Risoluzione dei problemi di integrazione ISE e FirePOWER per Identity Services

Sommario

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi ai criteri con visibilità TrustSec su Cisco Next-Generation Intrusion Prevention System (NGIPS). NGIPS versione 6.0 supporta l'integrazione con Identity Services Engine (ISE), consentendo di creare criteri di riconoscimento delle identità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione VPN di Cisco Adaptive Security Appliance (ASA)
- Configurazione di Cisco AnyConnect Secure Mobility Client
- Configurazione di base di Cisco FirePower Management Center
- Cisco ISE configuration
- Soluzioni Cisco TrustSec

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- CA (Certification Authority) di Microsoft Windows 2012
- Cisco ASA versione 9.3
- Software Cisco ISE versioni 1.4
- Cisco AnyConnect Secure Mobility Client versioni 4.2
- Cisco FirePower Management Center (FMC) versione 6.0
- Cisco FirePower NGIPS versione 6.0

Configurazione

FirePower Management Center (FMC) è la piattaforma di gestione di FirePower. Per l'integrazione con ISE sono disponibili due tipi di funzionalità:

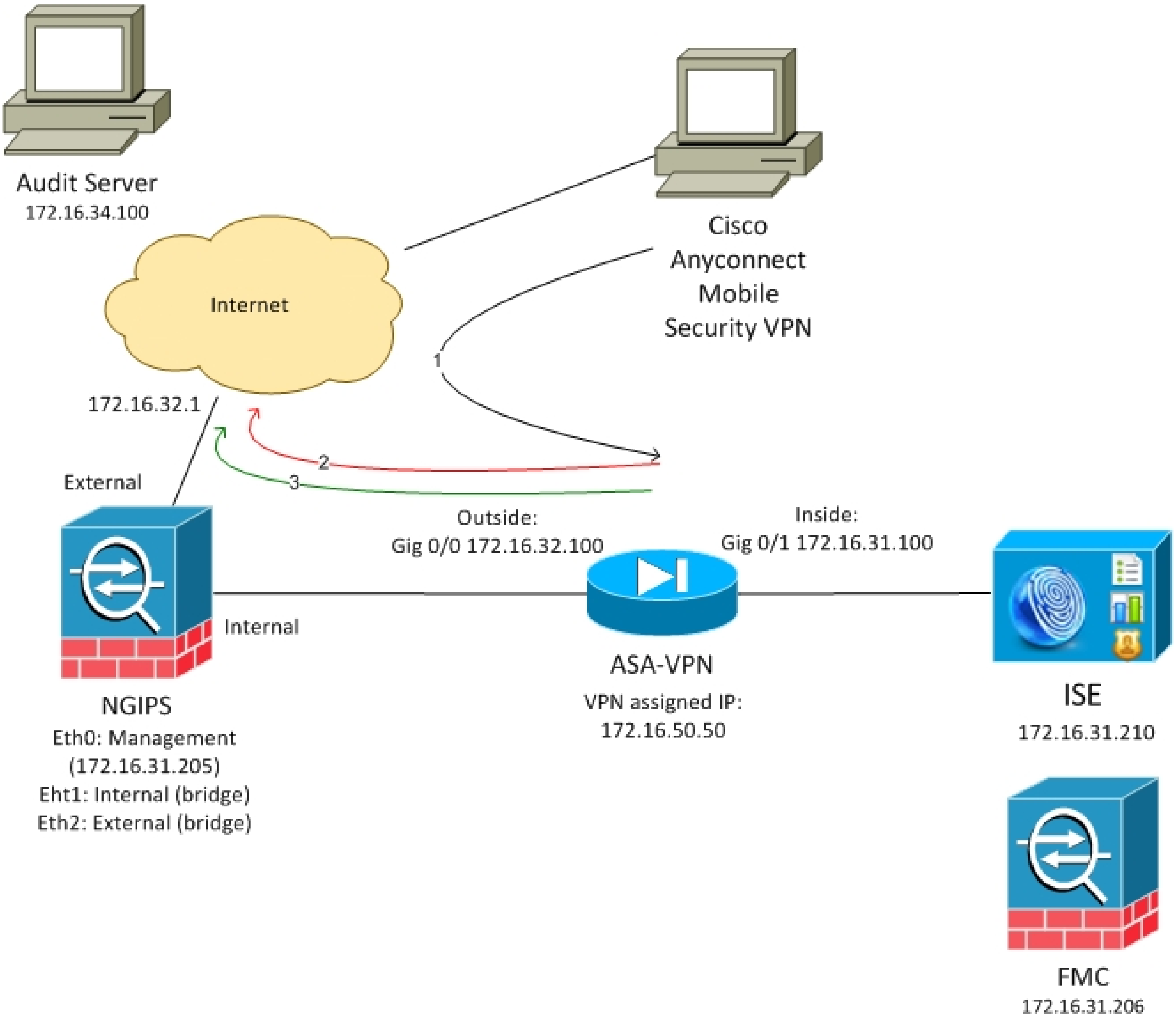
- Correzione: consente al FMC di mettere in quarantena l'aggressore tramite ISE, che modifica dinamicamente lo stato di autorizzazione sul dispositivo di accesso fornendo accesso limitato alla rete. Questa soluzione si presenta in due generazioni:

1. Script perl legacy che utilizza la chiamata API EPS (Endpoint Protection Service) ad ISE.
2. Modulo più recente che utilizza la chiamata del protocollo pxGrid ad ISE (questo modulo è supportato solo nella versione 5.4 - non è supportato nella versione 6.0, il supporto nativo è pianificato nella versione 6.1).

- Criterio: consente a FMC di configurare i criteri in base ai tag del gruppo di sicurezza TrustSec (SGT).

In questo articolo viene illustrata la seconda funzionalità. Per l'esempio di correzione, leggere la sezione dei riferimenti

Esempio di rete



FMC è configurato con criteri di controllo dell'accesso contenenti due regole:

- Nega per traffico HTTP con URL personalizzato (URL-attacco)
- Consenti traffico HTTP con URL personalizzato (URL di attacco) ma solo se l'utente è assegnato al tag SGT Audit (9) da ISE

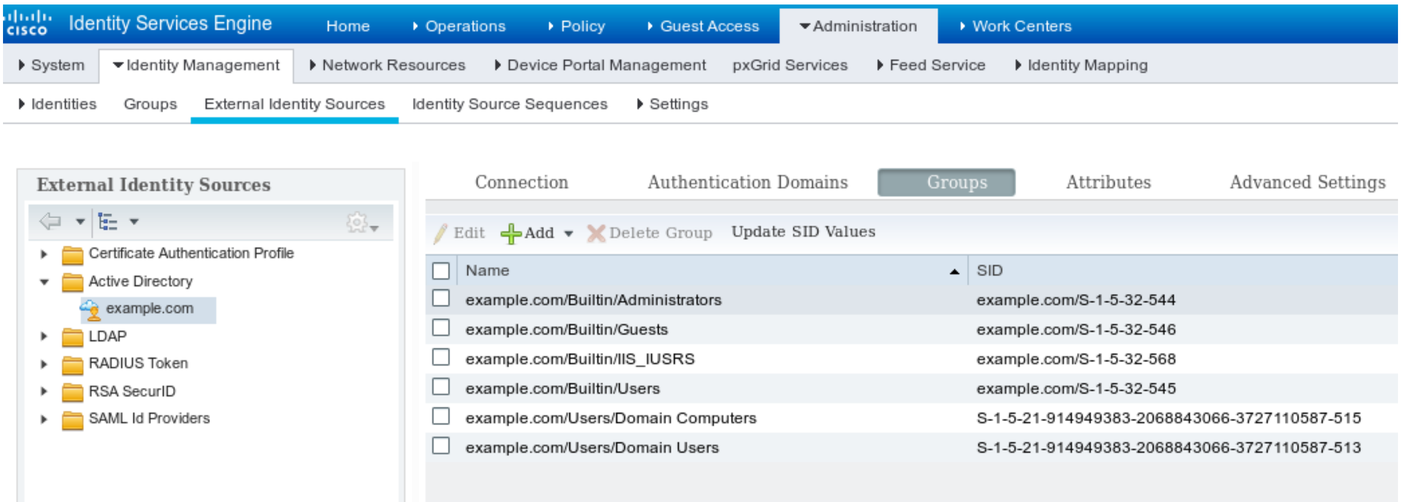
ISE decide di assegnare un tag di controllo a tutti gli utenti di Active Directory che appartengono al gruppo Administrator e utilizzano un dispositivo ASA-VPN per l'accesso alla rete.

