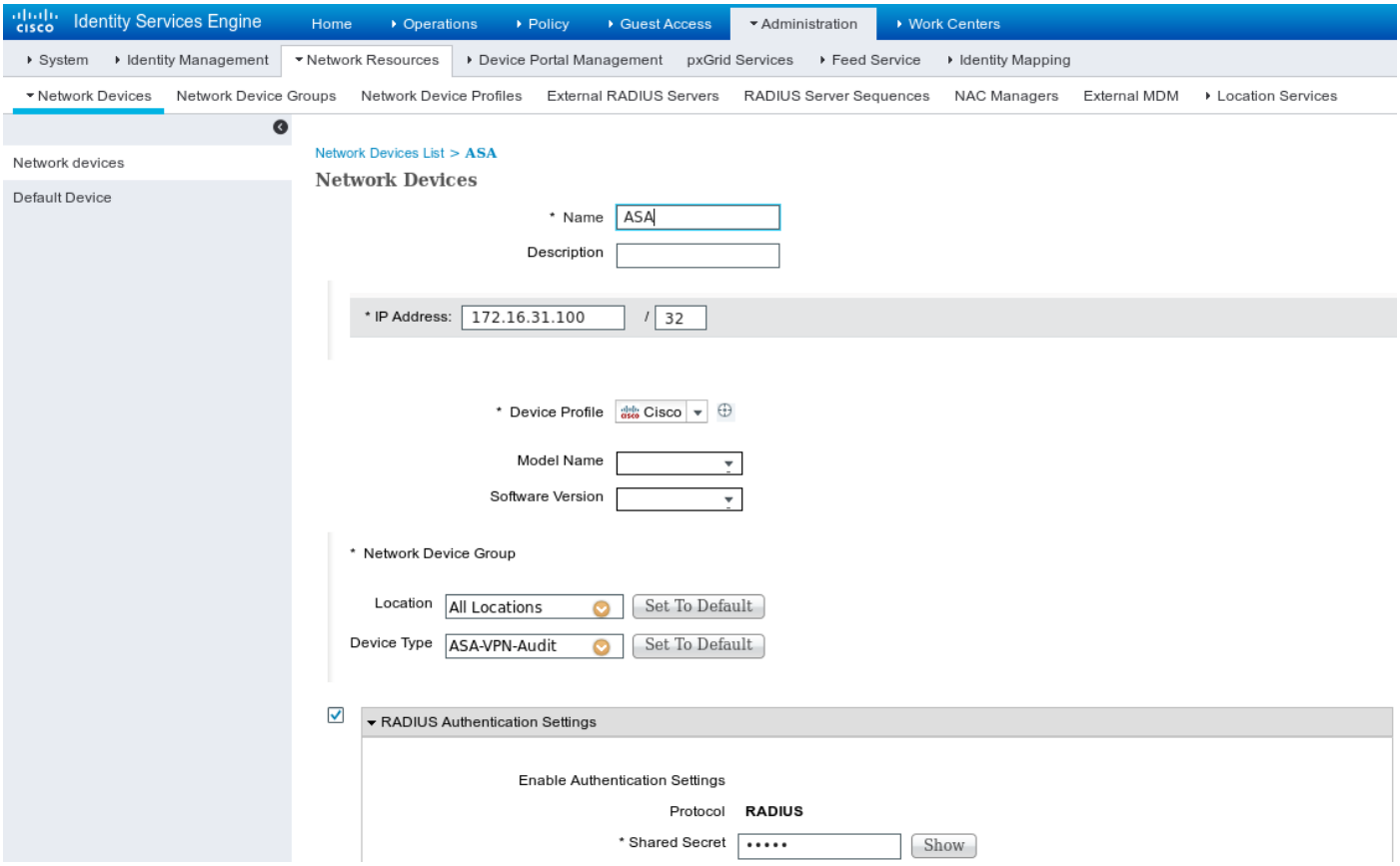
Active Directory

La integración AD debe ser configurada y los grupos correctos deben ser traídos (utilizan al grupo de los administradores para la condición de la regla de la autorización):



Dispositivo de acceso a la red

El ASA se agrega como dispositivo de red. La ASA-VPN-auditoría de encargo del grupo se utiliza, tal y como se muestra en de esta imagen:



Certificados para el pxGrid y el MNT

FMC utiliza ambos servicios en el ISE:

- pxGrid para SGT y perfilar la interrogación de los datos
- Supervisión e información (MNT) para la descarga a granel de la sesión

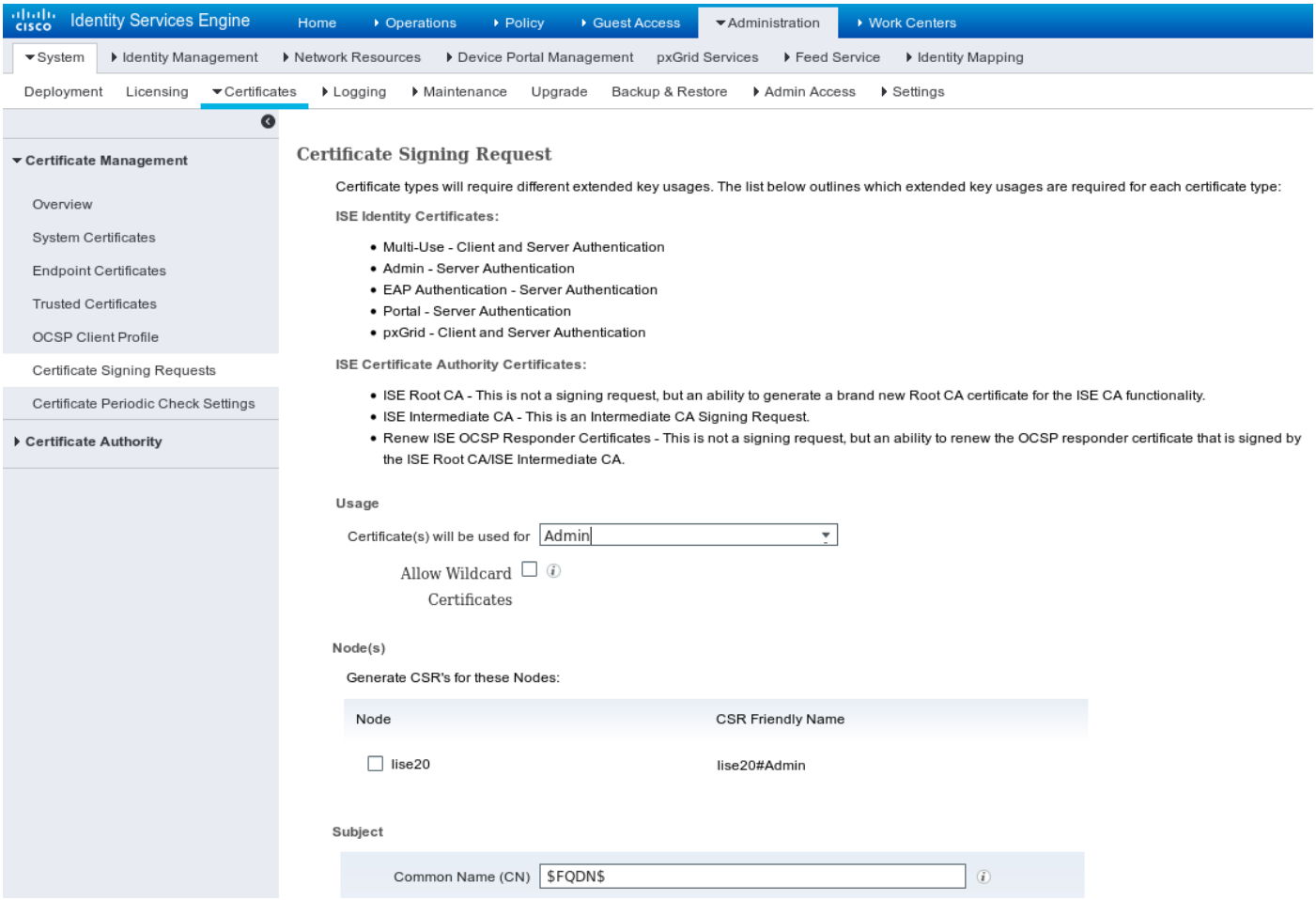
La Disponibilidad MNT es muy importante puesto que esta manera FMC está siendo informada cuál es la dirección IP de la sesión autenticada, también su nombre de usuario y etiqueta SGT. De acuerdo con eso, las directivas correctas pueden ser aplicadas. Note por favor que NGIPS no

soporta nativo las etiquetas SGT (en línea el marcar con etiqueta) como el ASA. Pero en el contrario al ASA, soporta los nombres SGT en vez de los números solamente.

Debido a esos requisitos el ISE y FMC necesita confiarse en servicio (certificado). El MNT utiliza apenas el certificado del lado del servidor, pxGrid utiliza ambo el certificado del lado del cliente y servidor.

Microsoft CA se utiliza para firmar todos los Certificados.

Para MNT (papel Admin) el ISE debe generar el pedido de firma de certificado (CSR), tal y como se muestra en de esta imagen:



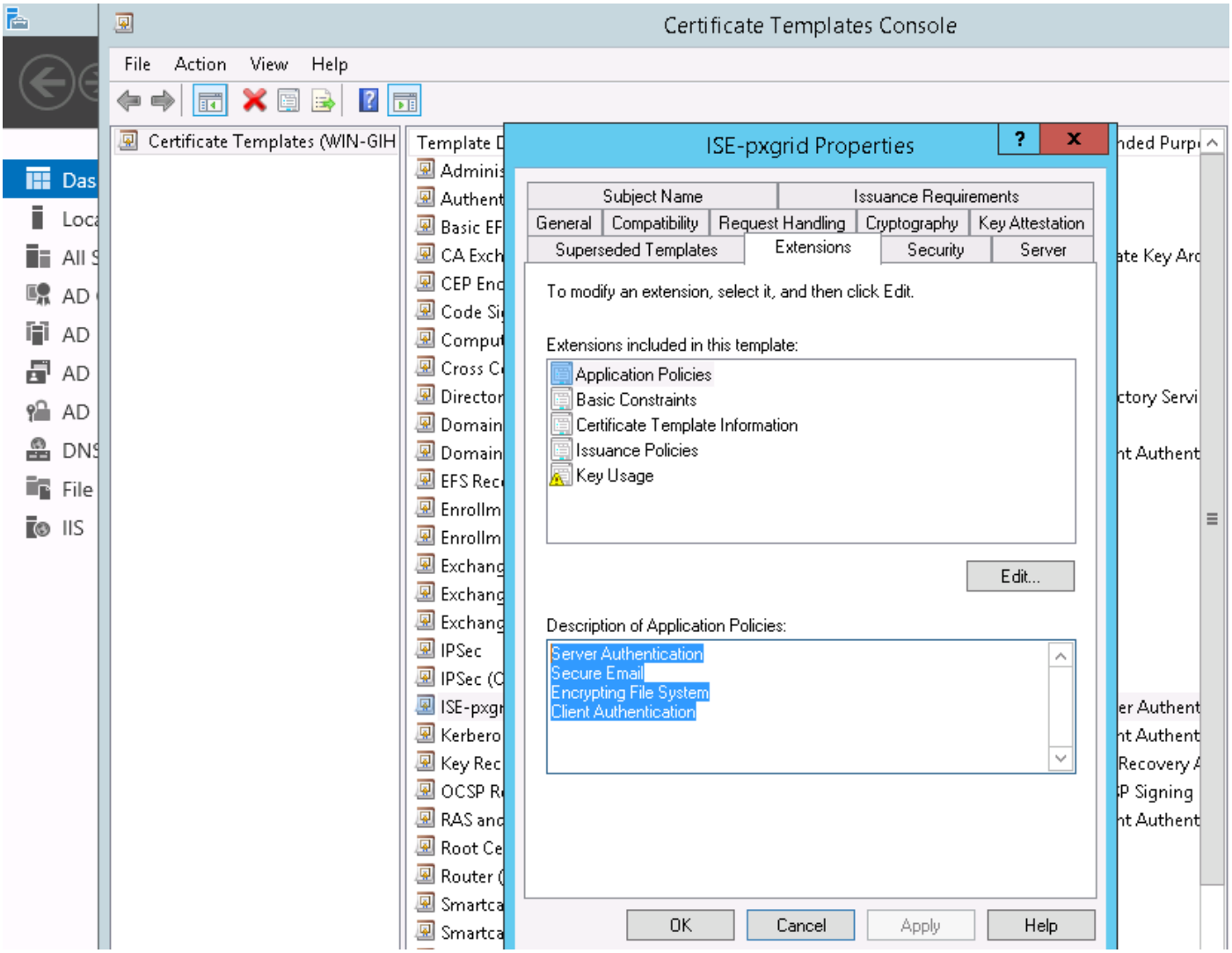
Después de ser firmada por Microsoft CA debe ser importado vía la opción del **certificado del lazo**.

