Pesquise defeitos o ISE e a integração de FirePOWER para serviços da identidade

Índice

Introdução

Este documento descreve como configurar e pesquisar defeitos políticas cientes de TrustSec no sistema da prevenção de intrusão da próxima geração de Cisco (NGIPS). A versão 6.0 NGIPS apoia a integração com o Identity Services Engine (ISE) que reserva construir políticas cientes baseadas identidade.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN adaptável da ferramenta de segurança de Cisco (ASA)
- Configuração de Cliente de mobilidade Cisco AnyConnect Secure
- Configuração básica do centro de gerenciamento de Cisco FirePOWER
- Configuração de Cisco ISE
- Soluções de Cisco TrustSec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Certificate Authority (CA) de Microsoft Windows 2012
- Versão ASA 9.3 de Cisco
- Versões de software 1.4 de Cisco ISE
- Versões 4.2 do Cliente de mobilidade Cisco AnyConnect Secure
- Versão 6.0 do centro de gerenciamento de Cisco FirePOWER (FMC)
- Versão 6.0 de Cisco FirePOWER NGIPS

Configurar

O centro de gerenciamento de FirePOWER (FMC) é a plataforma de gerenciamento para FirePOWER. Há dois tipos de funcionalidades relativas à integração ISE:

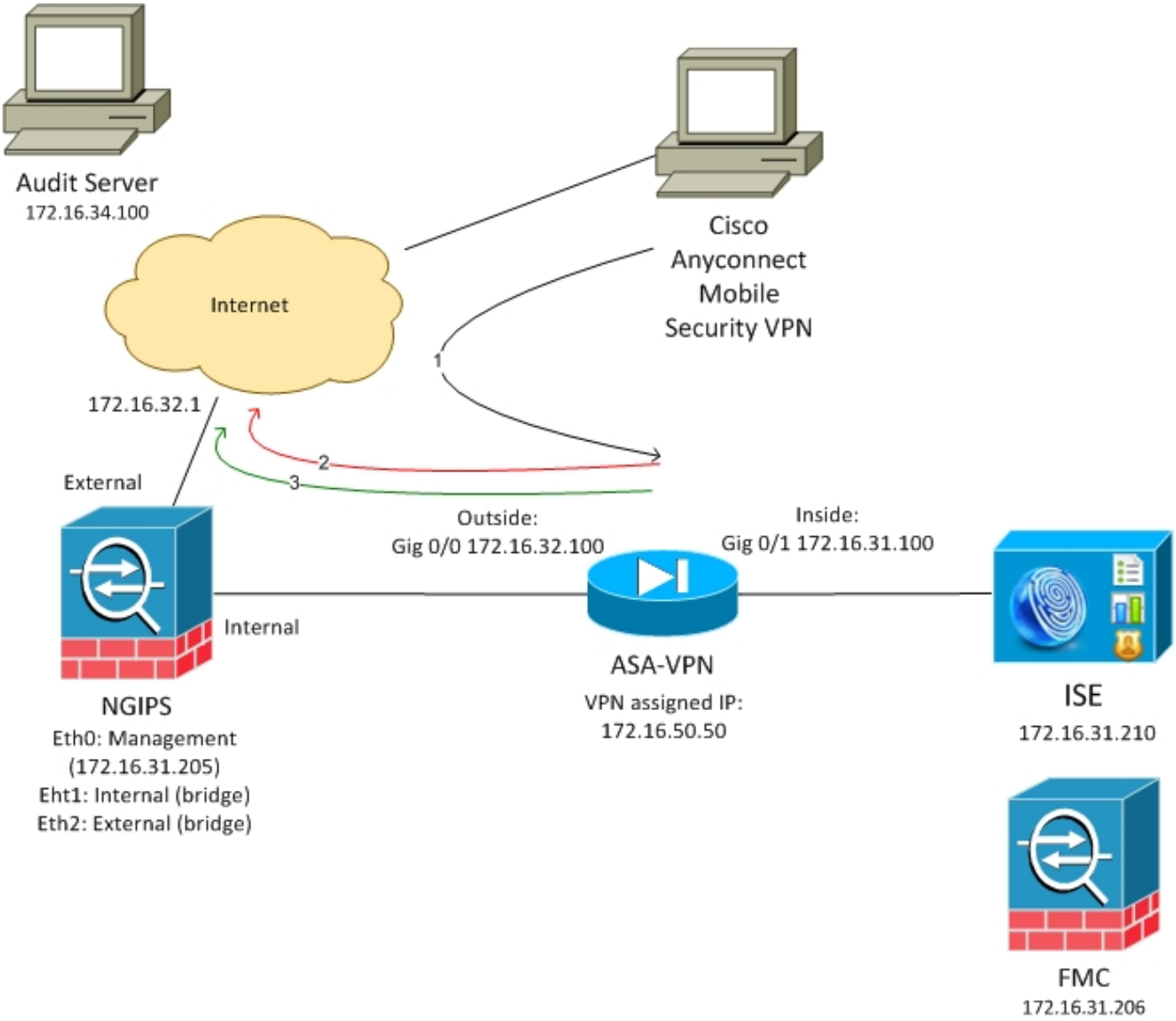
- Remediação - permite que FMC quarantine o atacante através do ISE, que está mudando dinamicamente o estado de autorização no dispositivo de acesso que fornece acesso de rede limitado. Há duas gerações desta solução:

1. Script Perl do legado usando o atendimento do serviço de proteção do valor-limite (EP) API ao ISE.
2. Módulo mais novo usando o atendimento do protocolo do pxGrid ao ISE (este módulo é apoiado somente na versão 5.4 - não apoiada em 6.0, suporte nativo de planeamento em 6.1).

- Política - permite que FMC configure as políticas baseadas nas etiquetas do grupo de segurança de TrustSec (SGT).

Este artigo centra-se sobre a segunda funcionalidade. Para a remediação o exemplo leu por favor a seção de referências

Diagrama de Rede



FMC é configurado com a política do controle de acesso que contém duas regras:

- Negue para o tráfego de HTTP com costume URL (a ataque-URL)
- Permita o tráfego de HTTP com costume URL (ataque-URL) mas somente se o usuário está atribuído para examinar (9) a etiqueta SGT pelo ISE

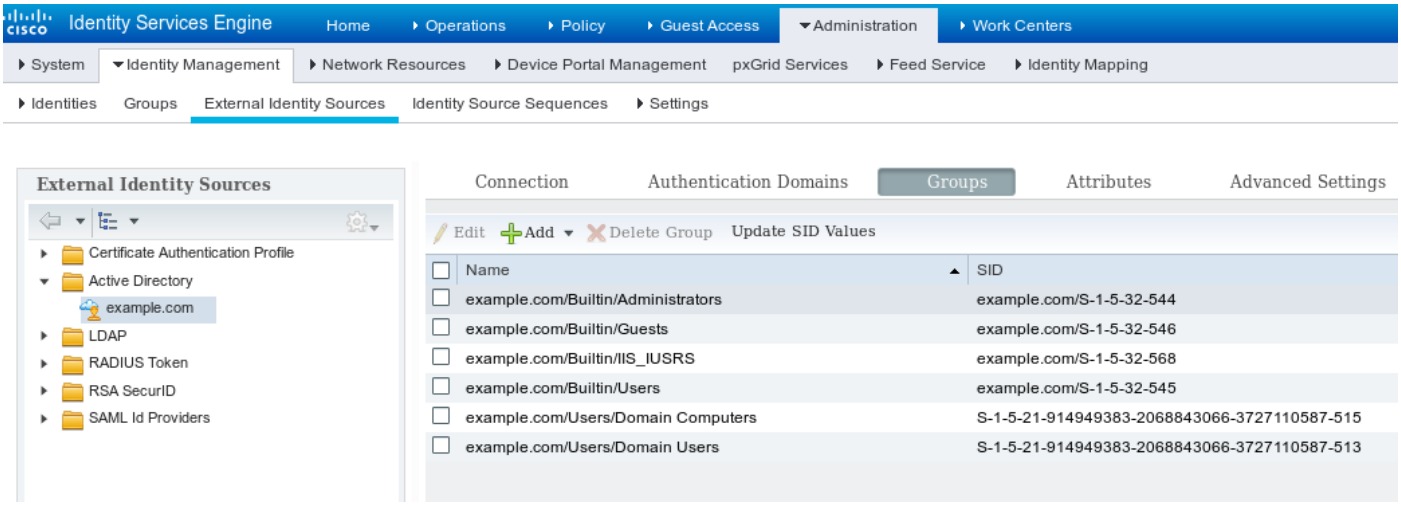
O ISE decide atribuir a etiqueta da auditoria a todos os usuários de diretório ativo que pertence ao grupo de administrador e usa o dispositivo ASA-VPN para o acesso de rede.

Rede dos acessos de usuário através da conexão de VPN no ASA. O usuário tenta então alcançar o server examinado usando URL ataque-URL - mas falha porque não foi atribuído para examinar o grupo SGT. Uma vez que isso é fixo, a conexão é bem sucedida.

ISE

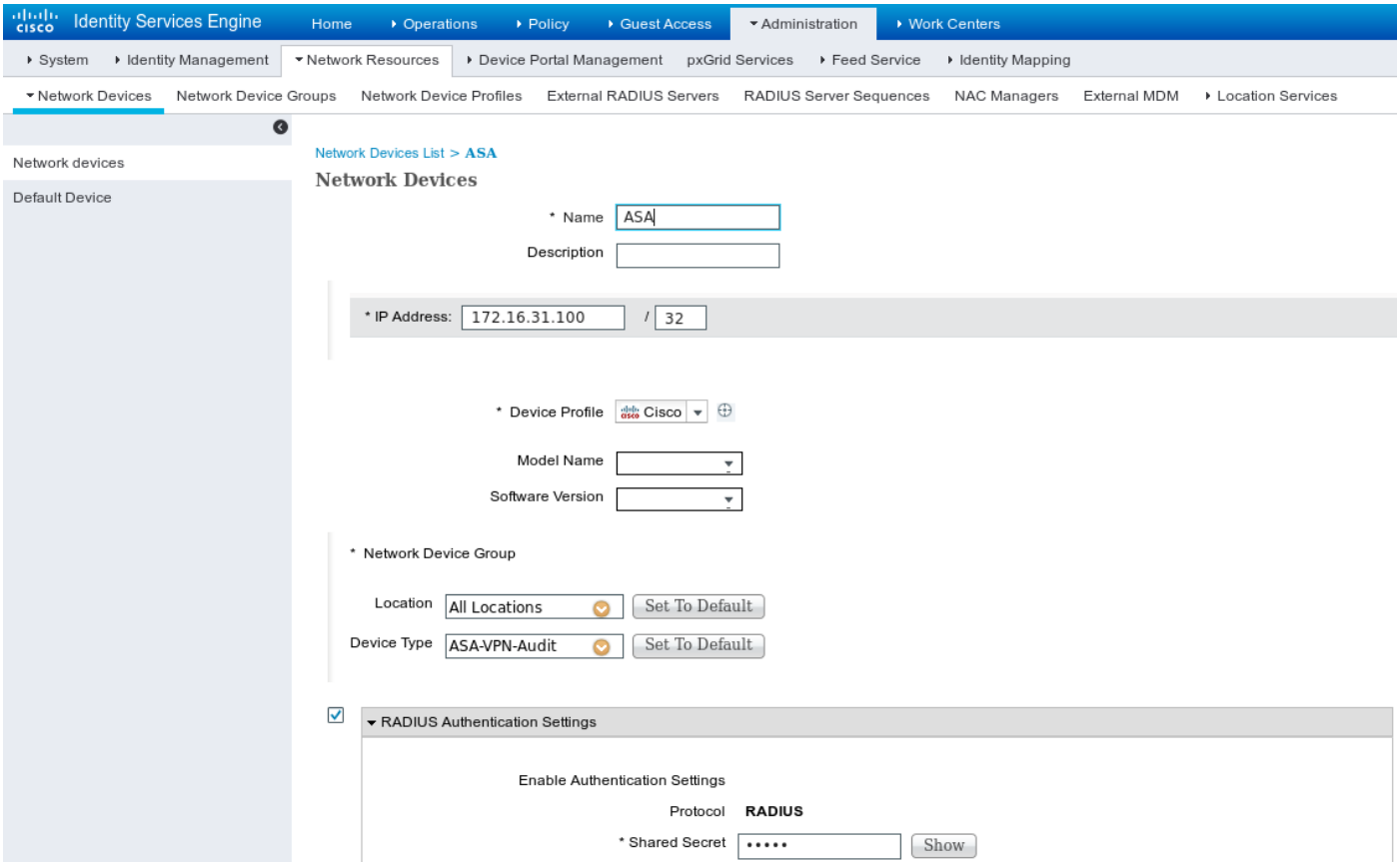
Diretório ativo

A integração AD deve ser configurada e os grupos corretos devem ser buscados (o grupo dos administradores é usado para a condição da regra da autorização):