L'utente accede alla rete tramite connessione VPN sull'appliance ASA. L'utente tenta quindi di accedere al server sottoposto ad audit utilizzando l'URL di attacco URL, ma l'operazione non riesce perché non è stato assegnato al gruppo Audit SGT. Una volta risolto questo problema, la connessione è riuscita.

ISE

Active Directory

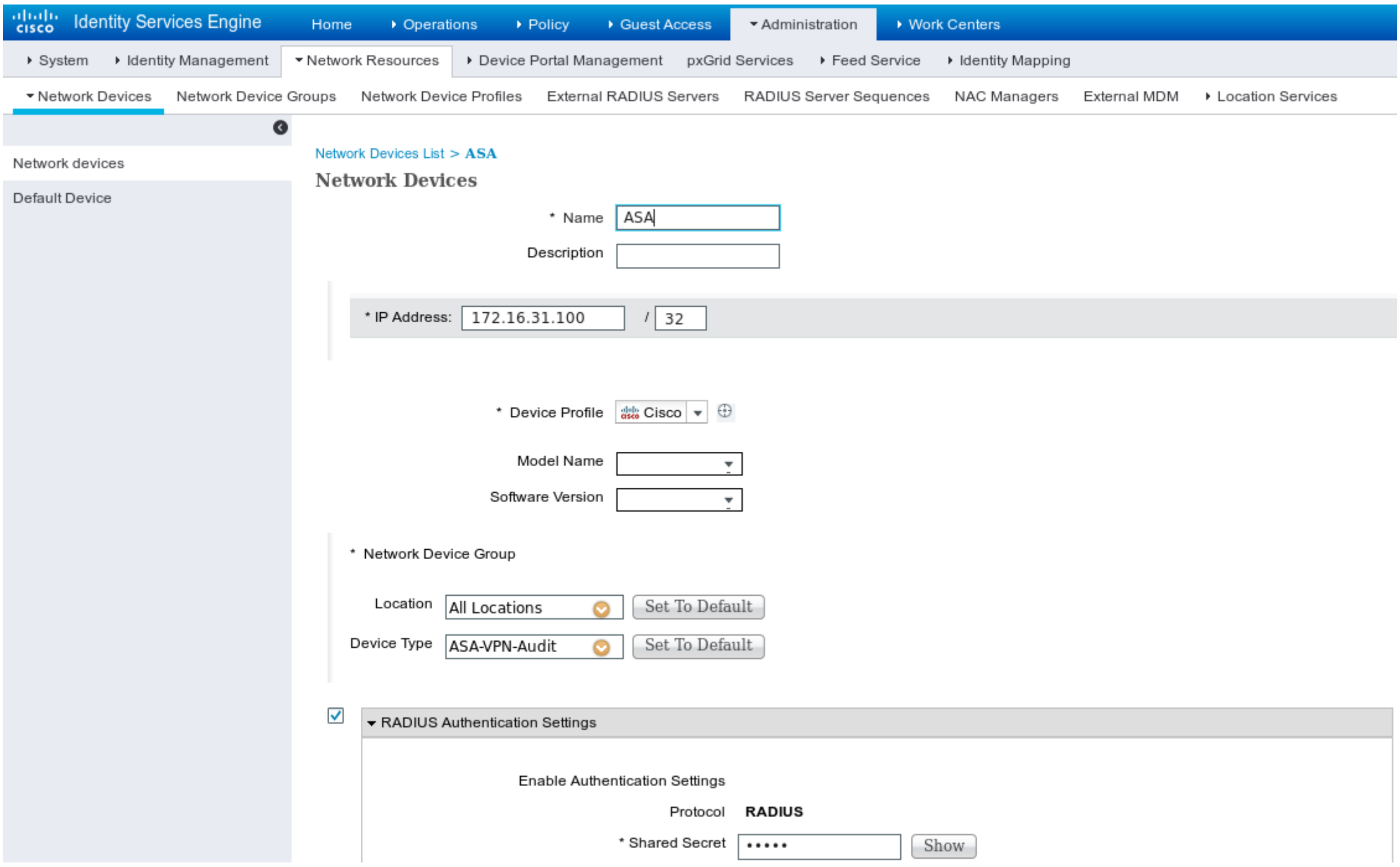
Ènecessario configurare l'integrazione di Active Directory e recuperare i gruppi corretti (il gruppo Administrators viene utilizzato per la condizione della regola di autorizzazione):