El proceso similar se debe seguir para el servicio del pxGrid. **Los certificados serán utilizados para la** opción deben hacer el pxGrid seleccionar.

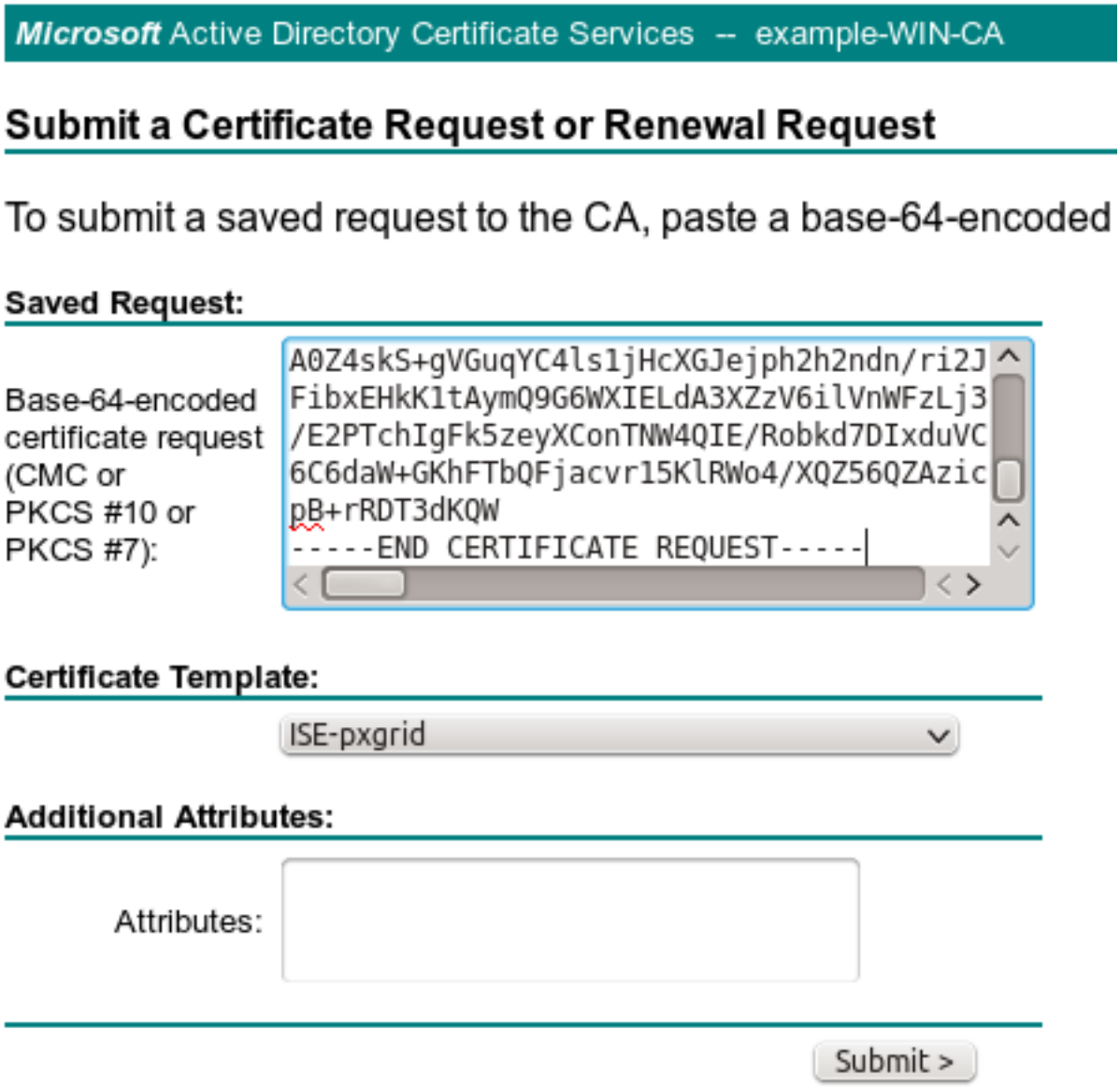
Puesto que no puede haber dos Certificados con el asunto idéntico es completamente aceptable agregar diferente valora para la sección OU o O (por ejemplo pxGrid).

> **Note**: Aseegurese por favor que para cada nombre de dominio completo (FQDN) para el ISE y FMC, el expediente correcto DNS está configurado en el servidor DNS.

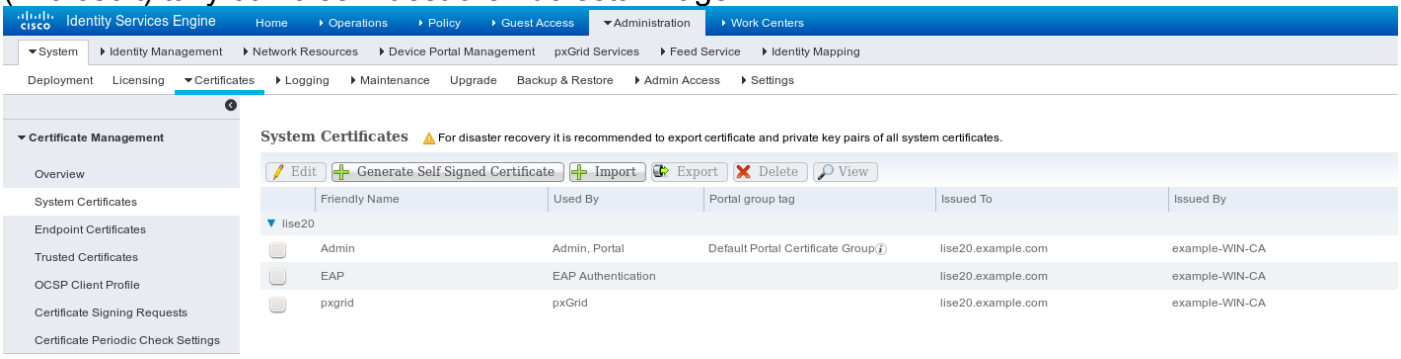
La única diferencia entre el Admin y el certificado del pxGrid está con el proceso de firma. Puesto que los Certificados del pxGrid deben haber extendido las opciones de uso dominantes para ambos plantilla personalizada de la autenticación de cliente y servidor en Microsoft CA se pueden utilizar para eso:



Cómo utilizar el servicio de Web de Microsoft para firmar el pxGrid CSR se muestra en esta imagen:

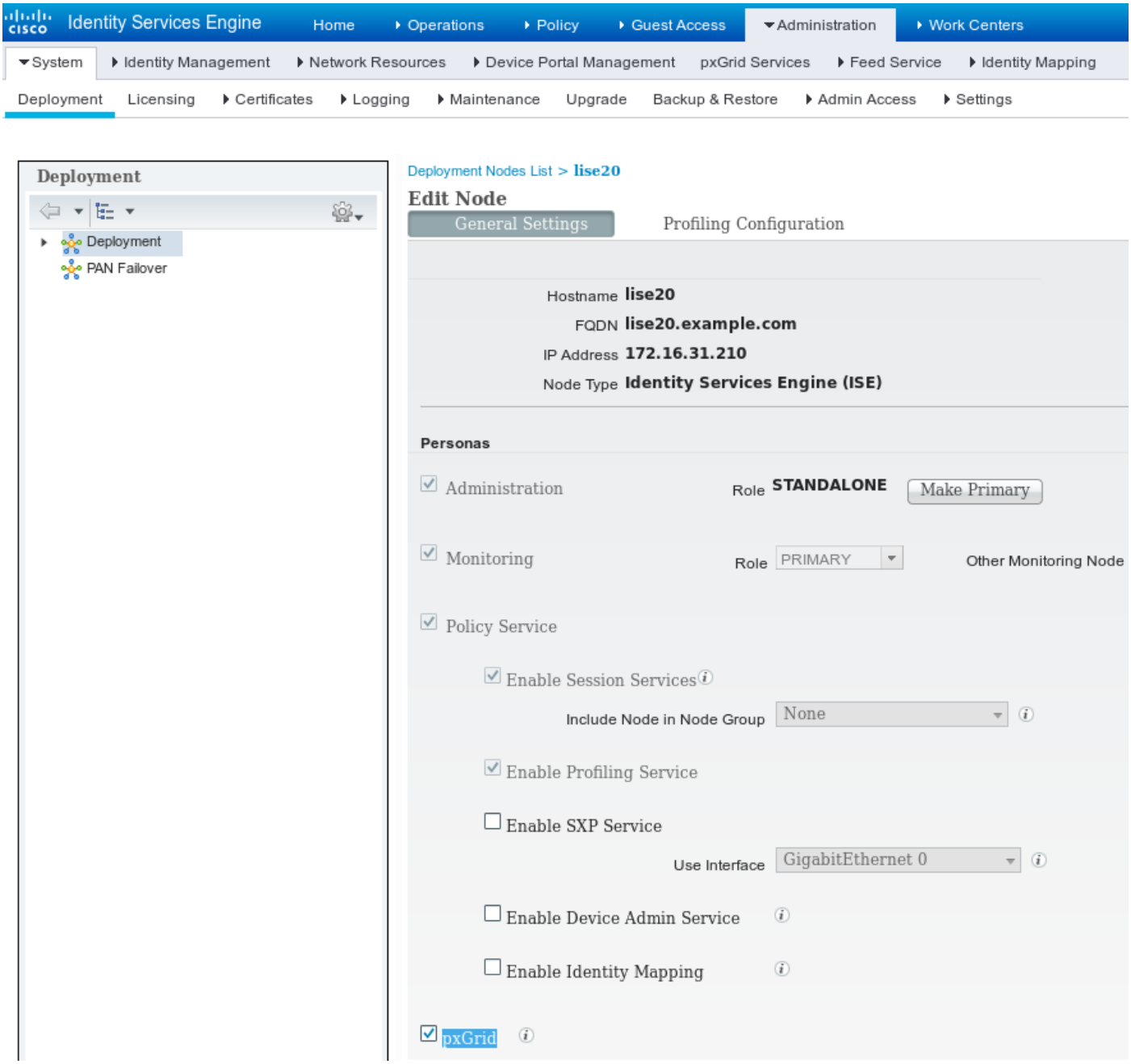


En el extremo el ISE debe tener el Admin y Certificados del pxGrid firmados por CA de confianza (Microsoft) tal y como se muestra en de esta imagen:

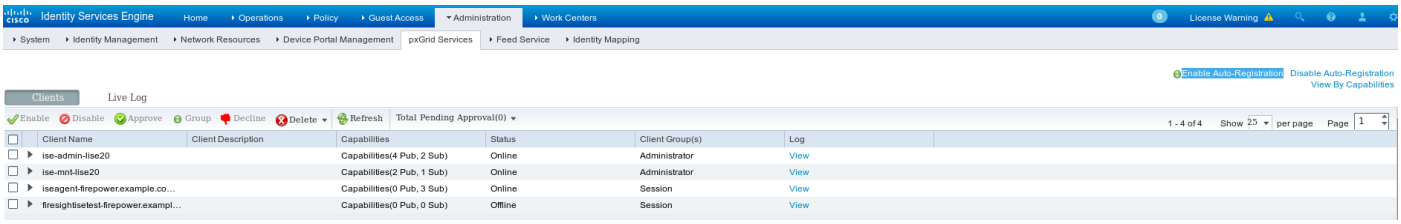


servicio del pxGrid

Con los Certificados correctos el papel del pxGrid del nodo específico se debe habilitar, tal y como se muestra en de esta imagen:



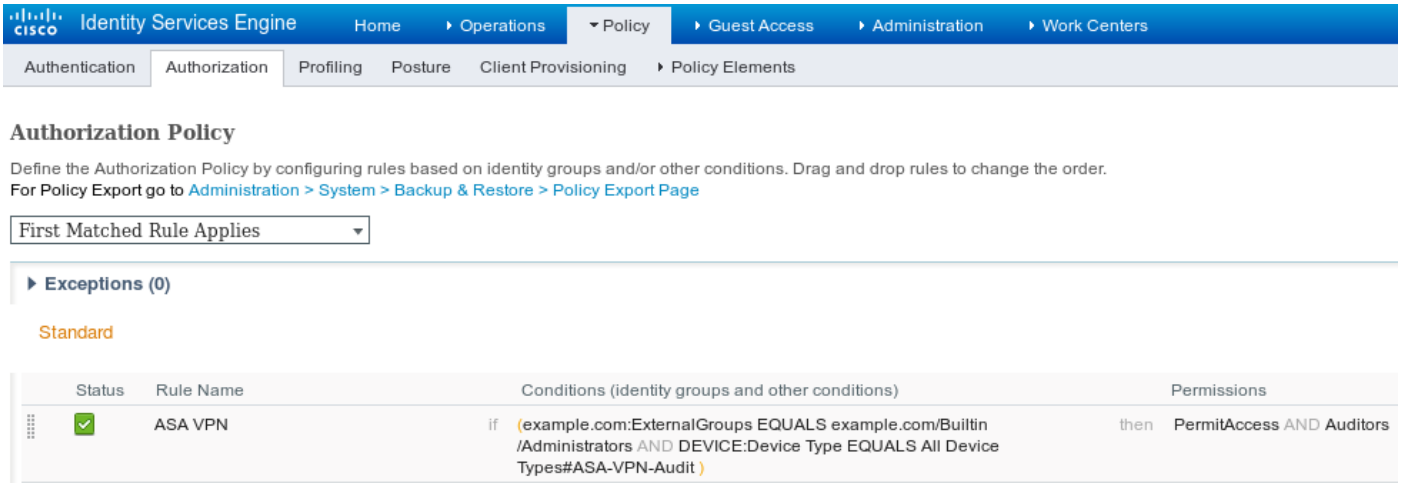
Y la aprobación automática se debe fijar a habilitado:



Directiva de la autorización

Se utiliza la directiva de la autenticación predeterminada (se realizan las operaciones de búsqueda AD si no encuentran al usuario local).

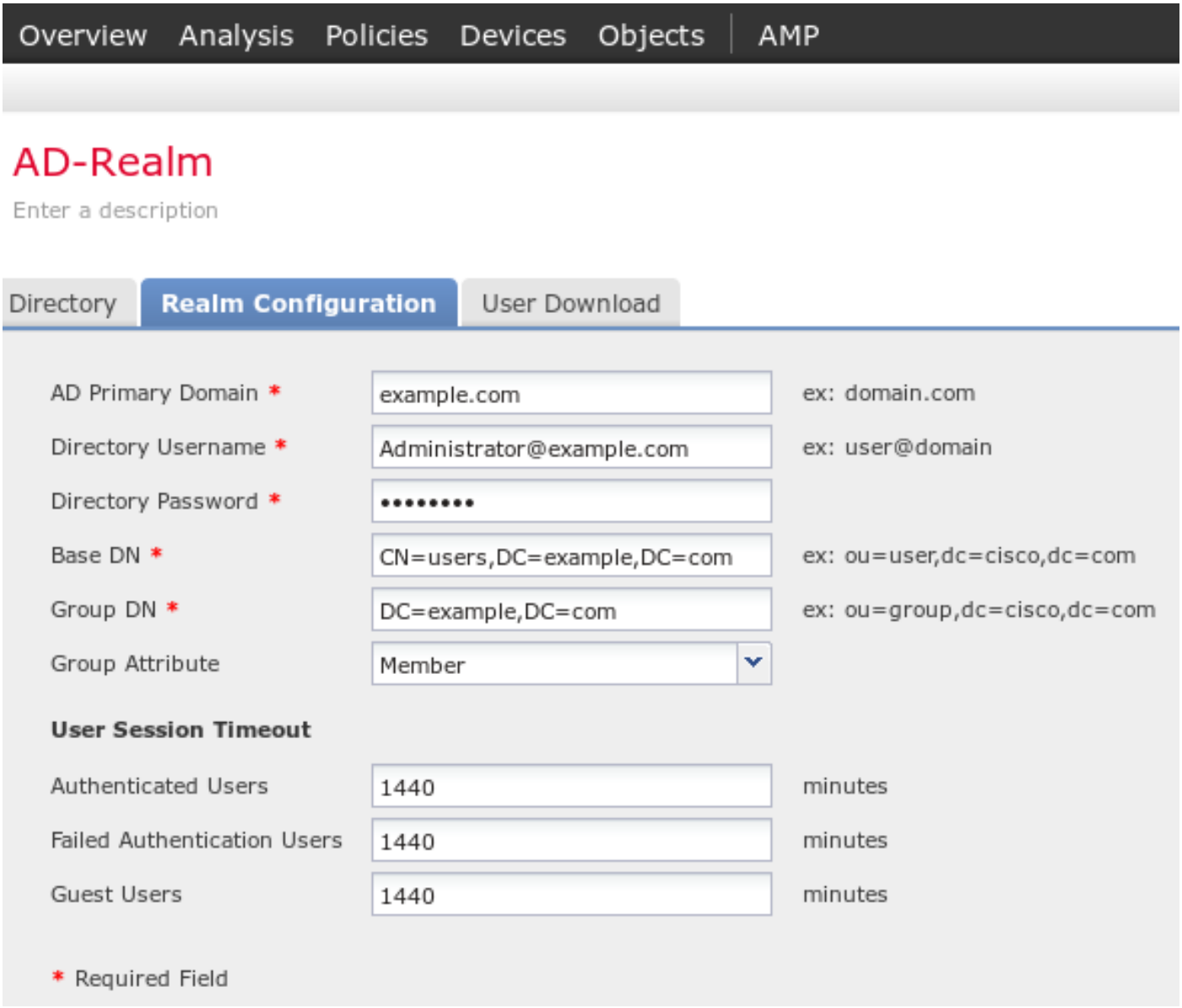
La directiva de la autorización se ha configurado para proporcionar el acceso a la red completo (permiso: PermitAccess) para los usuarios que autentican vía ASA-VPN y que pertenecen a los administradores del grupo del Active Directory - para esos interventores de la etiqueta de los usuarios SGT se vuelve:



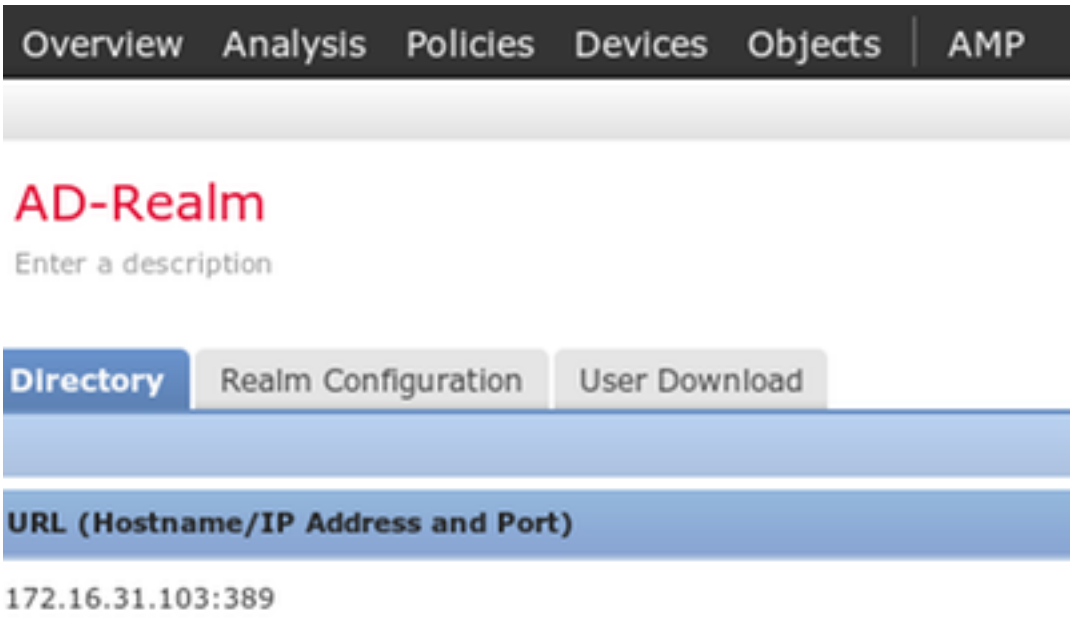
FMC

Reino del Active Directory

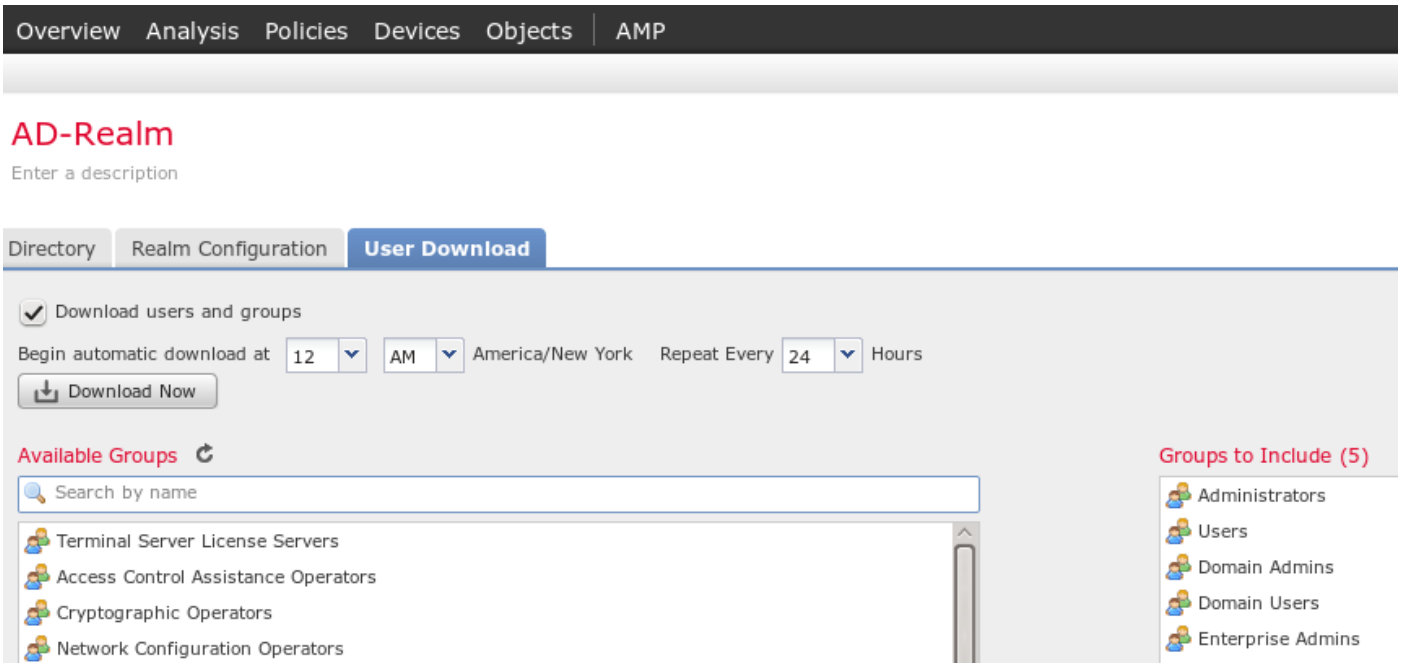
La configuración del reino se requiere para trabajar con la integración ISE (utilizar las directivas de la identidad y extraer la membresía del grupo para pasivo los usuarios autenticados). El reino se puede configurar para el Active Directory o el Lightweight Directory Access Protocol (LDAP). En este ejemplo se está utilizando el AD. **Del sistema > de la integración > del reino**:



Se utilizan las configuraciones del directorio estándar:

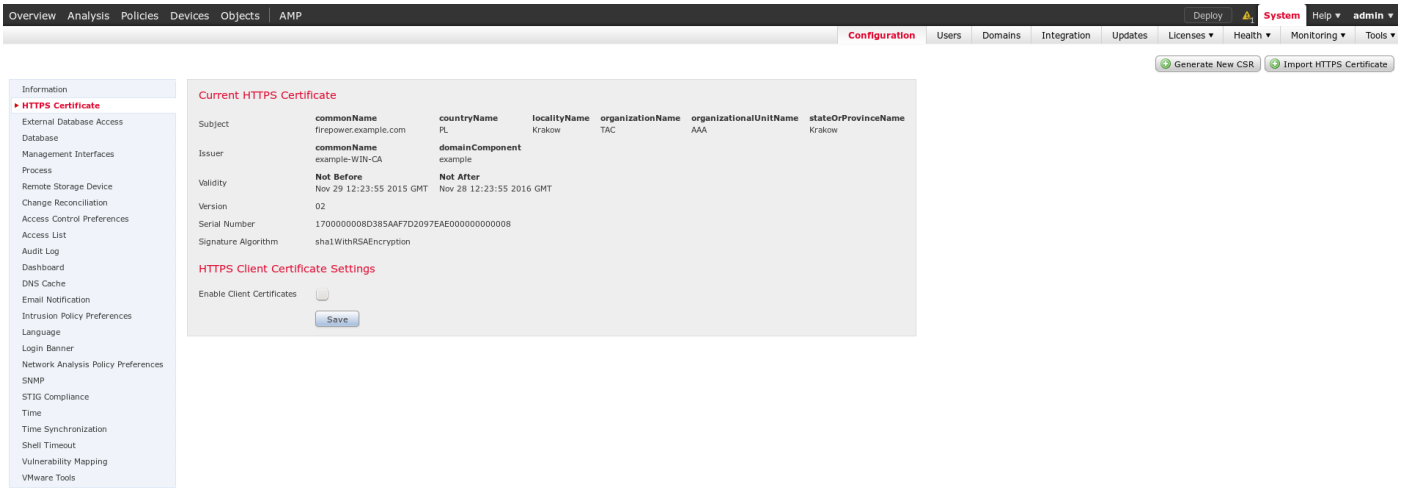


Y extraen algunos de los grupos AD (ser utilizado como la condición adicional en el control de acceso gobierna):



Certificados para el Admin y el pxGrid

Aunque no esté requerido, su una práctica adecuada de generar el CSR para el acceso admin. Firme ese CSR usando el AD de confianza, importación detrás el certificado firmado, tal y como se muestra en de esta imagen:

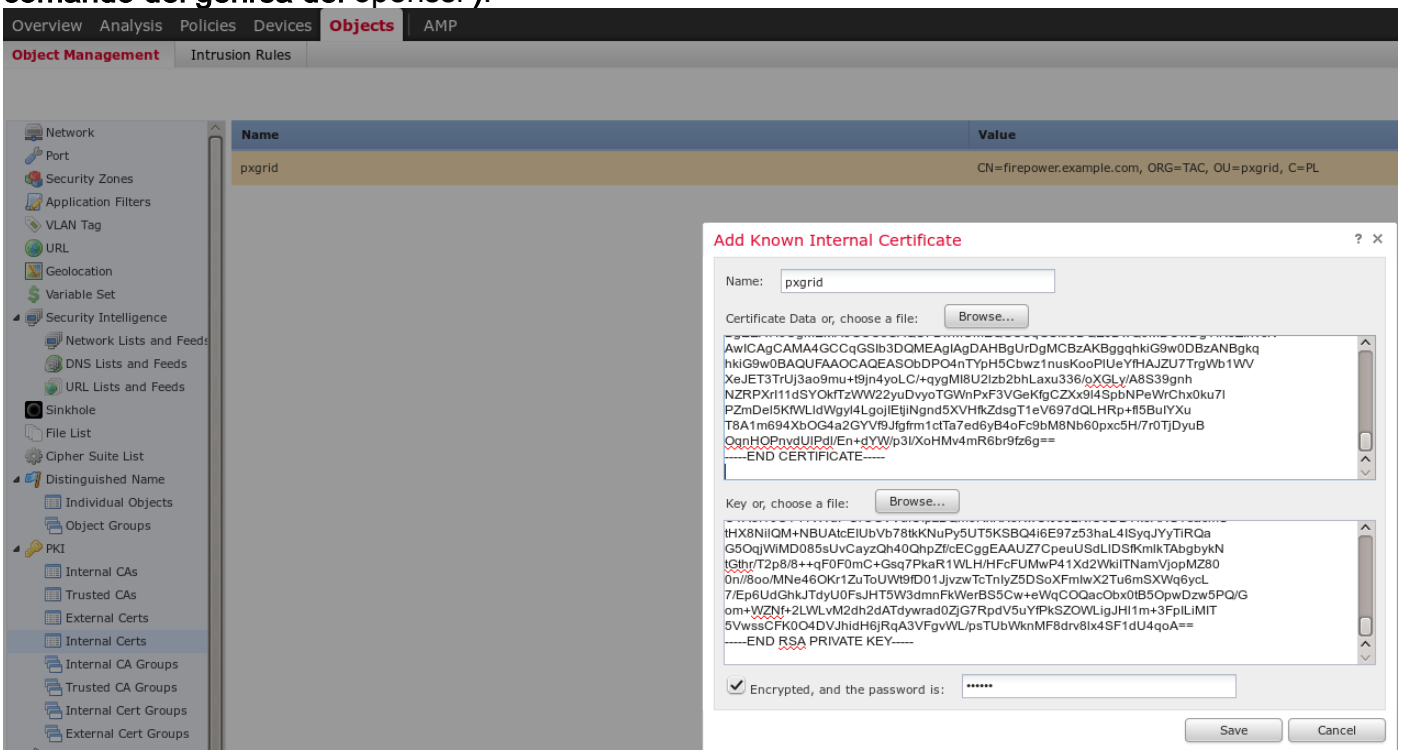


El certificado de CA necesita ser agregado a un almacén de confianza:

El paso más reciente es generar el certificado del pxGrid usado por FMC para autorizar al servicio del pxGrid ISE. Para generar CSR CLI necesita ser utilizada (o cualquier otra máquina externa con la herramienta del openssl).

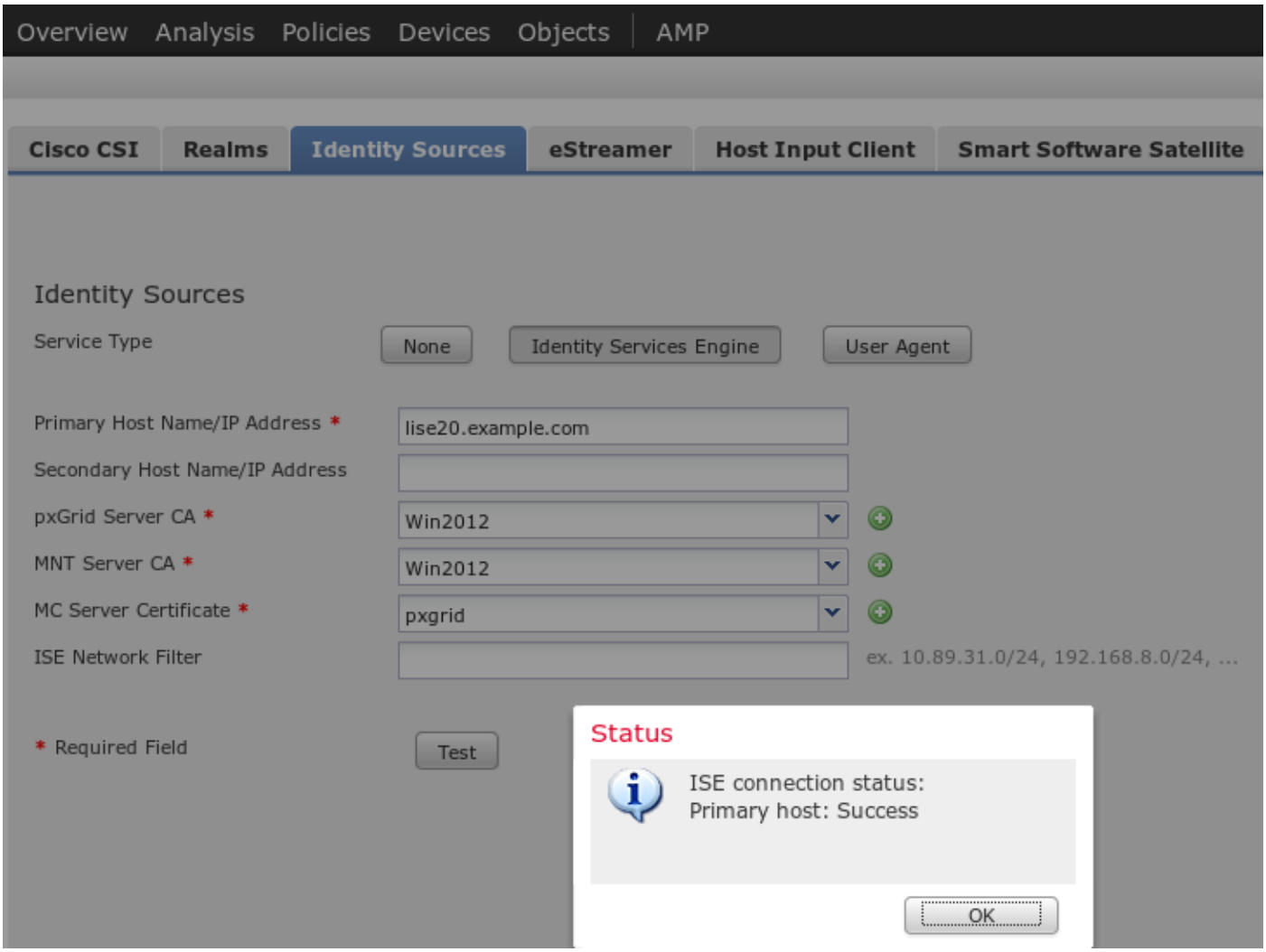
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#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