Dispositivo do acesso de rede

O ASA é adicionado como um dispositivo de rede. A ASA-VPN-auditoria feita sob encomenda do grupo é usada, segundo as indicações desta imagem:



Certificados para o pxGrid e o MNT

FMC usa ambos os serviços no ISE:

- pxGrid para SGT e perfilamento da pergunta dos dados
- Monitoração e relatório (MNT) para a transferência maioria da sessão

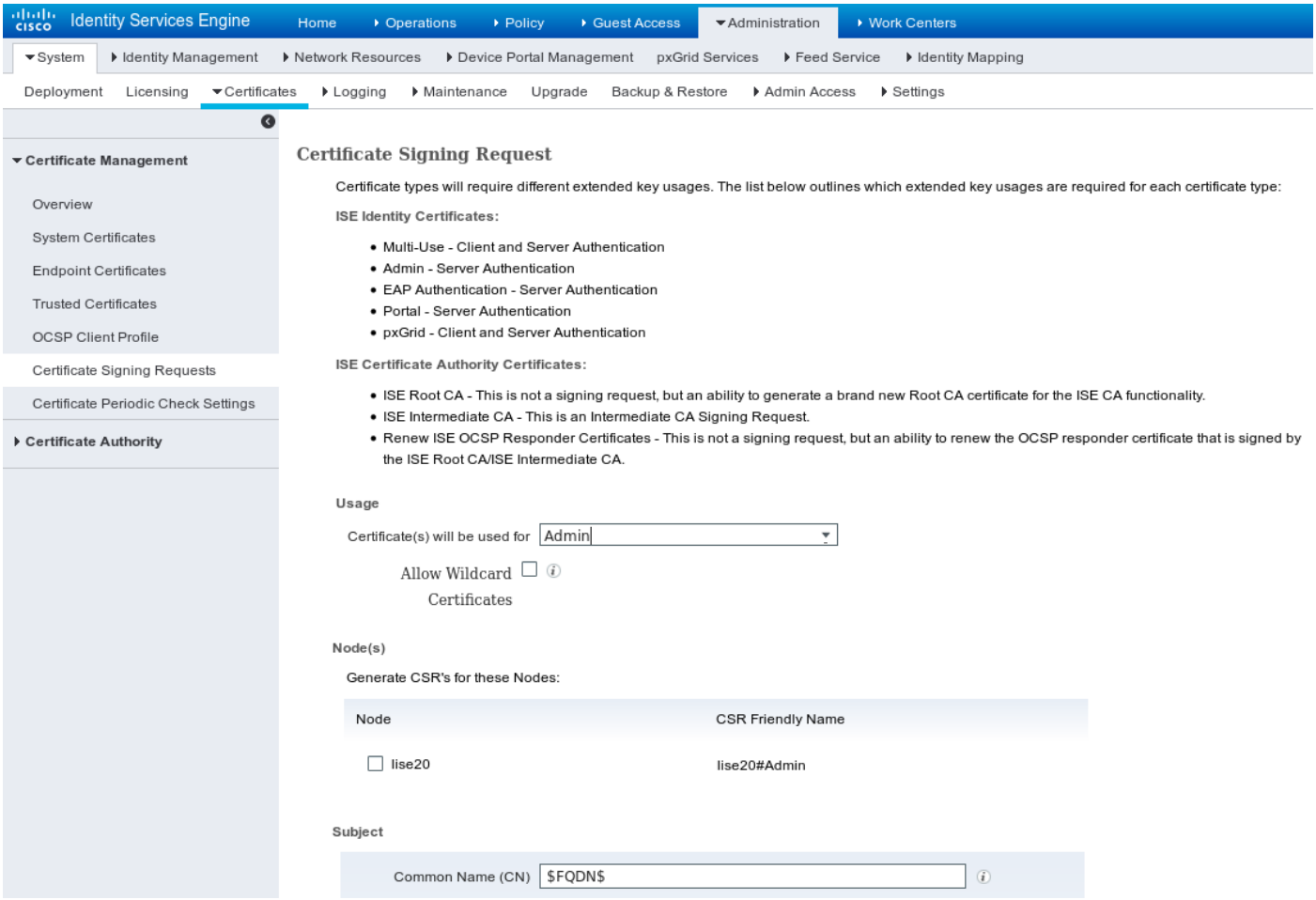
A Disponibilidade MNT é muito importante desde que esta maneira FMC está sendo informada o que é o endereço IP de Um ou Mais Servidores Cisco ICM NT da sessão autenticada, também seu username e etiqueta SGT. Baseado nisso, as políticas corretas podem ser aplicadas.

Observe por favor que NGIPS não apoia nativamente etiquetas SGT (inline colocação de etiquetas) como o ASA. Mas no contrário ao ASA, apoia nomes SGT em vez dos números somente.

Devido 2 aquelas exigências o ISE e FMC precisam de confiar-se serviço (certificado). O MNT usa apenas o certificado do lado de servidor, pxGrid usa ambo o certificado do lado do cliente e servidor.

Microsoft CA é usado para assinar todos os Certificados.

Para MNT (papel Admin) o ISE deve gerar a solicitação de assinatura de certificado (CSR), segundo as indicações desta imagem:



Após a assinatura por Microsoft CA deve ser importado através da opção do **certificado do ligamento**.

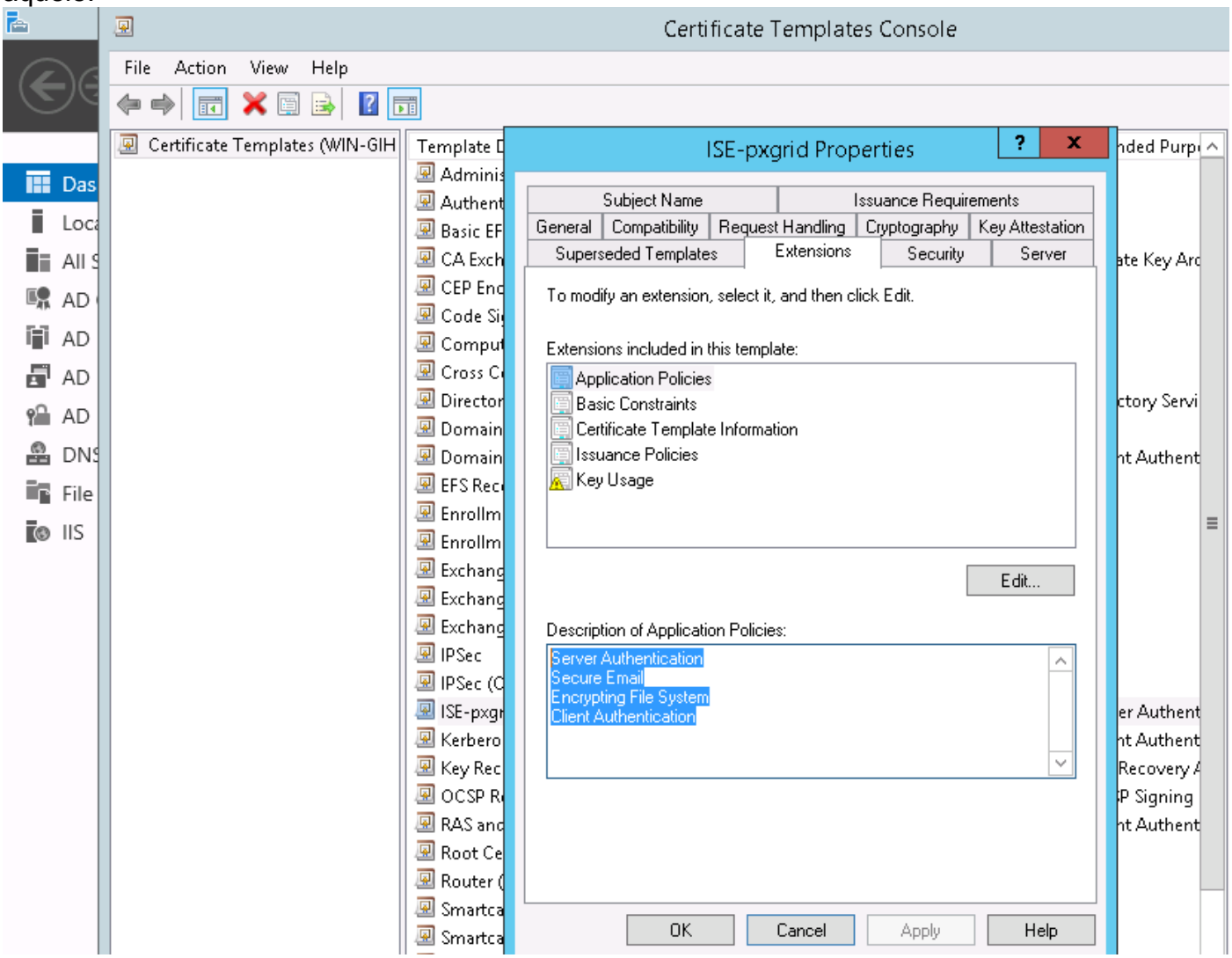
O processo similar deve ser seguido para o serviço do pxGrid. **Os certificados serão usados para a** opção devem ter o pxGrid selecionado.

Desde que não pode haver dois Certificados com nome do sujeito idêntico é inteiramente aceitável adicionar diferente avalia para OU ou seção O (por exemplo pxGrid).

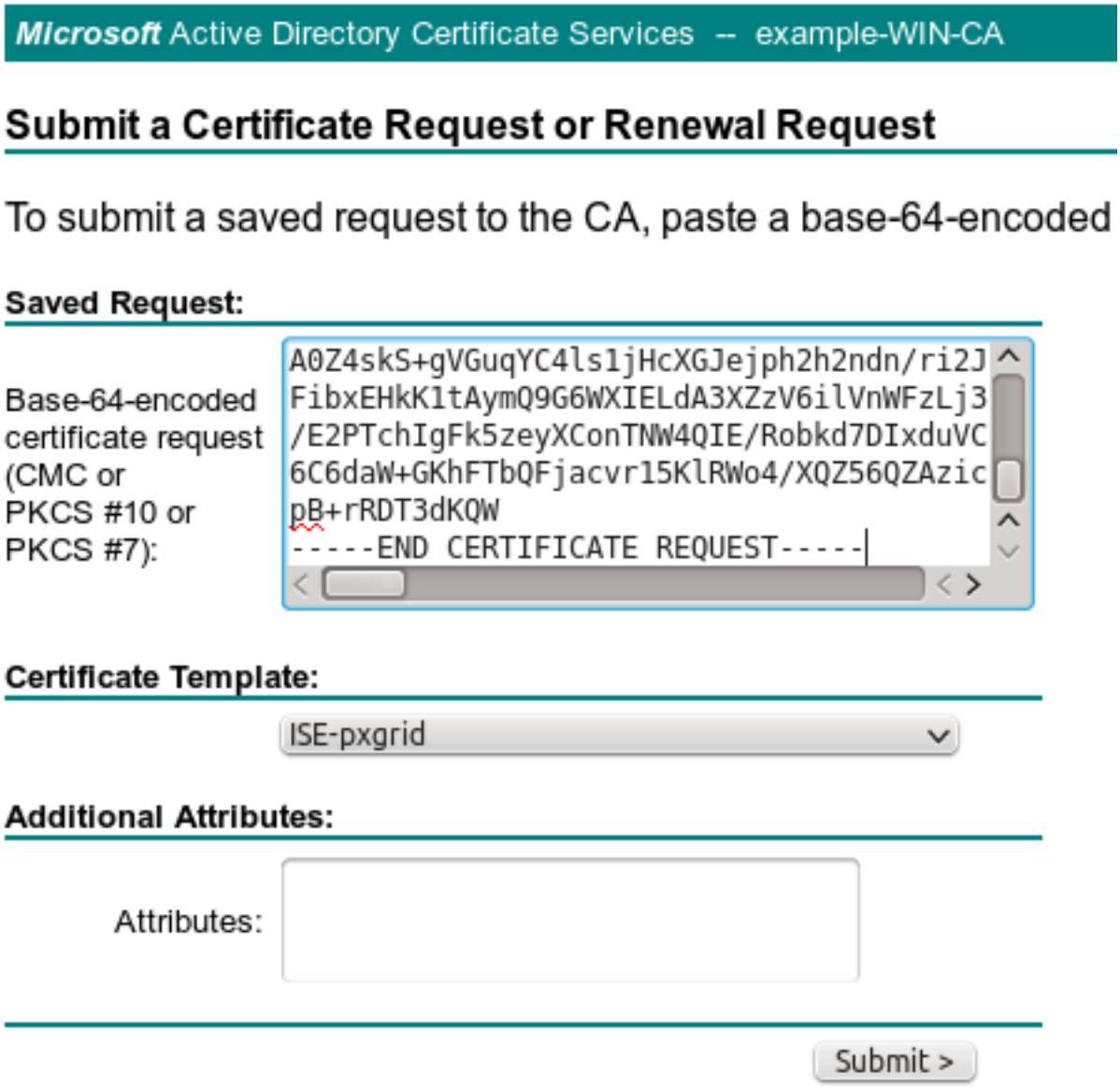
> **Note**: Certifique-se por favor de que para cada nome de domínio totalmente qualificado (FQDN) para o ISE e o FMC, o registro correto DNS está configurado no servidor DNS.