	Name	SID
□	example.com/Builtin/Administrators	example.com/S-1-5-32-544
□	example.com/Builtin/Guests	example.com/S-1-5-32-546
□	example.com/Builtin/IIS_IUSRS	example.com/S-1-5-32-568
□	example.com/Builtin/Users	example.com/S-1-5-32-545
□	example.com/Users/Domain Computers	S-1-5-21-914949383-2068843066-3727110587-515
□	example.com/Users/Domain Users	S-1-5-21-914949383-2068843066-3727110587-513

Dispositivo di accesso alla rete

L'ASA viene aggiunta come dispositivo di rete. Viene usato il gruppo personalizzato ASA-VPN-Audit, come mostrato nell'immagine:



Network Devices

* Name: ASA

Description:

* IP Address: 172.16.31.100 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

Device Type: ASA-VPN-Audit

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: •••••

Certificati per pxGrid e MnT

FMC utilizza entrambi i servizi su ISE:

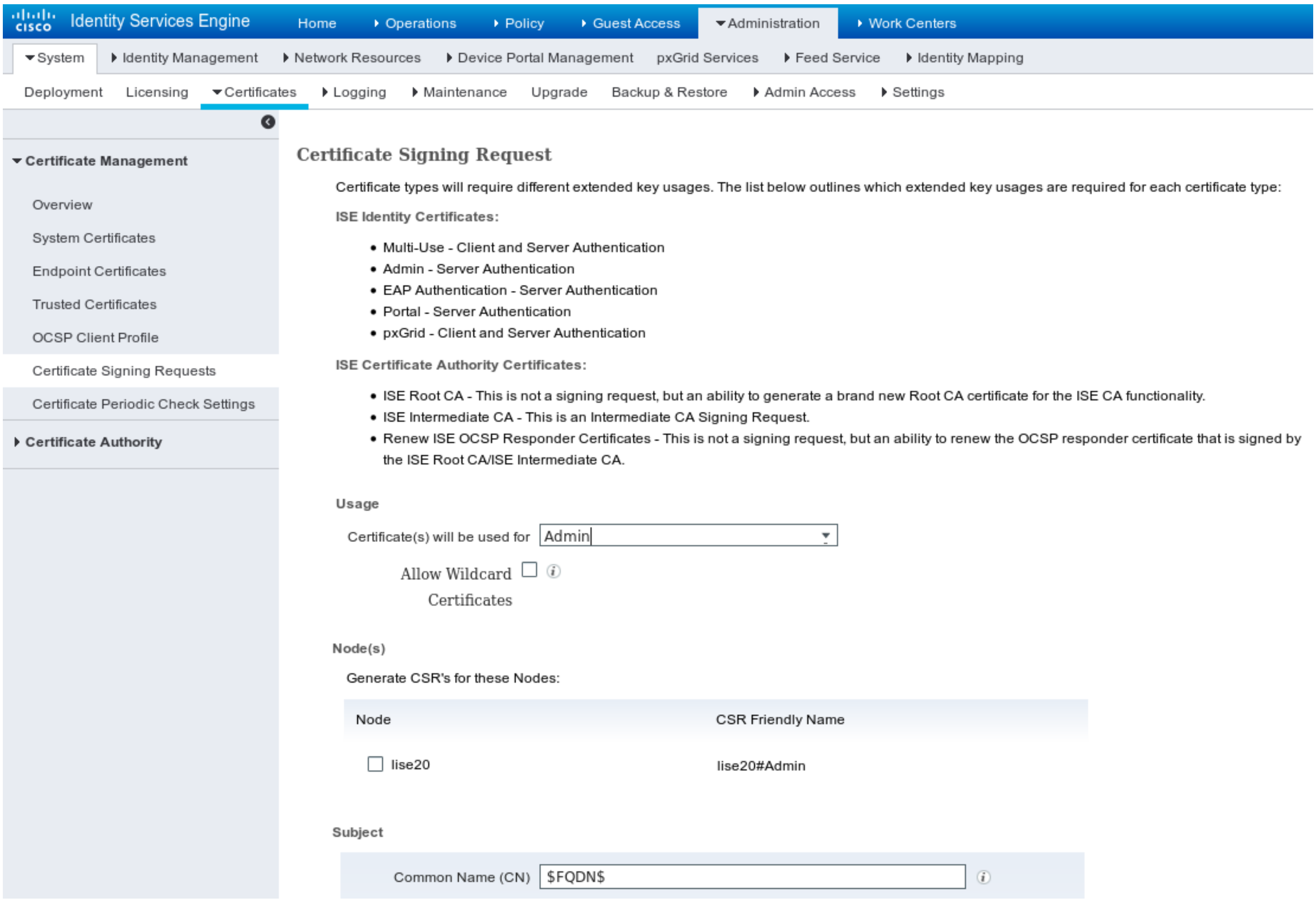
- pxGrid per SGT e query di profiling dei dati
- MnT (Monitoring and Reporting) per il download di sessioni in blocco