Fire.csr una vez generados, la firman usando Microsoft CA (plantilla del pxGrid). Importe detrás la clave privada (fire.key) y el certificado firmado (fire.pem) al almacén de certificados interno FMC. Para la clave privada utilice la contraseña configurada durante la generación de la clave (**comando del genrsa del** openssl):



Integración ISE

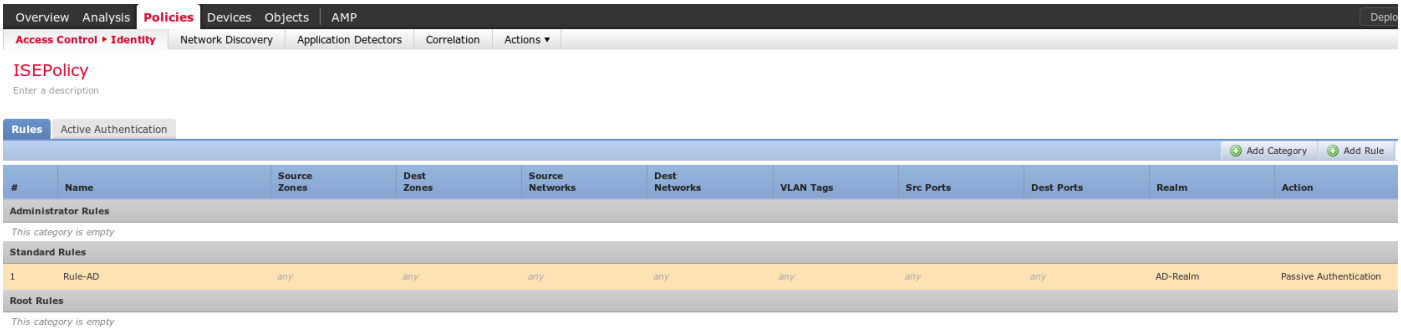
Una vez que todos los Certificados son integración instalada de la configuración ISE del **sistema > de la integración**:



Utilice CA importado para la validación de los Certificados del pxGrid y de los servicios MNT. Para la consola de administración (MC) utilice el certificado interno generado para el pxGrid.

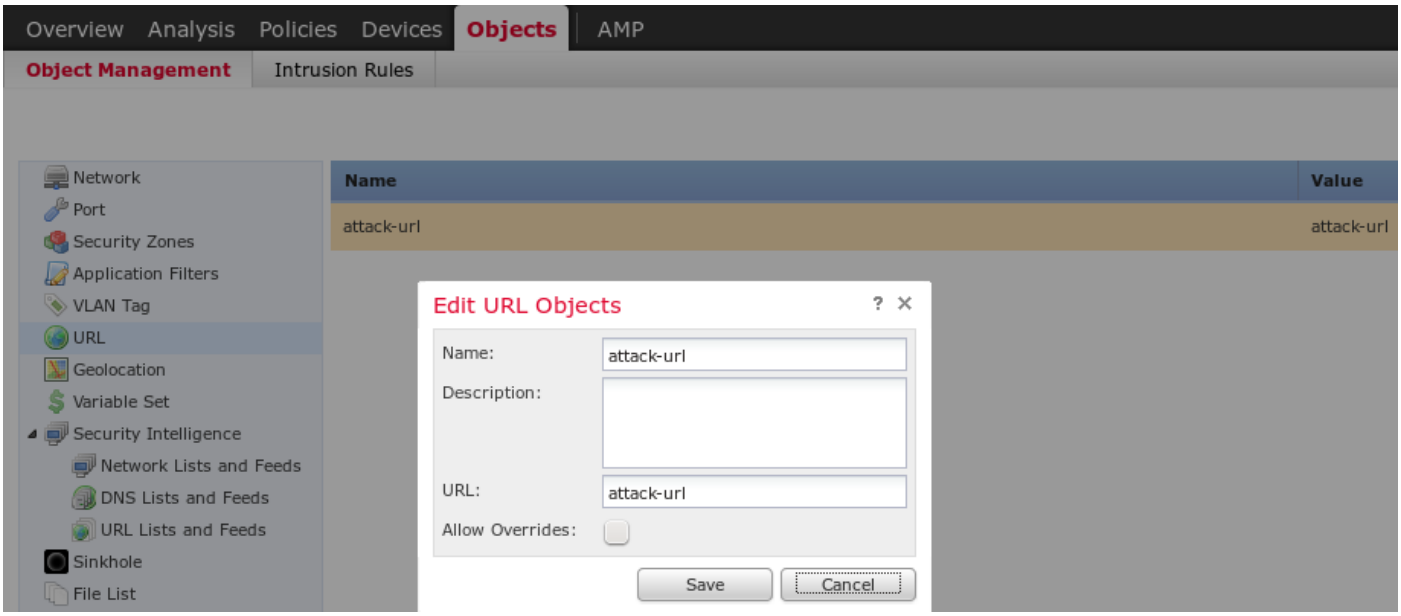
Directiva de la identidad

Configure la directiva de la identidad que está utilizando el reino previamente configurado AD para la autenticación pasiva:

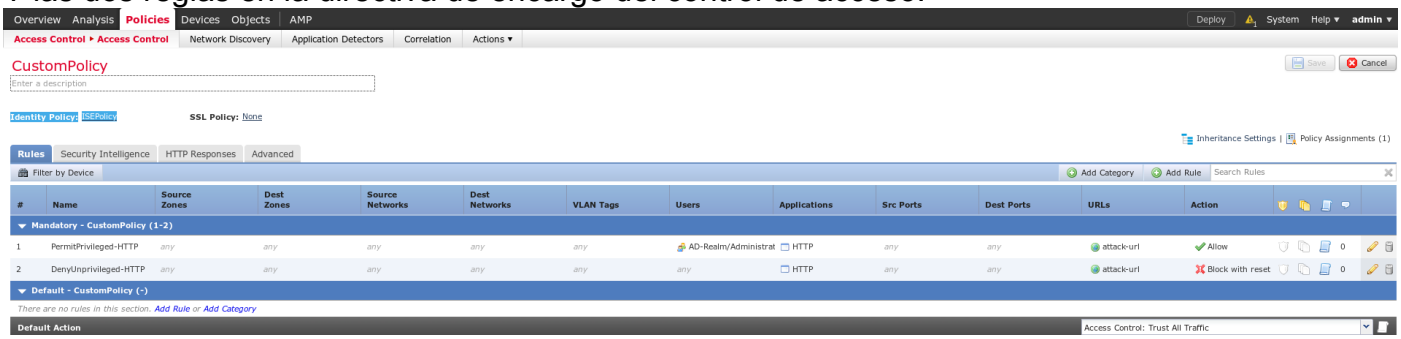


Directiva del control de acceso

Por este ejemplo se ha creado la aduana URL:



Y las dos reglas en la directiva de encargo del control de acceso:

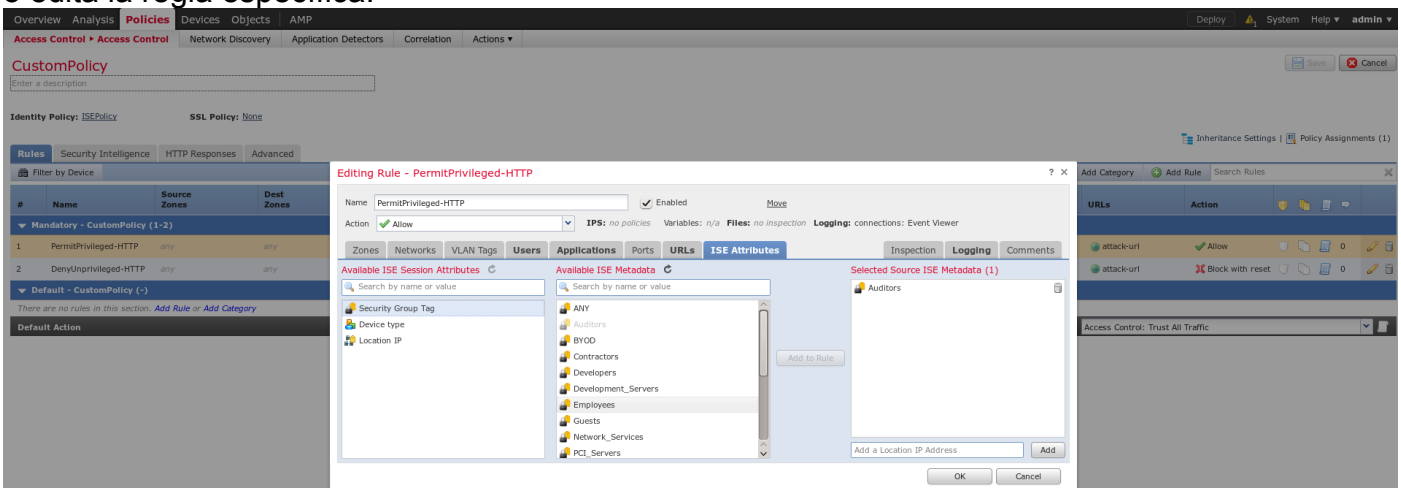


La regla PermitPrivileged-HTTP permite a todos los usuarios que pertenecen al grupo de los administradores AD que se han asignado la etiqueta SGT. Interventores para ejecutar el ataque HTTP en todas las blancos.

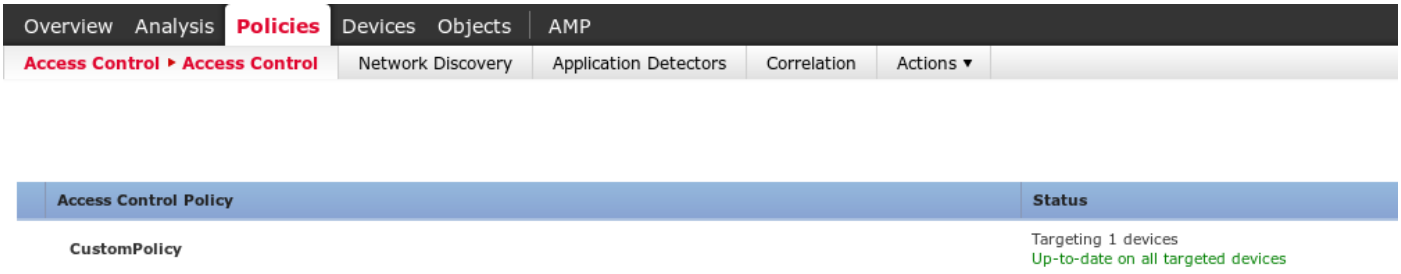
El DenyUnprivileged-HTTP niega esa acción al resto de los usuarios.