A única diferença entre o Admin e o certificado do pxGrid é com processo de assinatura. Desde que os Certificados do pxGrid devem ter estendido as opções de uso chaves para ambos molde personalizado da autenticação de cliente e servidor em Microsoft CA podem ser usadas para

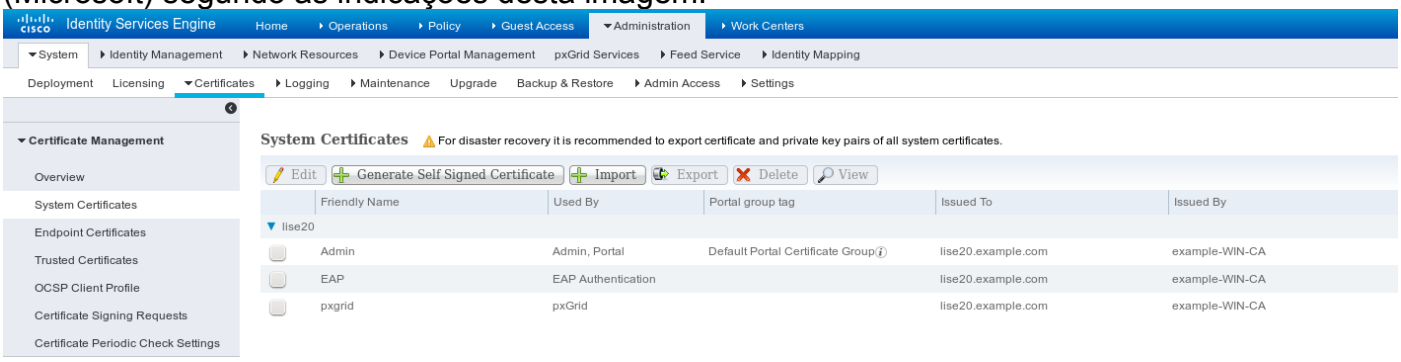
aquele:



Como usar o serviço de microsoft web para assinar o pxGrid CSR é mostrada nesta imagem:

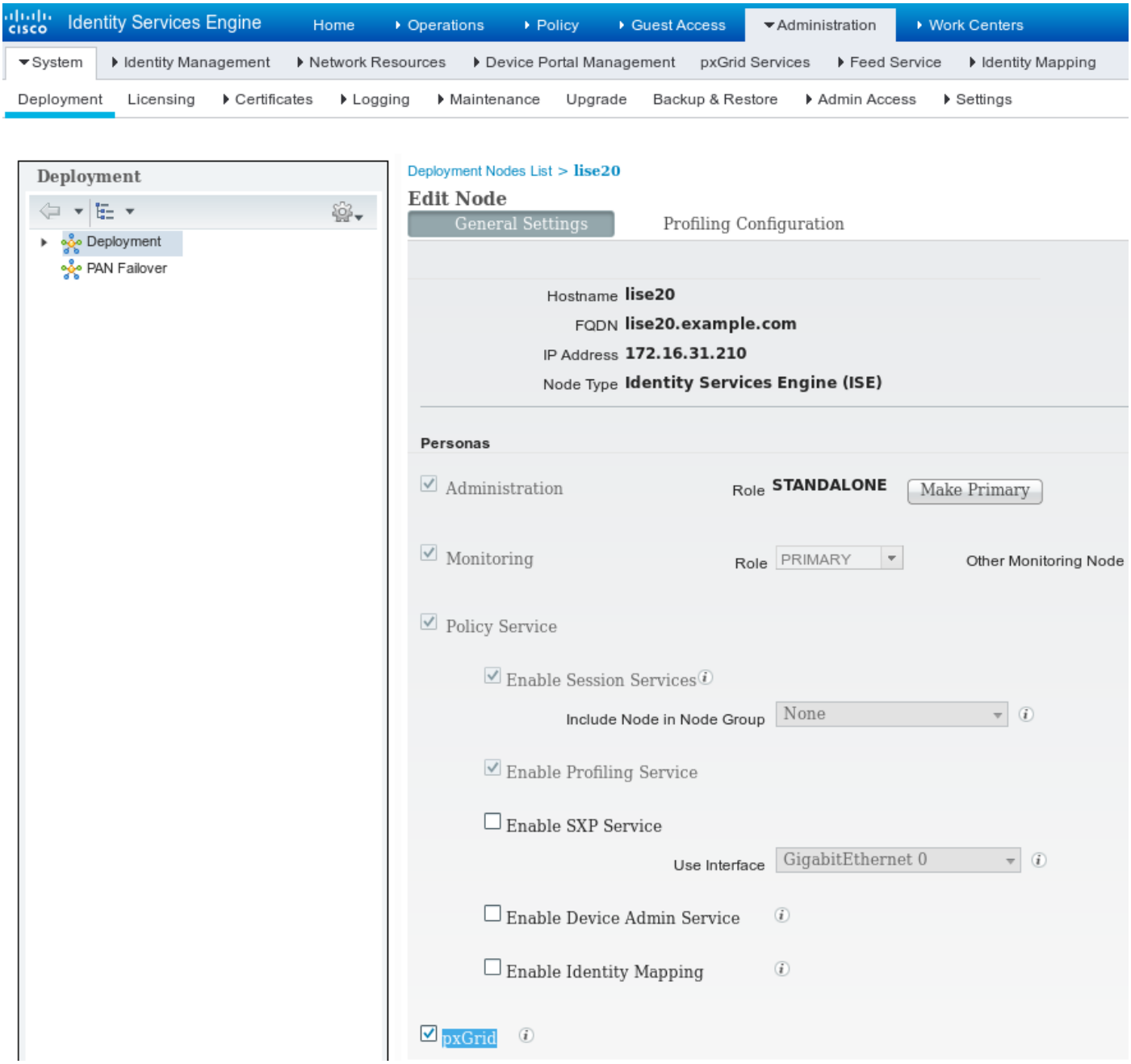


Na extremidade o ISE deve ter o Admin e os Certificados do pxGrid assinados por CA confiado (Microsoft) segundo as indicações desta imagem:

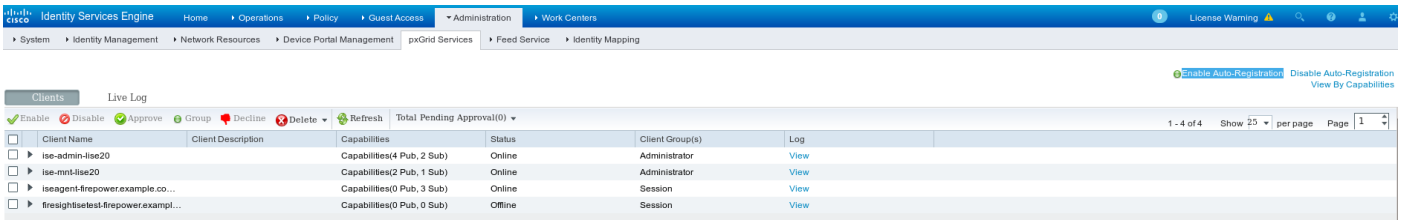


serviço do pxGrid

Com os Certificados corretos o papel do pxGrid para o nó específico deve ser permitido, segundo as indicações desta imagem:



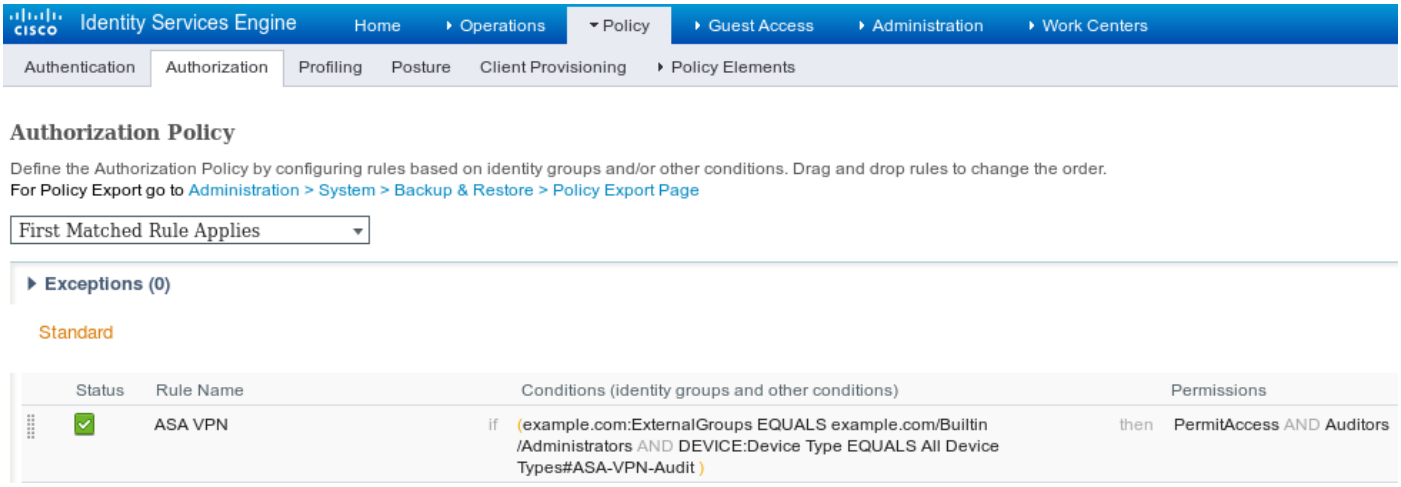
E a aprovação automática deve ser ajustada ao permitido:



Política da autorização

A política da autenticação padrão está usada (a consulta AD é executada se o usuário local não é encontrado).