La disponibilità di MnT è molto importante poiché in questo modo FMC viene informato su quale sia l'indirizzo IP della sessione autenticata, nonché il nome utente e il tag SGT. In base a ciò, è possibile applicare le policy corrette. Notare che NGIPS non supporta i tag SGT nativi (tagging in linea) come nell'appliance ASA. Ma al contrario di ASA, supporta solo nomi SGT anziché numeri.

A causa di tali requisiti, sia ISE che FMC devono fidarsi a vicenda (certificato). MnT utilizza solo il certificato lato server, pxGrid utilizza sia il certificato lato client che quello lato server.

La CA Microsoft viene utilizzata per firmare tutti i certificati.

Per MnT (ruolo Admin), ISE deve generare una richiesta di firma del certificato (CSR), come mostrato nell'immagine:



Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: Admin

Allow Wildcard Certificates ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☐ lise20	lise20#Admin

Subject

Common Name (CN): $FQDN$

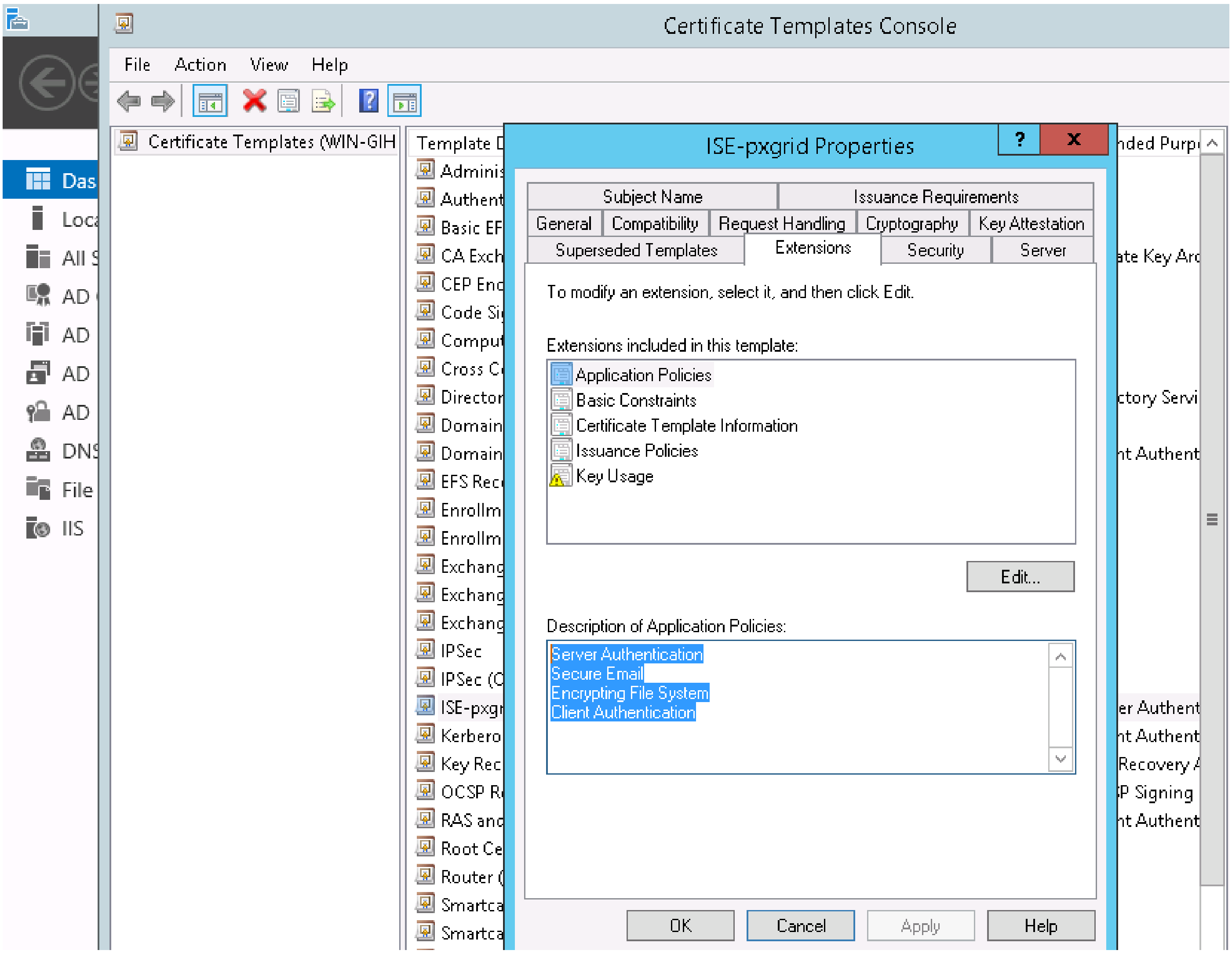
Dopo essere stato firmato da Microsoft CA deve essere importato tramite l'opzione **Bind Certificate**.

È necessario seguire un processo simile per il servizio pxGrid. **Per l'**opzione **verrà utilizzato uno o più certificati** con pxGrid selezionato.

Poiché non possono esistere due certificati con lo stesso nome soggetto, è possibile aggiungere un valore diverso per OU o sezione O (ad esempio pxGrid).

> **Nota:** Verificare che per ogni nome di dominio completo (FQDN) sia per ISE che per FMC sia configurato il record DNS corretto nel server DNS.

L'unica differenza tra il certificato Admin e il certificato pxGrid è con il processo di firma. Poiché i certificati pxGrid devono disporre di opzioni di utilizzo chiavi esteso sia per l'autenticazione client che per l'autenticazione server, è possibile utilizzare un modello personalizzato in Microsoft CA per tale scopo:



To modify an extension, select it, and then click Edit.