También note que la directiva previamente creada de la identidad se ha asignado a esta directiva del control de acceso.

En esta lengueta sus no posibles ver las etiquetas SGT, pero ésas son visibles mientras que crea o edita la regla específica:

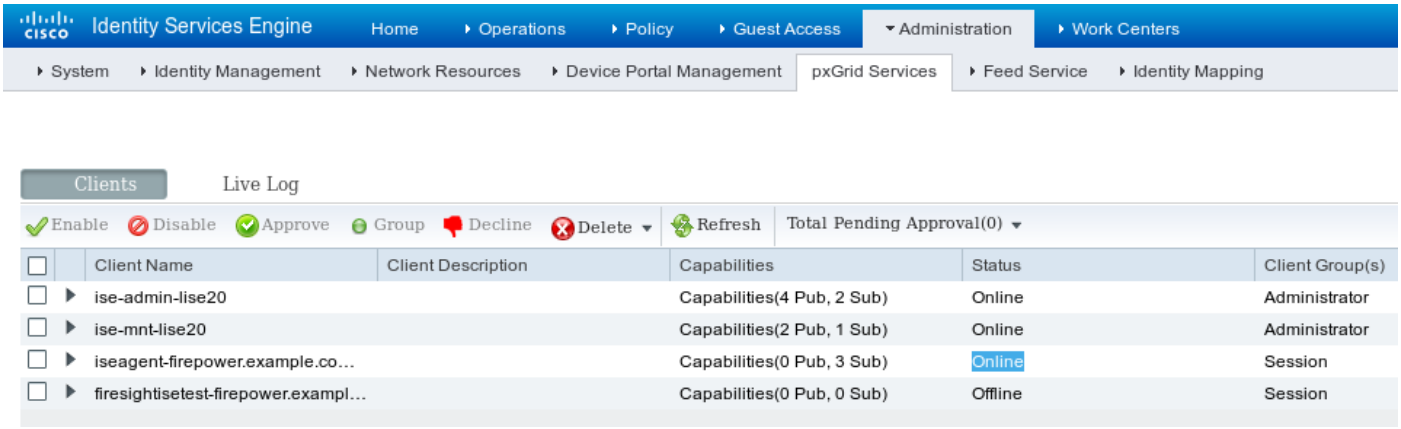


Asegúrese de que la directiva esté asignada al NGIPS y todos los cambios están desplegados:

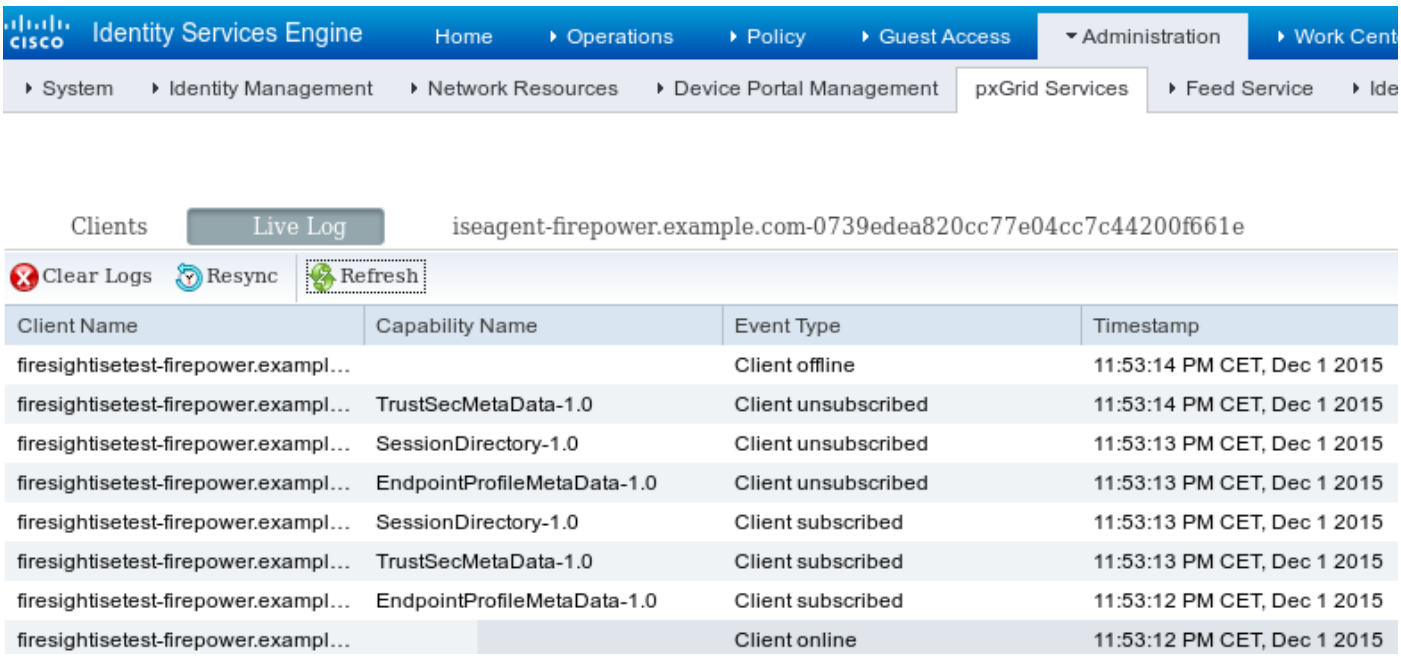


Verificación

Después de que todo se configure correctamente el ISE debe ver al cliente del pxGrid el inscribir para un servicio de sesión (Online del estatus).



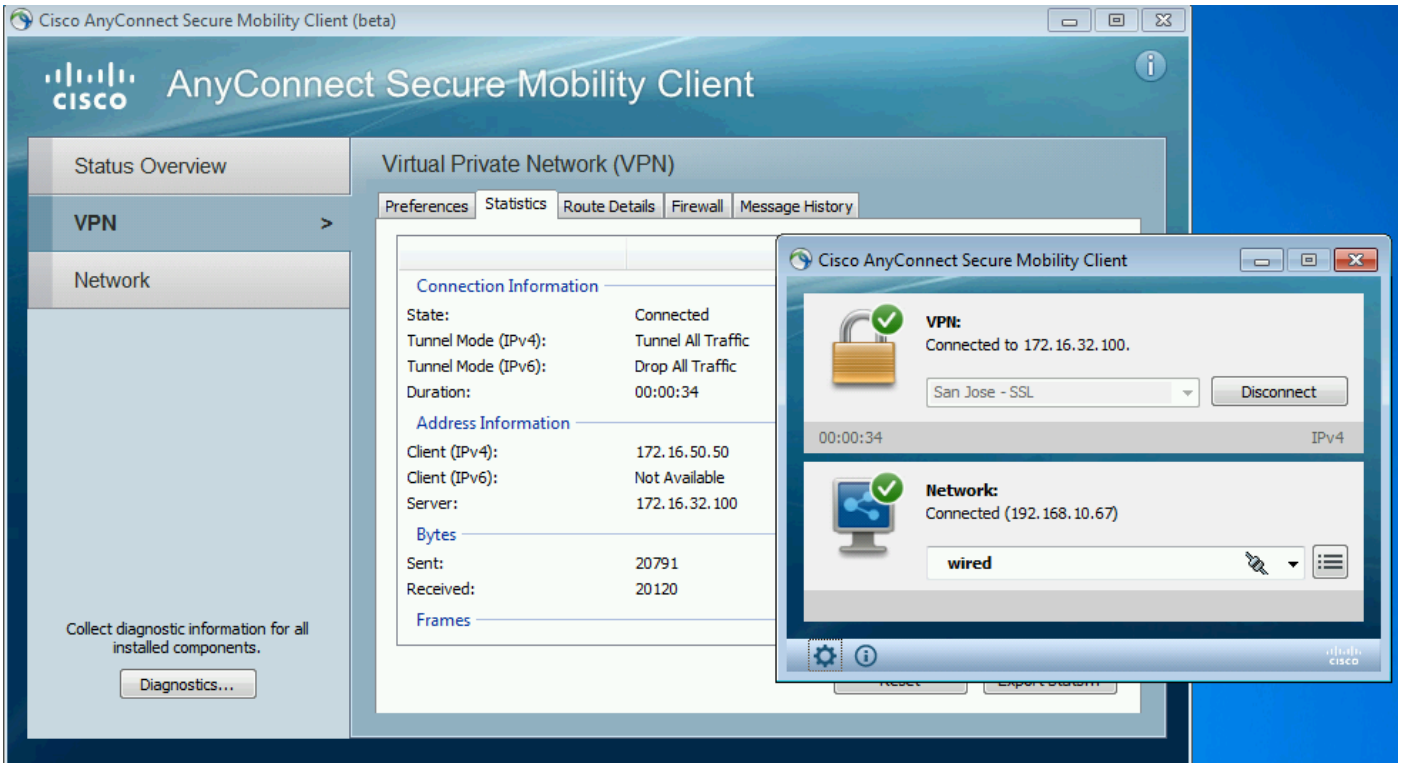
De los registros usted puede también confirmar que FMC ha inscrito para el servicio de TrustSecMetaData (etiquetas SGT) - consiguieron todas las etiquetas y desinscribieron.



Establecimiento de la sesión de VPN

La primera prueba se realiza para un escenario cuando la autorización en el ISE no vuelve la etiqueta correcta SGT (NGIPS no permite las pruebas de auditoría).

Una vez que la sesión de VPN está ENCIMA de la interfaz de usuario de AnyConnect (UI) puede proporcionar más detalles:



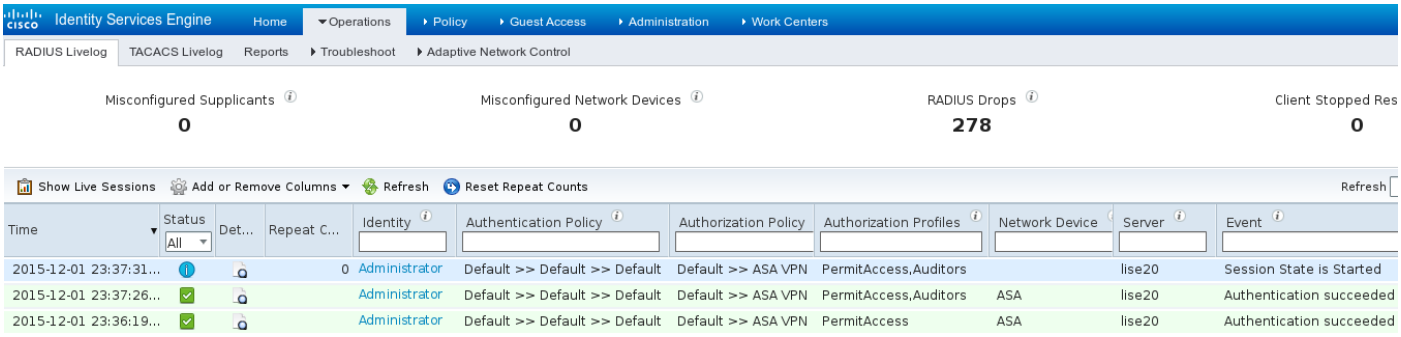
Se establece el ASA puede confirmar la sesión:

```
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
```

Note por favor que el ASA ve cualquier etiqueta SGT vuelta para esta autenticación. El ASA no se configura para TrustSec - para saltar la información de todos modos.