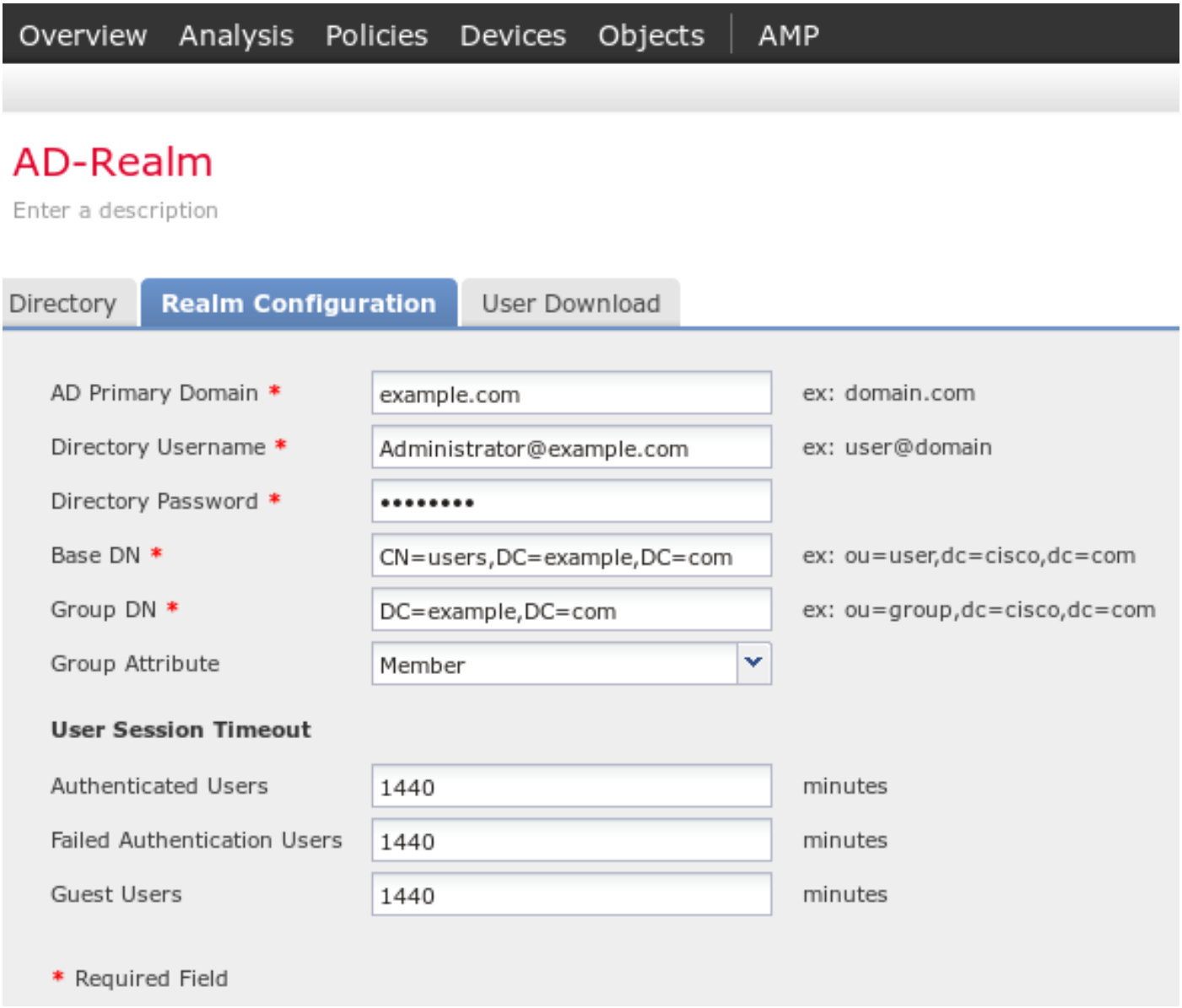
A política da autorização foi configurada para fornecer o acesso de rede completo (permissão: PermitAccess) para os usuários que autenticam através de ASA-VPN e que pertencem aos administradores do grupo do diretório ativo - para aqueles auditores da etiqueta dos usuários SGT é retornado:



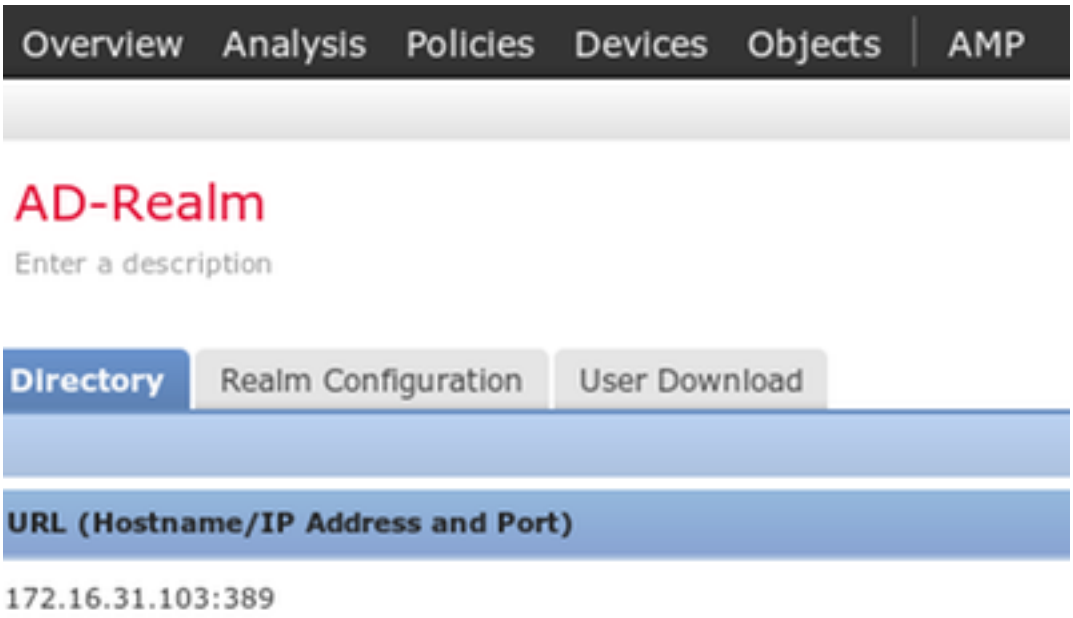
FMC

Reino do diretório ativo

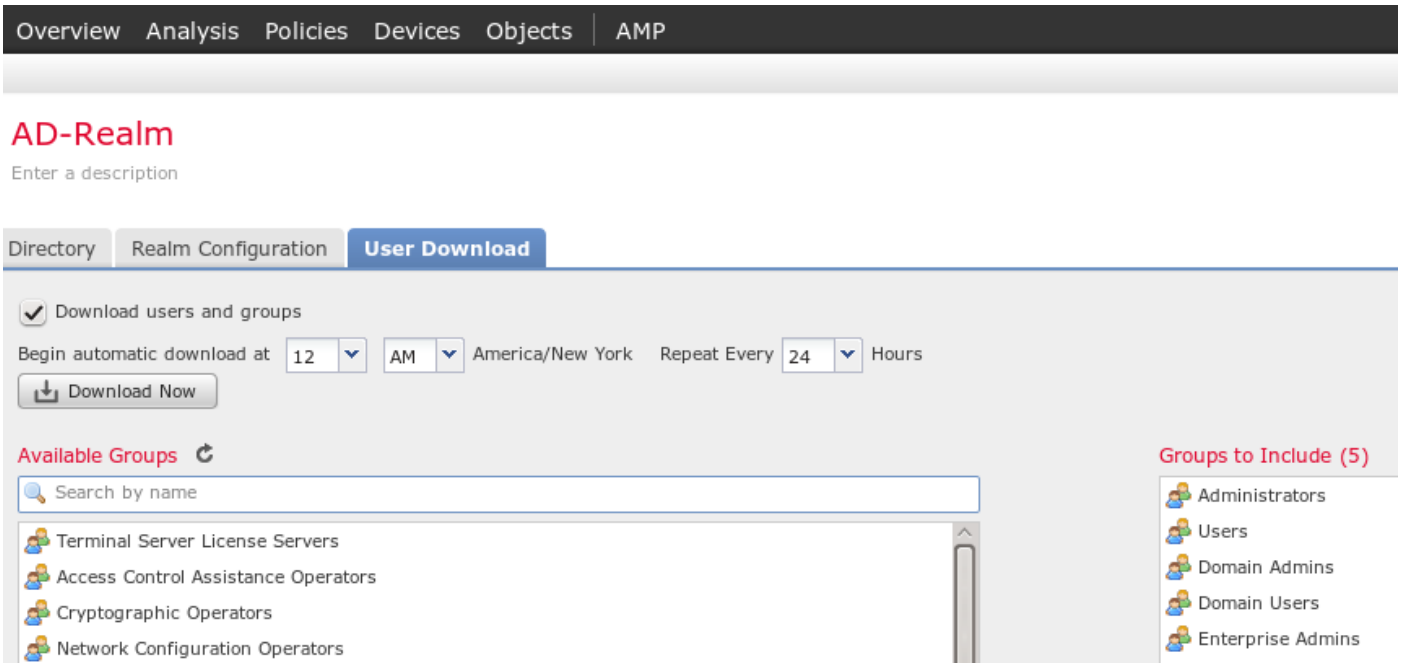
A configuração do reino é exigida a fim trabalhar com integração ISE (para usar políticas da identidade e para recuperar passivamente a membrasia do clube para usuários autenticados). O reino pode ser configurado para o diretório ativo ou o Lightweight Directory Access Protocol (LDAP). Neste exemplo o AD está sendo usado. **Do sistema > da integração > do reino**:



Os ajustes do diretório padrão são usados:

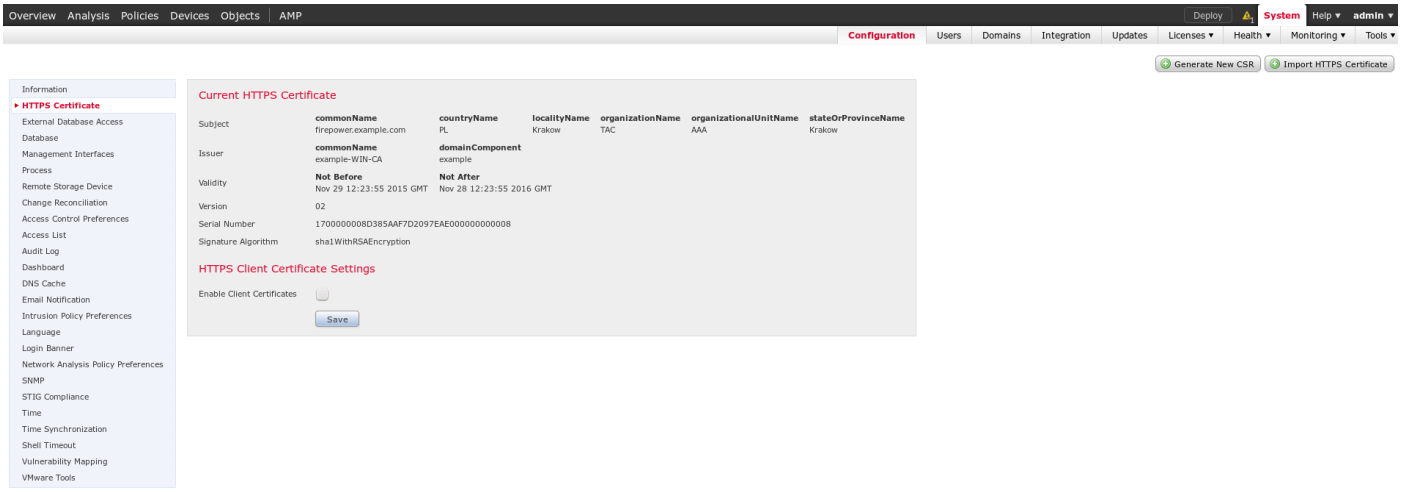


E alguns dos grupos AD são recuperados (para ser usado como a condição adicional no controle de acesso ordena):



Certificados para o Admin e o pxGrid

Embora não exigido, seu uma boa prática gerar o CSR para o acesso admin. Assine que o CSR usando o AD confiado, importa para trás o certificado assinado, segundo as indicações desta imagem:

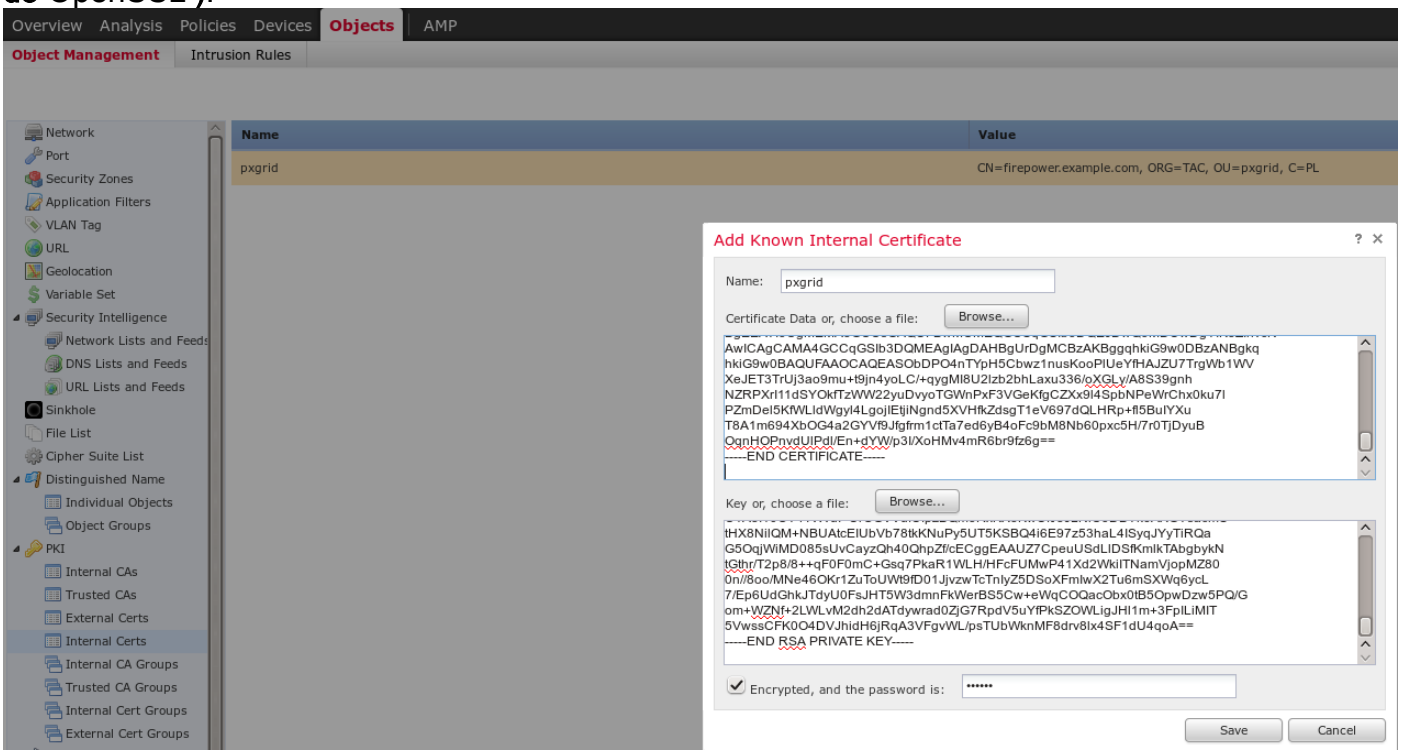


O certificado de CA precisa de ser adicionado a uma loja confiada:

A última etapa é gerar o certificado do pxGrid usado por FMC para autorizar ao serviço do pxGrid ISE. Para gerar CSR CLI precisa de ser usada (ou alguma outra máquina externo com ferramenta do OpenSSL).

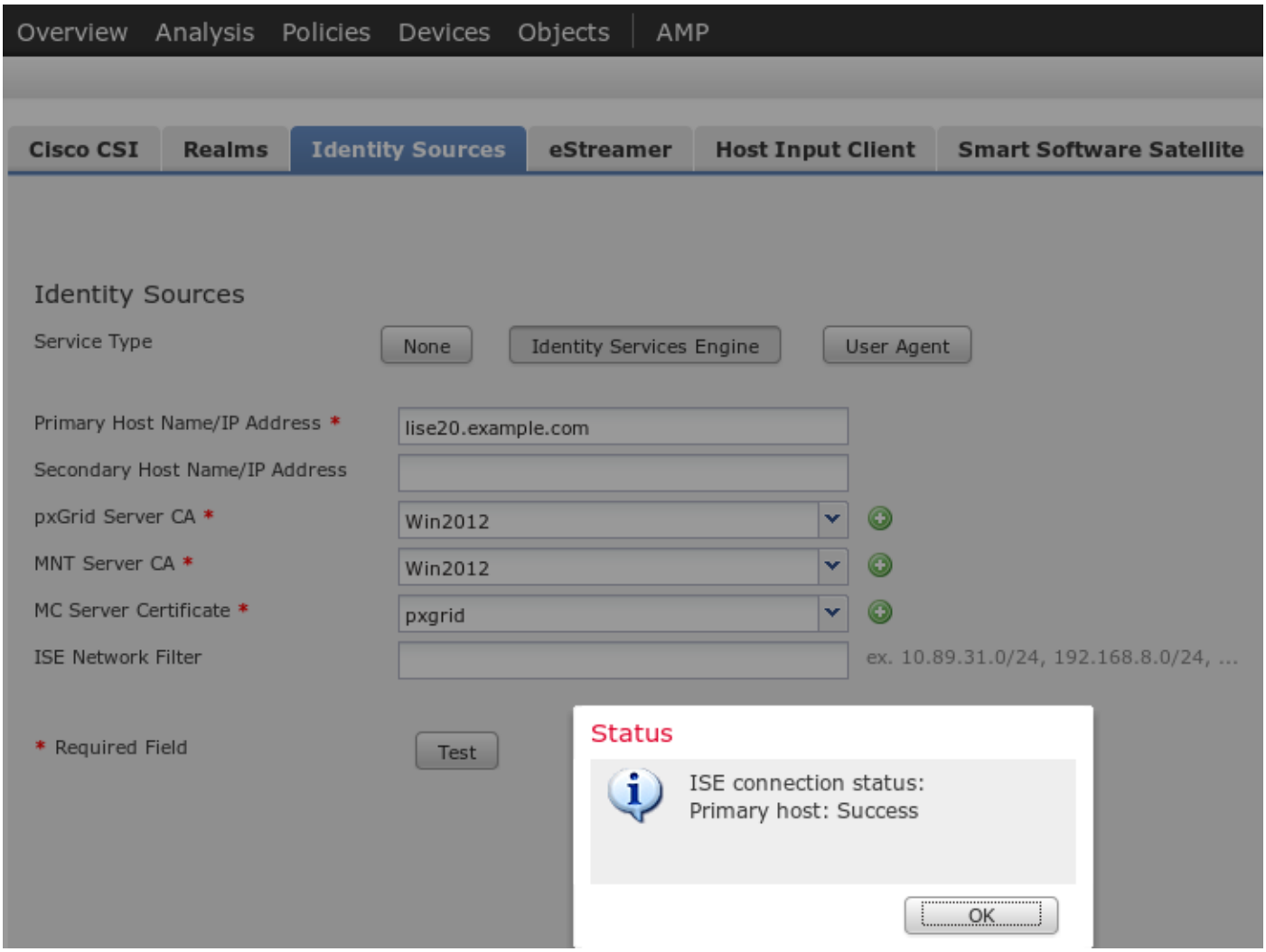
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#
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 uma vez gerados, assinam-na que usa Microsoft CA (molde do pxGrid). Importe para trás a chave privada (fire.key) e o certificado assinado (fire.pem) à loja interna do certificado FMC. Para a chave privada use a senha estabelecida durante a geração da chave (**comando do genrsa do** OpenSSL):



Integração ISE

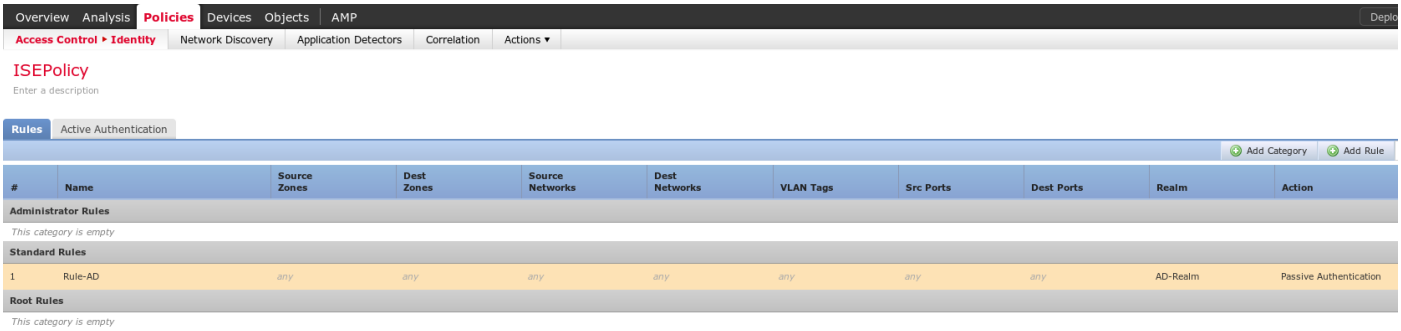
Uma vez que todos os Certificados são instalados configurar a integração ISE do **sistema > da integração**:



Use CA importado para a validação dos Certificados do pxGrid e dos serviços MNT. Para o console de gerenciamento (MC) use o certificado interno gerado para o pxGrid.

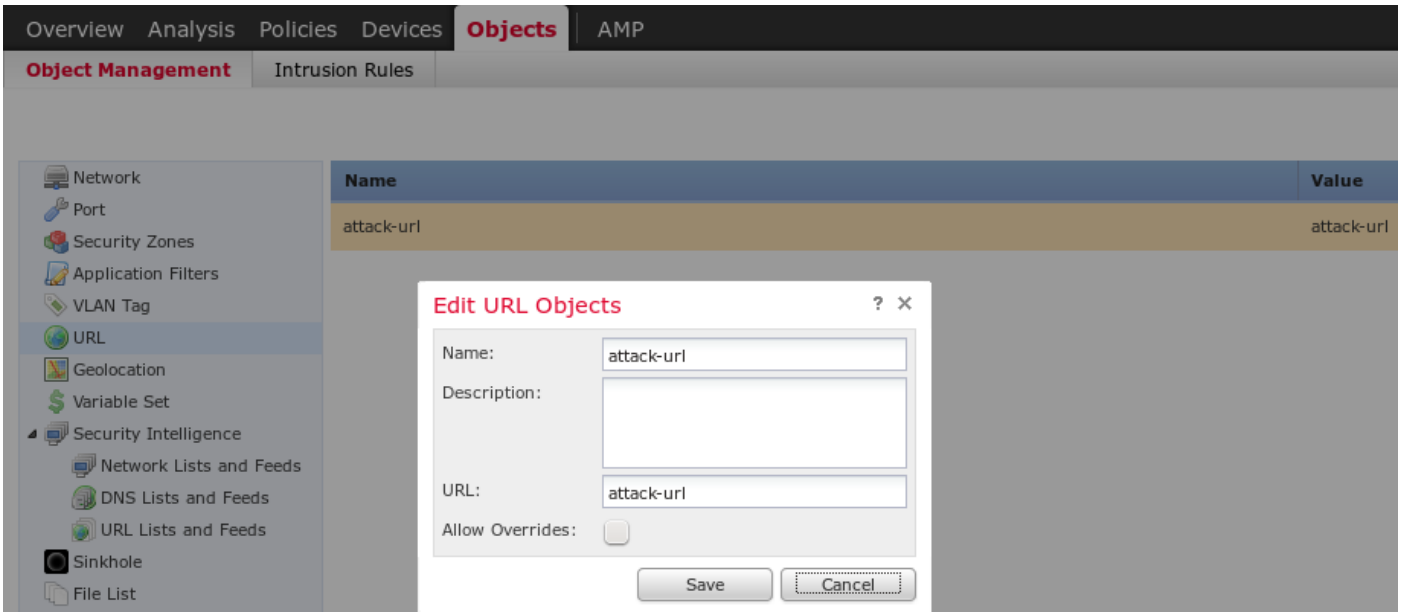
Política da identidade

Configurar a política da identidade que está utilizando o reino previamente configurado AD para a autenticação passiva:

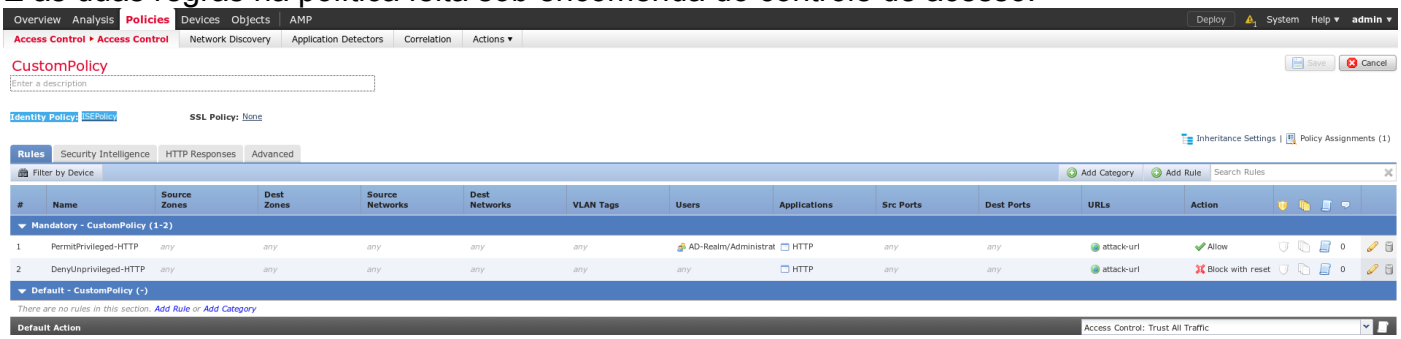


Política do controle de acesso

Para este exemplo o costume URL foi criado:



E as duas regras na política feita sob encomenda do controle de acesso:

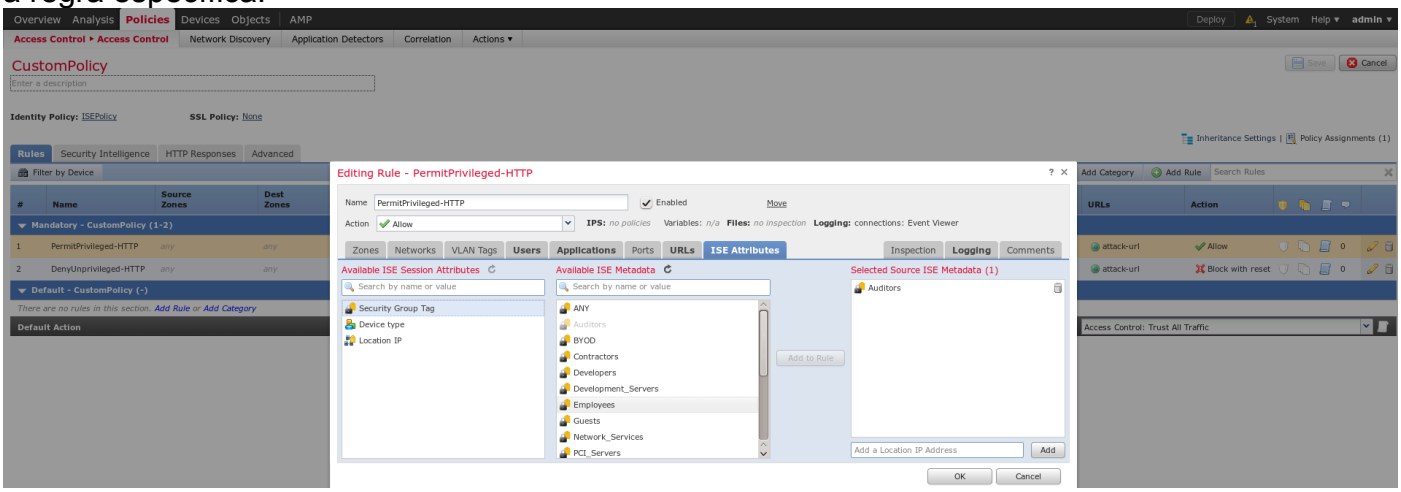


A regra PermitPrivileged-HTTP permite todos os usuários que pertencem ao grupo dos administradores AD que foram atribuídos a etiqueta SGT. Auditores para executar o ataque HTTP em todos os alvos.

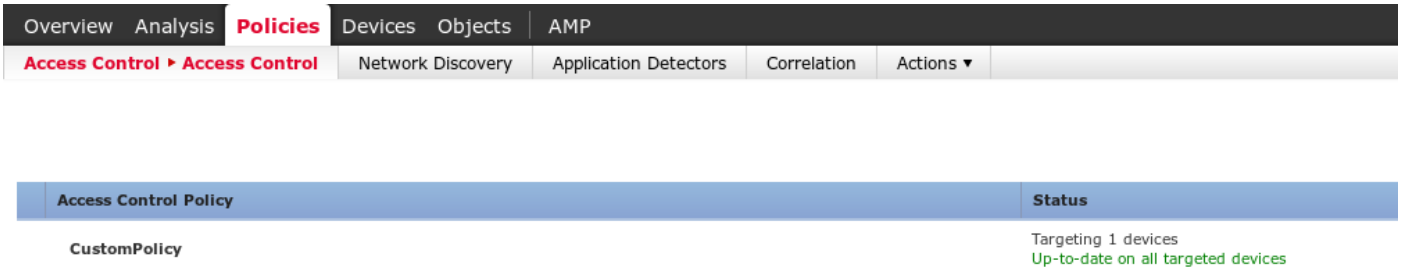
O DenyUnprivileged-HTTP nega essa ação a todos usuários restantes.

Igualmente observe que a política previamente criada da identidade esteve atribuída a esta política do controle de acesso.

Nesta aba seus não possíveis ver etiquetas SGT, mas naquelas são visíveis ao criar ou ao editar a regra específica:

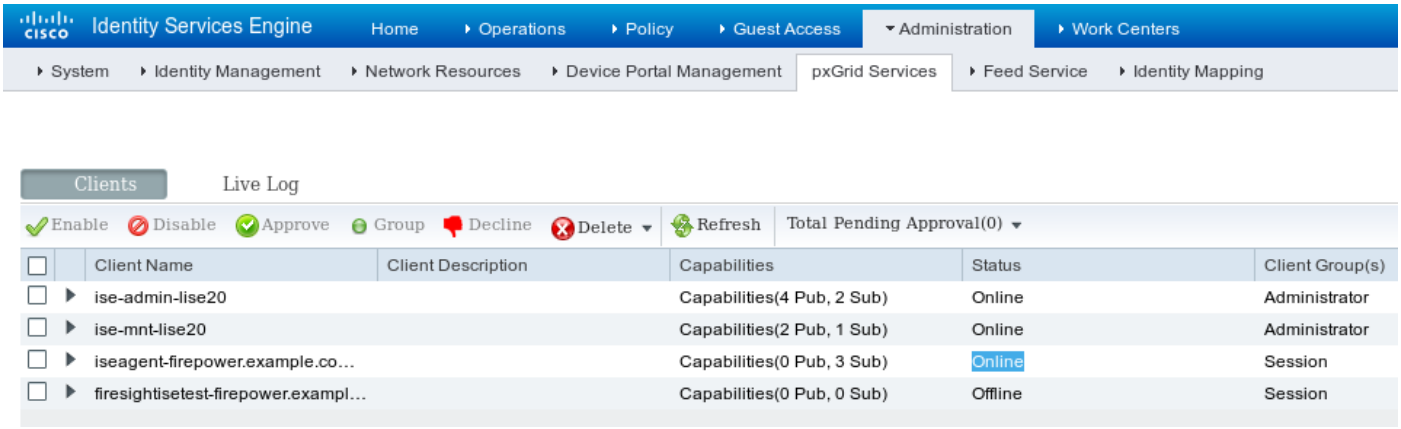


Assegure-se de que a política esteja atribuída ao NGIPS e todas as mudanças estejam distribuídas:

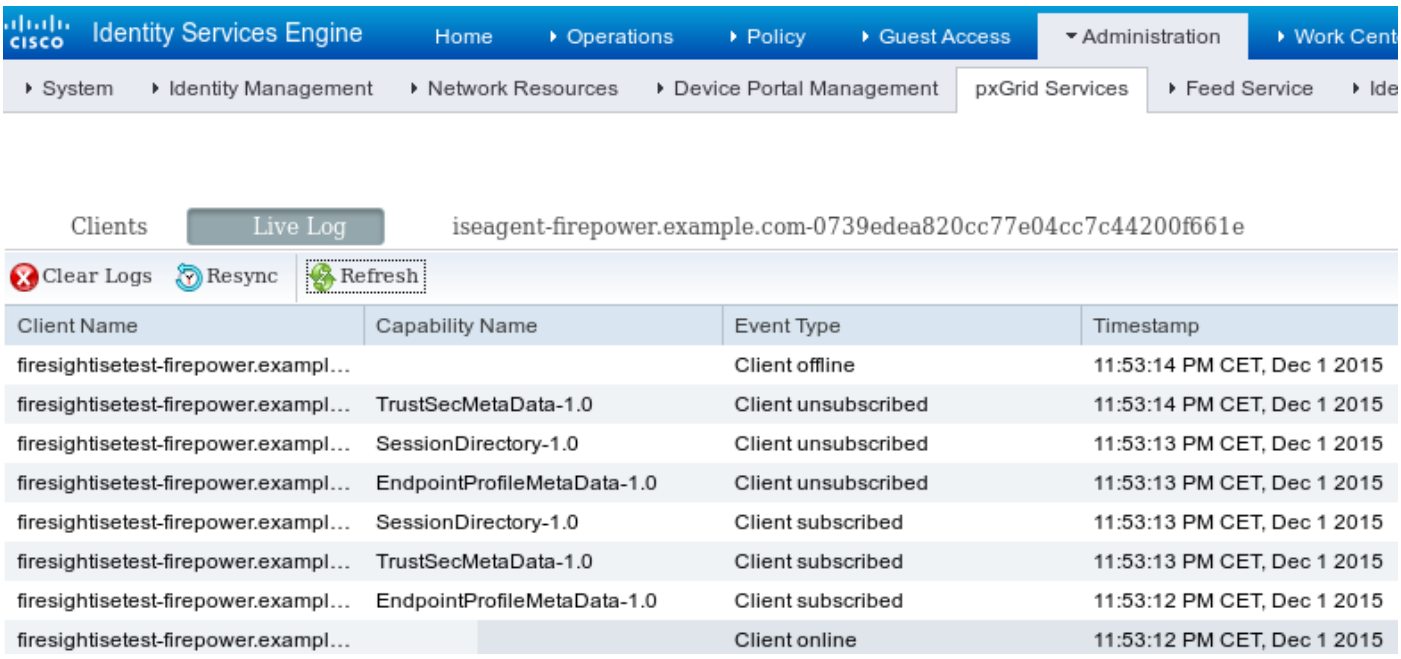


Verificar

Depois que tudo é configurado corretamente o ISE deve ver o cliente do pxGrid subscrever para um serviço de sessão (Online do estado).



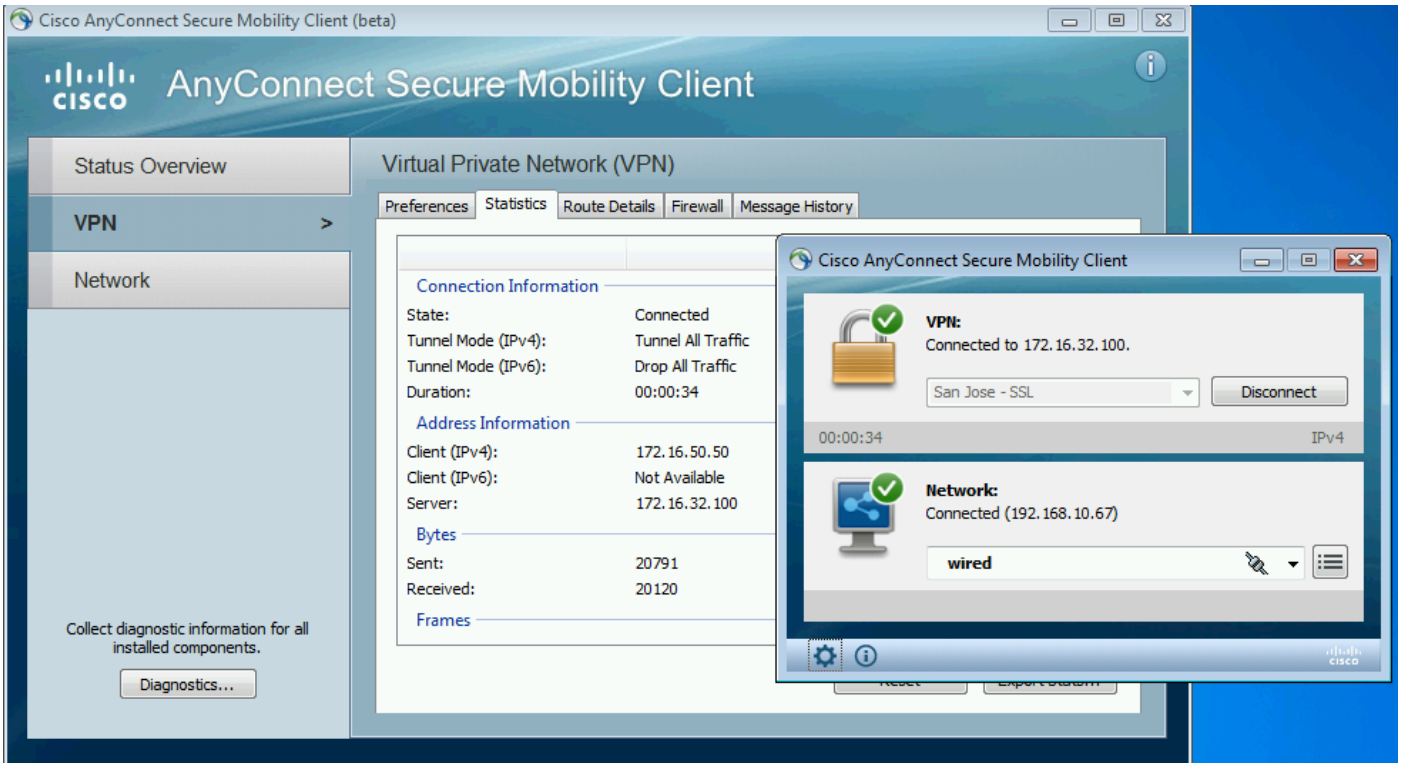
Dos logs você pode igualmente confirmar que FMC subscreveu para o serviço de TrustSecMetaData (etiquetas SGT) - obtiveram todas as etiquetas e unsubscribed.



Estabelecimento da sessão de VPN

O primeiro teste está executado para uma encenação quando a autorização no ISE não retorna a etiqueta correta SGT (NGIPS não permite testes de auditoria).

Uma vez que a sessão de VPN é ACIMA da interface do utilizador de AnyConnect (UI) pode fornecer mais detalhes:



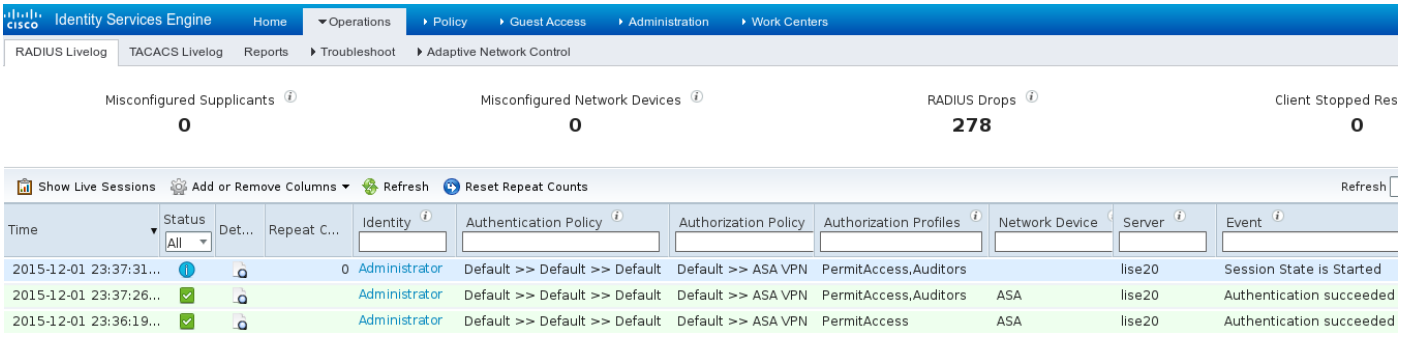
O ASA pode confirmar a sessão é estabelecido:

```
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
```

Observe por favor que o ASA vê toda a etiqueta SGT retornada para esta autenticação. O ASA não é configurado para TrustSec - de modo que a informação é saltada de qualquer maneira.

O ISE é igualmente relatando a autorização bem sucedida (o log em 23:36:19) - nenhuma etiqueta SGT retornada:



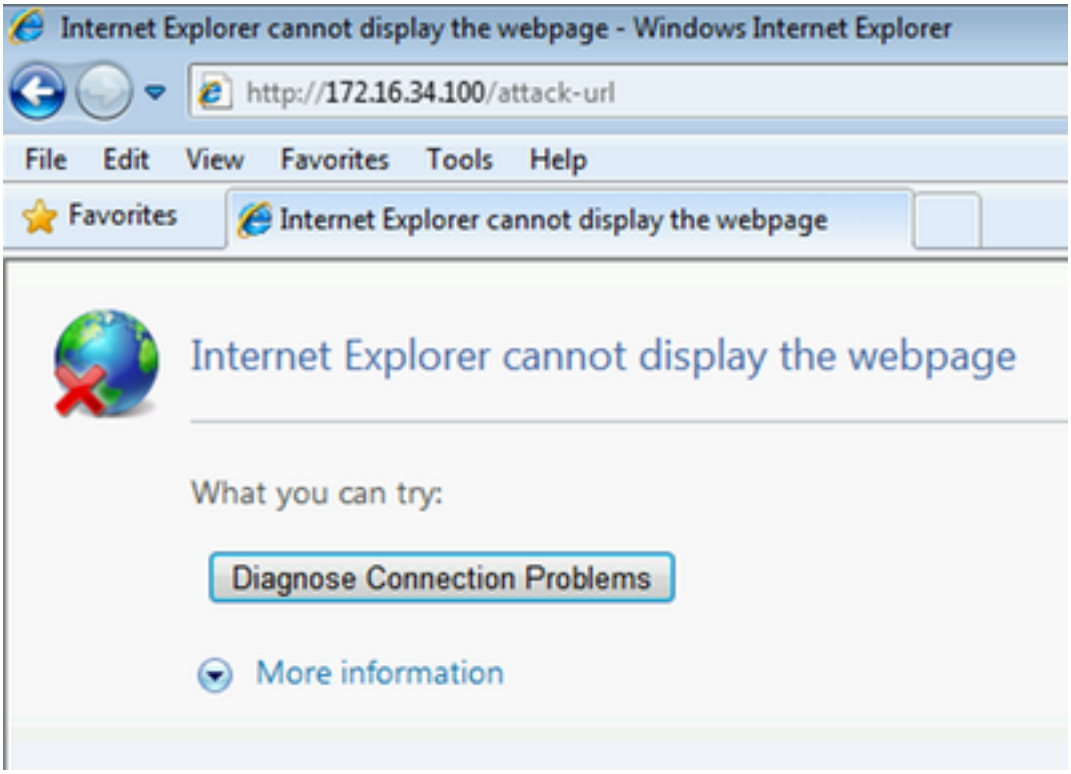
FMC que obtém dados de sessão do MNT

Nessa fase FMC em /var/log/messages relata uma sessão nova (recebida como um subscritor para o serviço do pxGrid) para a consulta do nome de usuário de administrador e do peform AD para a membrasia do clube:

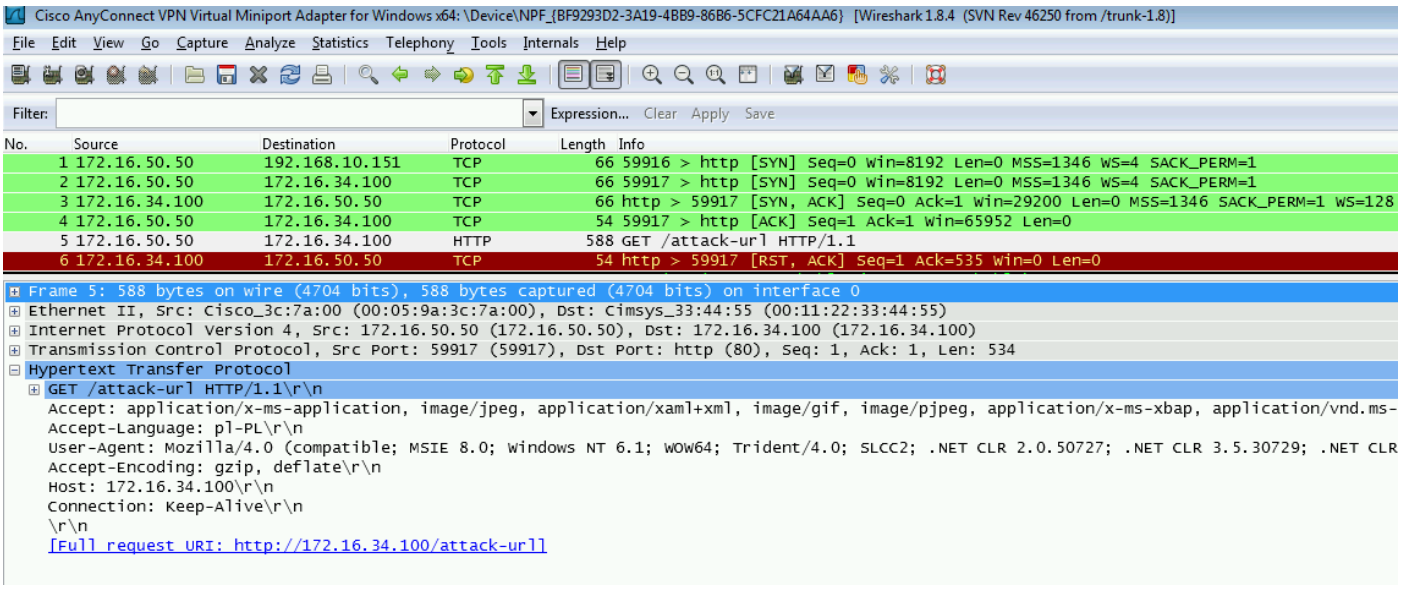
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

Acesso de rede Unprivileged e privilegiado

Quando nas tentativas desse usuário da fase para abrir o navegador da Web e o alcançar examinou o server, a conexão será terminada:



Pode ser confirmada pelas capturas de pacote de informação tomadas do cliente (o TCP RST envia conforme a configuração FMC):

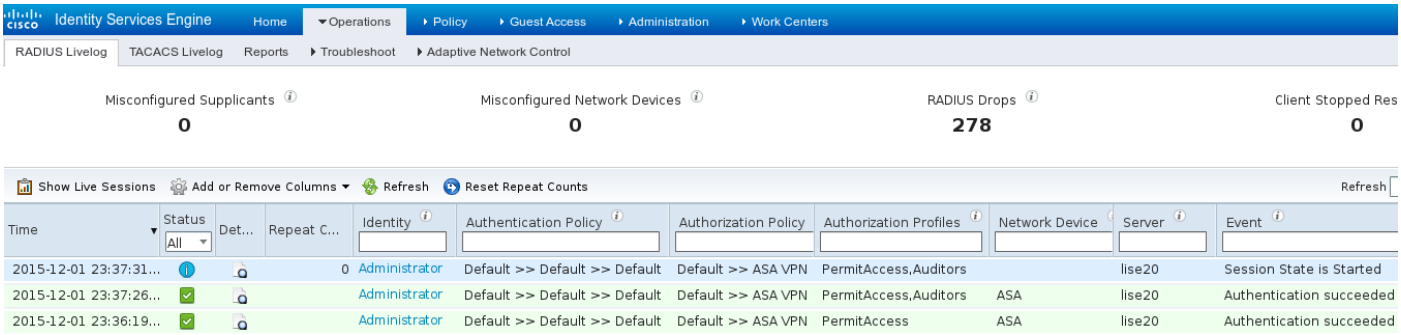


Uma vez que o ISE é configurado para retornar, a sessão da etiqueta ASA da auditoria relata:

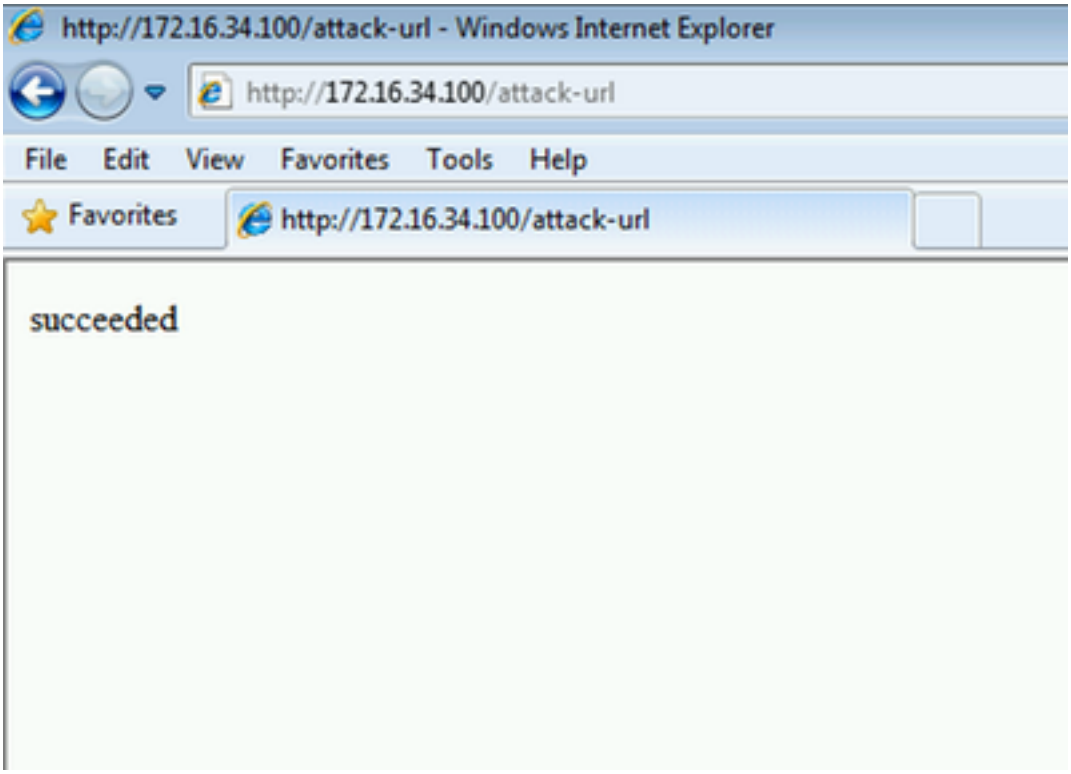
```
asav# show vpn-sessiondb anyconnect

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
```

O ISE é igualmente relata um auditor da etiqueta da autorização bem sucedida (o log em 23:37:26) - SGT é retornado:

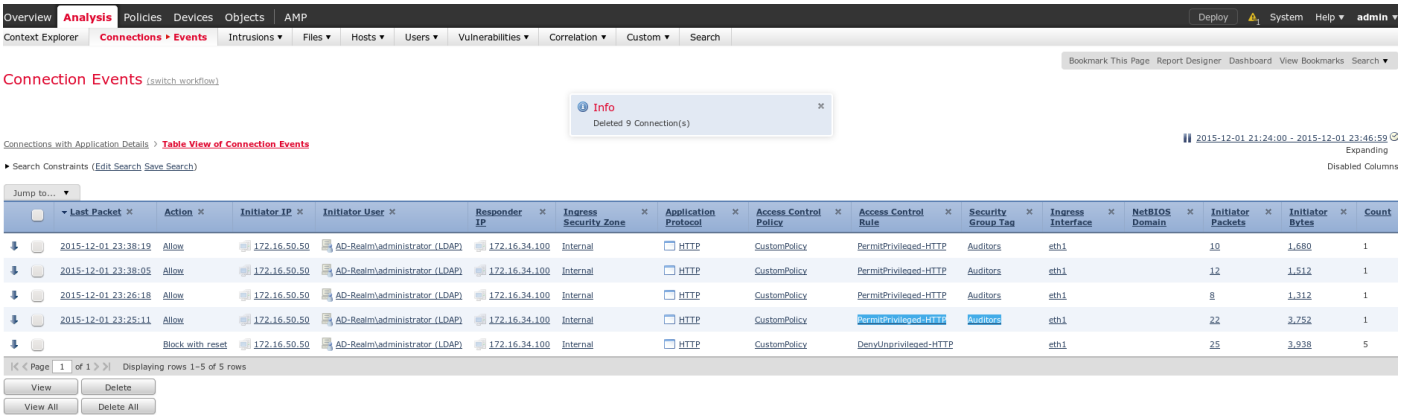


E o usuário pode alcançar o serviço mencionado:



Acesso de registro FMC

Esta atividade pode ser confirmada pelo relatório do evento de conexão:



Primeiramente, o usuário não teve nenhuma etiqueta SGT atribuída e bateu a regra DenyUnprivileged-HTTP. Uma vez que a etiqueta do auditor esteve atribuída pela regra ISE (e recuperada por FMC), o PermitPrivileged-HTTP está usado e o acesso é permitido.

Igualmente observe isso para ter o indicador, as colunas múltiplas foram removidas porque normalmente a etiqueta da regra e do grupo de segurança do controle de acesso é indicada como uma das últimas colunas (e da barra de rolagem horizontal precisa de ser usado). Que a vista personalizada pode ser salvar e reutilizado no futuro.

Troubleshooting

FMC debuga

Para verificar os logs do responsável componente DDA para ver se há a verificação /var/log/messages de serviços da identidade arquivam:

```
[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 obter mais detalhado debugar-la é possível para matar o processo DDA (da raiz após o sudo) e para executá-lo com debugam o argumento:

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

Pergunta SGT através do pxGrid

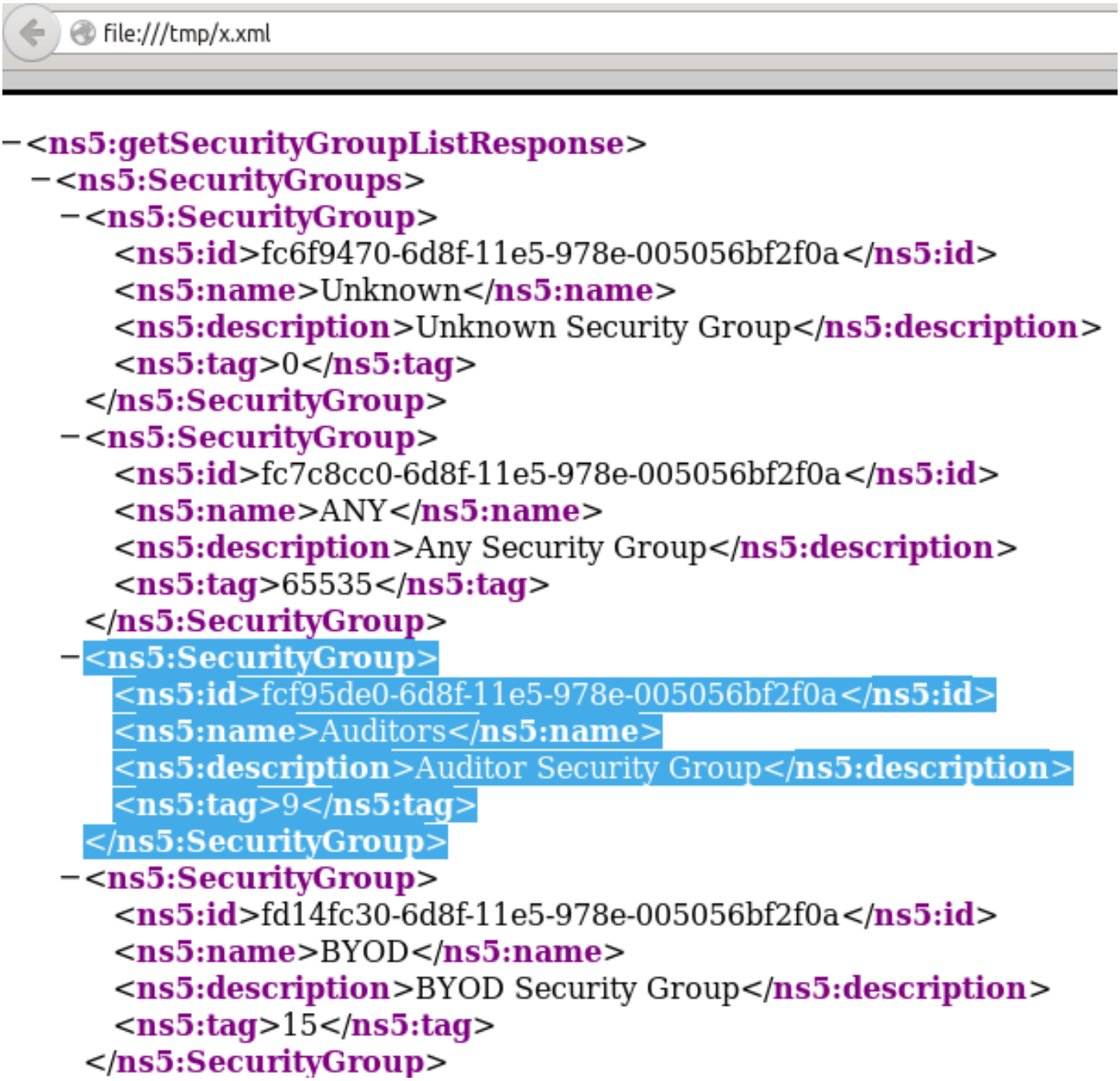
A operação está executada quando o **botão Test Button** está clicado na **seção de integração ISE**

ou quando a lista SGT é refrescada, ao adicionar a regra na política do controle de acesso.

```
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>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>]

Para o melhor xml da vista um índice desse log pode ser copiado ao arquivo do xml e ser aberto por um navegador da Web. Você pode confirmar que SGT específico (auditoria) está sendo recebido assim como todo SGT restante está sendo definido no ISE:



Pergunta da sessão através do RESTO API ao MNT

Aquela é igualmente parte de uma operação de teste (observe por favor que o hostname e a porta MNT estão passados através do pxGrid). A transferência maioria da sessão é usada:

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>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:getSec
urityGroupListResponse>]
```

E resultado analisado gramaticalmente (1 sessão ativa recebida):

```
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}
```

Nessa fase NGIPS é tentativas para correlacionar esse username (e domínio) com o username 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
```

O LDAP é usado para encontrar um usuário e uma membrasia do clube:

```
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.
```

O ISE debuga

Após ter permitido o nível de rastreamento debugar para o componente do pxGrid seu possível verificar cada operação (mas sem payload/dados como em FMC).

Exemplo com recuperação da 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
```

Erros

CSCuv32295 - O ISE pode enviar a informação de domínio nos campos de nome de usuário

CSCus53796 - Incapaz de obter o FQDN do host para a pergunta do volume do RESTO

CSCuv43145 - PXGRID & reinício do serviço do mapeamento da identidade, importação/supressão da loja da confiança

Referências

- Configurar serviços da remediação com integração ISE e de FirePOWER
- Configurando o pxGrid em um ambiente distribuído ISE
- Certificados Como de distribuição com pxGrid de Cisco: Configurando o nó CA-assinado do pxGrid ISE e o cliente CA-assinado do pxGrid
- Integração do pxGrid da versão 1.3 ISE com aplicativo do pxLog IPS
- Guia do administrador do Cisco Identity Services Engine, liberação 2.0
- Guia de referência do Cisco Identity Services Engine API, liberação 1.2 – Introdução a S repousante externo…
- Guia de referência do Cisco Identity Services Engine API, liberação 1.2 – Introdução ao RES de monitoração…
- Guia do administrador do Cisco Identity Services Engine, liberação 1.3
- Suporte Técnico e Documentação - Cisco Systems