El ISE está también señalando la autorización exitosa (el registro en 23:36:19) - ninguna etiqueta SGT vuelta:



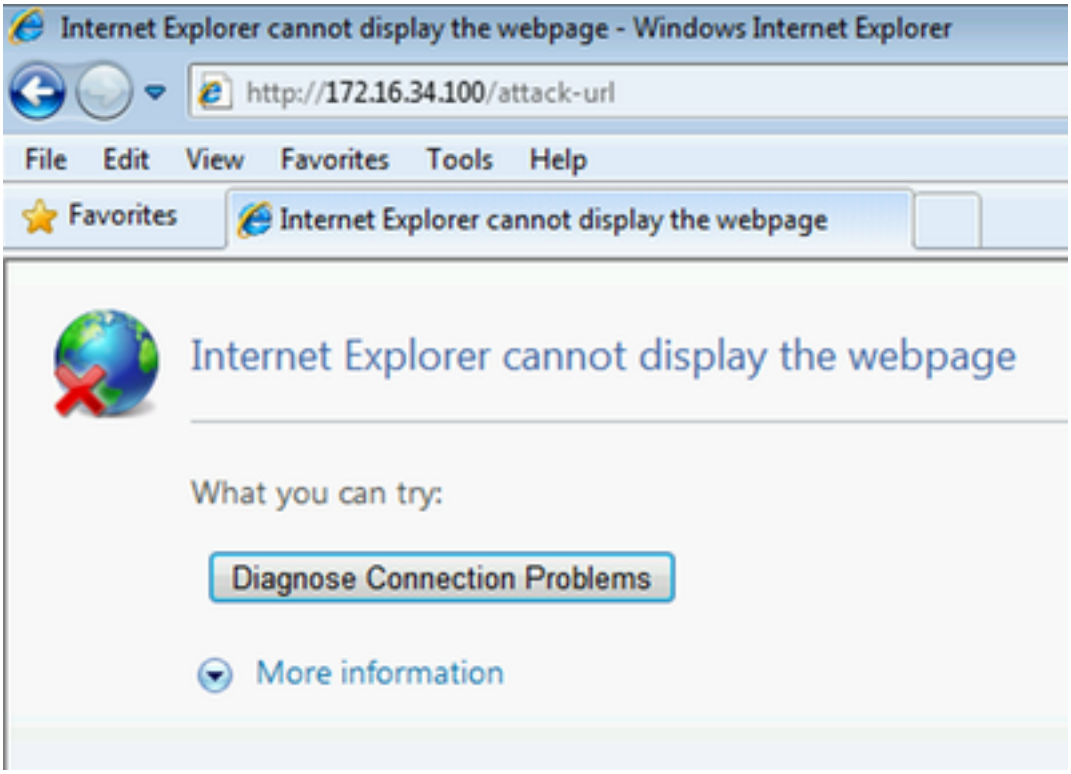
FMC que consigue los datos de la sesión del MNT

En esa etapa FMC en /var/log/messages señala una nueva sesión (recibida como suscriptor para el servicio del pxGrid) para las operaciones de búsqueda del nombre de usuario del administrador y del peform AD para la membresía del grupo:

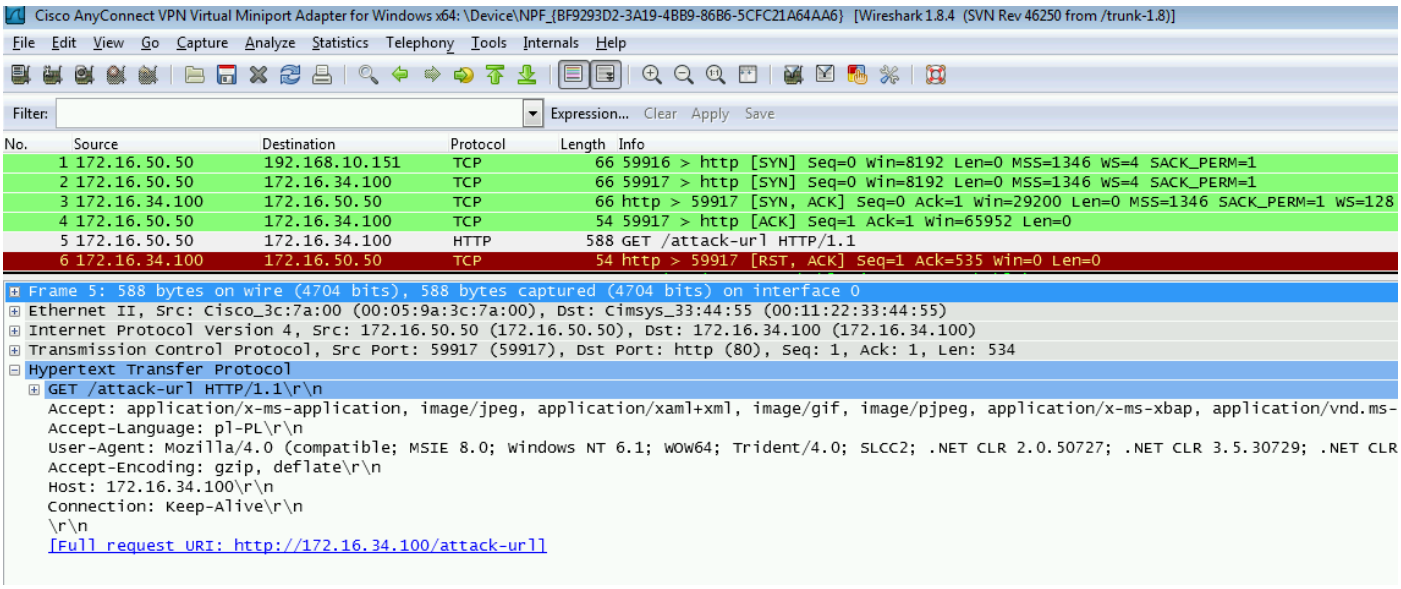
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

Acceso a la red no privilegiado y privilegiado

Cuando en los intentos de ese usuario de la etapa para abrir al buscador Web y a accederlo auditoría el servidor, la conexión será terminada:



Puede ser confirmada por las capturas de paquetes tomadas del cliente (el TCP RST envía según la configuración FMC):

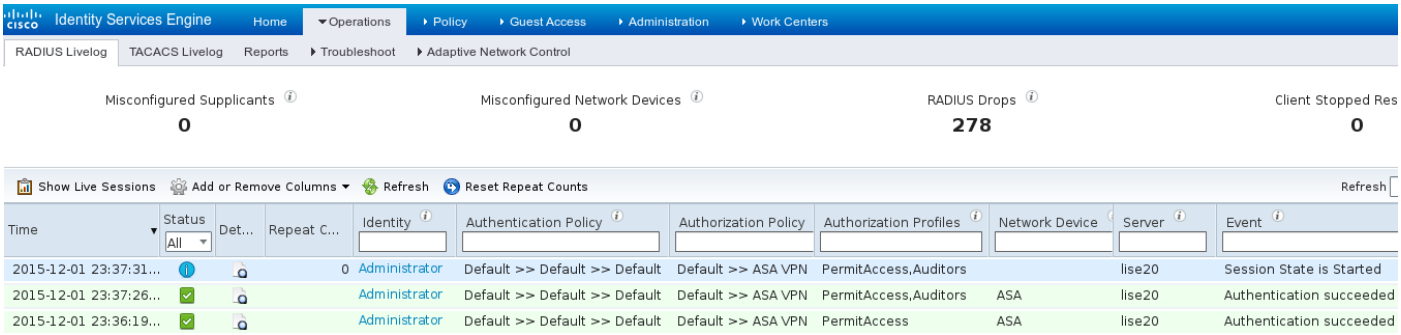


Una vez que el ISE se configura para volver, la sesión de la etiqueta ASA de la auditoría señala:

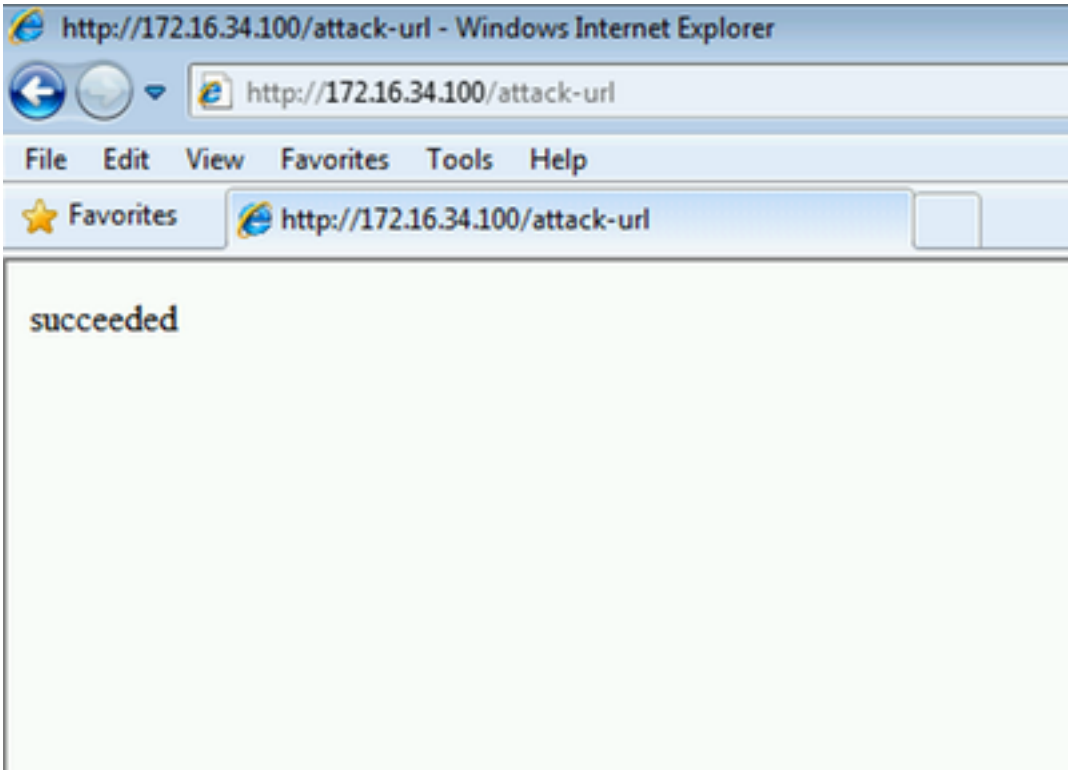
```
asav# show vpn-sessiondb anyconnect

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`

Se vuelve el ISE es también señala a un interventor de la etiqueta de la autorización exitosa (el registro en 23:37:26) - SGT:

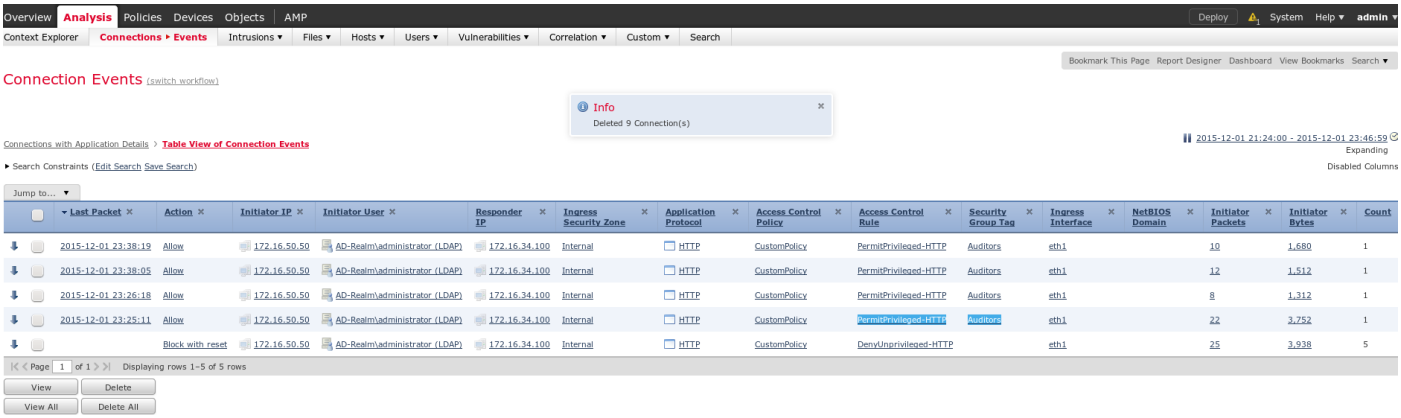


Y el usuario puede acceder el servicio mencionado:



Acceso del registro FMC

Esta actividad se puede confirmar por el informe del evento de conexión:



Primero, el usuario no hizo ninguna etiqueta SGT asignar y golpeaba la regla DenyUnprivileged-HTTP. Una vez que la etiqueta del interventor ha sido asignada por la regla ISE (y extraída por FMC), se utiliza el PermitPrivileged-HTTP y se permite el acceso.

También note eso para tener la visualización, se han quitado las columnas múltiples porque normalmente se visualizan la regla del control de acceso y la etiqueta del grupo de seguridad mientras que una de las columnas más recientes (y de la barra de desplazamiento horizontal necesita ser utilizado). Que la visión personalizada se puede guardar y reutilizar en el futuro.

Troubleshooting

Debugs FMC

Para marcar los registros del componente adi responsables del control /var/log/messages de los

servicios de la identidad clasifían:

```
[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
```

Para conseguir más detallado lo hace el debug de es posible matar al proceso adi (de la raíz después del sudo) y ejecutarlo con el argumento del debug:

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

Interrogación SGT vía el pxGrid

Se ejecuta la operación cuando el **botón Test Button** se hace clic en la **sección de integración ISE** o cuando se restaura la lista SGT, mientras que agrega la regla en la directiva del control de acceso.

```
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.ISEConnection [DEBUG]
adi.cpp:319:HandleLog(): Querying Security Group metaData...
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): pxgrid_connection_query(connection*:0x10c7da0, capability: 0x1064510,
request:<getSecurityGroupListRequest xmlns='http://www.cisco.com/pxgrid/identity'/>)...
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK|<ns5:getSecurityGroupListResponse
xmlns:ns2='http://www.cisco.com/pxgrid' xmlns:ns3='http://www.cisco.com/pxgrid/net'
xmlns:ns4='http://www.cisco.com/pxgrid/admin' xmlns:ns5='http://www.cisco.com/pxgrid/identity'
xmlns:ns6='http://www.cisco.com/pxgrid/eps' xmlns:ns7='http://www.cisco.com/pxgrid/netcap'
xmlns:ns8='http://www.cisco.com/pxgrid/anc'><ns5:SecurityGroups><ns5:SecurityGroup><ns5:id>fc6f9
470-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Unknown</ns5:name><ns5:description>Unknown
Security
Group</ns5:description><ns5:tag>0</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc7c8c
c0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>ANY</ns5:name><ns5:description>Any Security
Group</ns5:description><ns5:tag>65535</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc
f95de0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Auditors</ns5:name><ns5:description>Auditor
Security
Group</ns5:description><ns5:tag>9</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd14fc
30-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>BYOD</ns5:name><ns5:description>BYOD Security
Group</ns5:description><ns5:tag>15</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd2fb
020-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Contractors</ns5:name><ns5:description>Contractor Security
Group</ns5:description><ns5:tag>5</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd4e34
a0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Developers</ns5:name><ns5:description>Developer
Security
Group</ns5:description><ns5:tag>8</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd6d2e
50-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Development_Servers</ns5:name><ns5:description>Development
Servers Security
Group</ns5:description><ns5:tag>12</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fda10
f90-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Employees</ns5:name><ns5:description>Employee
Security
Group</ns5:description><ns5:tag>4</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdbcd4
f0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Guests</ns5:name><ns5:description>Guest
Security
Group</ns5:description><ns5:tag>6</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdd9ab
c0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Network_Services</ns5:name><ns5:description>Network Services
Security
Group</ns5:description><ns5:tag>3</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdf4d4
e0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>PCI_Servers</ns5:name><ns5:description>PCI
Servers Security
Group</ns5:description><ns5:tag>14</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe11a
bb0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Point_of_Sale_Systems</ns5:name><ns5:description>Point of Sale
Security
Group</ns5:description><ns5:tag>10</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe2d2
2f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Servers</ns5:name><ns5:description>Production Servers
Security
Group</ns5:description><ns5:tag>11</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe487
320-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Users</ns5:name><ns5:description>Production User
Security
Group</ns5:description><ns5:tag>7</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe62d8
f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Quarantined_Systems</ns5:name><ns5:description>Quarantine
```

Security
Group</ns5:description><ns5:tag>255</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe7d
3ec0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Test_Servers</ns5:name><ns5:description>Test
Servers Security
Group</ns5:description><ns5:tag>13</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe99c
770-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>TrustSec_Devices</ns5:name><ns5:description>TrustSec Devices
Security
Group</ns5:description><ns5:tag>2</ns5:tag></ns5:SecurityGroup></ns5:SecurityGroups></ns5:getSec
urityGroupListResponse>]

Para un mejor xml de la visión un contenido de ese registro se puede copiar al archivo del xml y abrir por un buscador Web. Usted puede confirmar que se está recibiendo SGT específico (auditoría) así como el resto del SGT se está definiendo en el ISE:

−<ns5:getSecurityGroupListResponse>
−<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>

Interrogación de la sesión vía el RESTO API al MNT

Eso es también una probar la operación de la parte de (note por favor que ese nombre de host y puerto MNT está pasado vía el pxGrid). Se utiliza la descarga a granel de la sesión:

Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.ISEConnection [DEBUG]
adi.cpp:319:HandleLog(): **Querying Security Group metaData...**
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): **pxgrid_connection_query**(connection*:0x10c7da0, capability: 0x1064510,
request:<getSecurityGroupListRequest xmlns='http://www.cisco.com/pxgrid/identity'/>)...
Dec 01 23:14:38 firepower SF-IMS[24106]: [24139] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK|<ns5:getSecurityGroupListResponse
xmlns:ns2='http://www.cisco.com/pxgrid' xmlns:ns3='http://www.cisco.com/pxgrid/net'
xmlns:ns4='http://www.cisco.com/pxgrid/admin' xmlns:ns5='http://www.cisco.com/pxgrid/identity'
xmlns:ns6='http://www.cisco.com/pxgrid/eps' xmlns:ns7='http://www.cisco.com/pxgrid/netcap'
xmlns:ns8='http://www.cisco.com/pxgrid/anc'><ns5:SecurityGroups><ns5:SecurityGroup><ns5:id>fc6f9
470-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Unknown</ns5:name><ns5:description>Unknown
Security
Group</ns5:description><ns5:tag>0</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc7c8c
c0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>ANY</ns5:name><ns5:description>Any Security
Group</ns5:description><ns5:tag>65535</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fc
f95de0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Auditors</ns5:name><ns5:description>Auditor
Security
Group</ns5:description><ns5:tag>9</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd14fc
30-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>BYOD</ns5:name><ns5:description>BYOD Security
Group</ns5:description><ns5:tag>15</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd2fb
020-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Contractors</ns5:name><ns5:description>Contractor Security
Group</ns5:description><ns5:tag>5</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd4e34
a0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Developers</ns5:name><ns5:description>Developer
Security
Group</ns5:description><ns5:tag>8</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fd6d2e
50-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Development_Servers</ns5:name><ns5:description>Development
Servers Security
Group</ns5:description><ns5:tag>12</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fda10
f90-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Employees</ns5:name><ns5:description>Employee
Security
Group</ns5:description><ns5:tag>4</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdbcd4
f0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Guests</ns5:name><ns5:description>Guest
Security
Group</ns5:description><ns5:tag>6</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdd9ab
c0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Network_Services</ns5:name><ns5:description>Network Services
Security
Group</ns5:description><ns5:tag>3</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fdf4d4
e0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>PCI_Servers</ns5:name><ns5:description>PCI
Servers Security
Group</ns5:description><ns5:tag>14</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe11a
bb0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Point_of_Sale_Systems</ns5:name><ns5:description>Point of Sale
Security
Group</ns5:description><ns5:tag>10</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe2d2
2f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Servers</ns5:name><ns5:description>Production Servers
Security
Group</ns5:description><ns5:tag>11</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe487
320-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Production_Users</ns5:name><ns5:description>Production User
Security
Group</ns5:description><ns5:tag>7</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe62d8
f0-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>Quarantined_Systems</ns5:name><ns5:description>Quarantine
Security
Group</ns5:description><ns5:tag>255</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe7d
3ec0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Test_Servers</ns5:name><ns5:description>Test
Servers Security

```
Group</ns5:description><ns5:tag>13</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe99c
770-6d8f-11e5-978e-
005056bf2f0a</ns5:id><ns5:name>TrustSec_Devices</ns5:name><ns5:description>TrustSec Devices
Security
Group</ns5:description><ns5:tag>2</ns5:tag></ns5:SecurityGroup></ns5:SecurityGroups></ns5:getSec
urityGroupListResponse>]
```

Y resultado analizado (1 sesión activa recibida):

```
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}
```

En esa etapa NGIPS es intentos para correlacionar ese nombre de usuario (y el dominio) con el nombre de usuario Reino-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
```

El LDAP se utiliza para encontrar un usuario y una membresía del grupo:

```
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.
```

Debugs ISE

Después de habilitar el debug del nivel de traza para el componente del pxGrid su posible marcar cada operación (pero sin el payload/los datos tenga gusto en FMC).

Ejemplo con la extracción de la etiqueta 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
```

Bug

CSCuv32295 - El ISE puede enviar la información sobre el dominio en los campos de nombre de usuario

CSCus53796 - Incapaz de conseguir el FQDN del host para la interrogación del bulto del RESTO

CSCuv43145 - PXGRID y reinicio del servicio de la asignación de la identidad, importación/cancelación del almacén de la confianza

Referencias

- Servicios de la corrección de la configuración con la integración ISE y de FirePOWER
- Configurar el pxGrid en un entorno distribuido ISE
- Cómo que despliega los Certificados con el pxGrid de Cisco: Configurar el nodo CA-firmado del pxGrid ISE y al cliente CA-firmado del pxGrid
- Integración del pxGrid de la versión 1.3 ISE con la aplicación del pxLog IPS
- Guía del administrador del Cisco Identity Services Engine, versión 2.0
- Guía de referencia del Cisco Identity Services Engine API, versión 1.2 – Introducción a S relajante externo…
- Guía de referencia del Cisco Identity Services Engine API, versión 1.2 – Introducción a la RES de la supervisión…
- Guía del administrador del Cisco Identity Services Engine, versión 1.3
- Soporte Técnico y Documentación - Cisco Systems