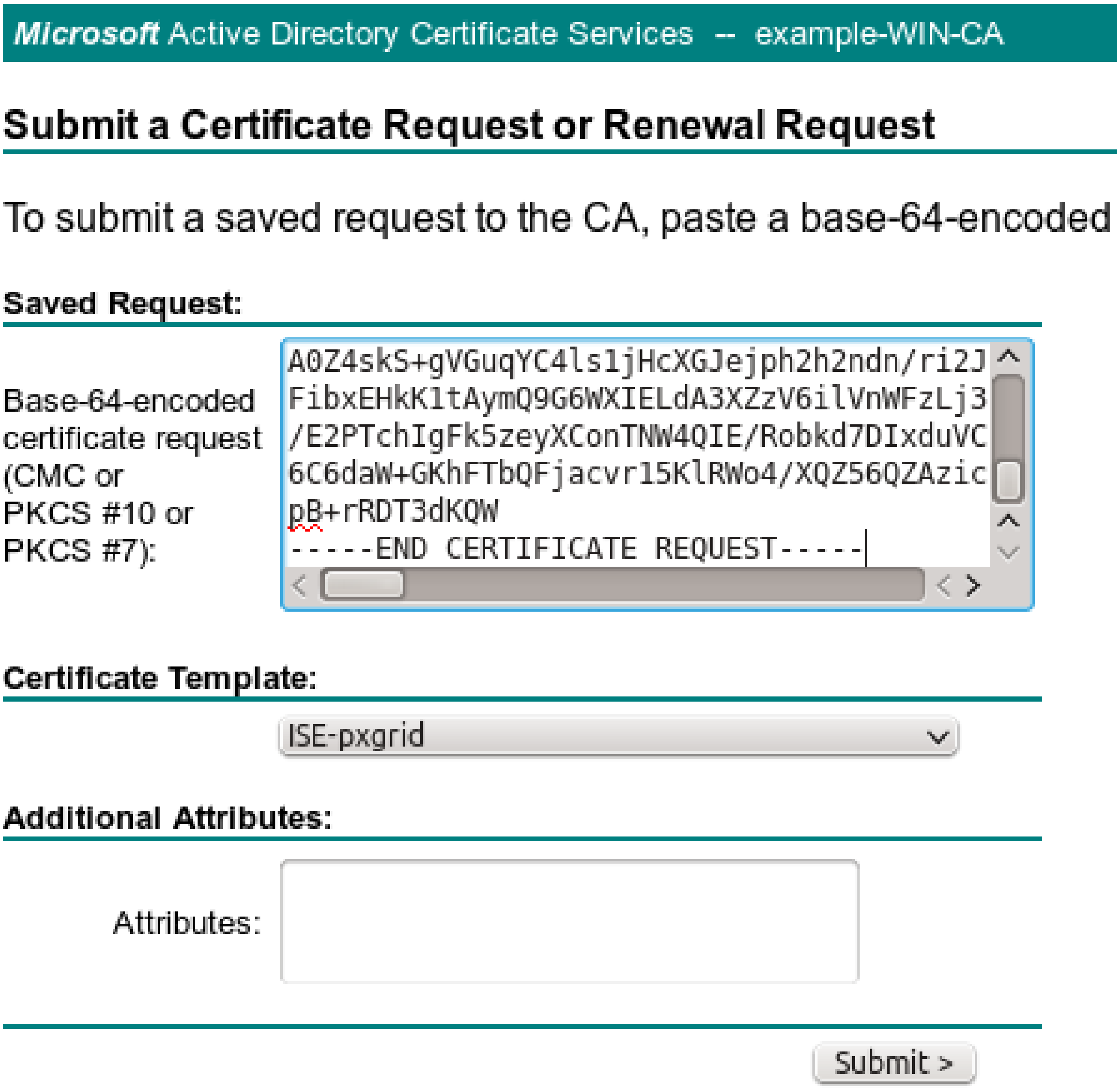
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Server Authentication
Secure Email
Encrypting File System
Client Authentication

In questa immagine è illustrato come utilizzare il servizio Web Microsoft per firmare PxGrid CSR:



Microsoft Active Directory Certificate Services -- example-WIN-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
A0Z4skS+gVGuqYC4ls1jHcXGJejph2h2ndn/ri2J
FibxEHkK1tAymQ9G6WXIELdA3XZzV6ilVnWFzLj3
/E2PTchIgFk5zeyXConTNW4QIE/Robkd7DIxduVC
6C6daW+GKhFTbQFjacvr15KlRWo4/XQZ56QZAzic
pB+rRDT3dKQW
-----END CERTIFICATE REQUEST-----
```

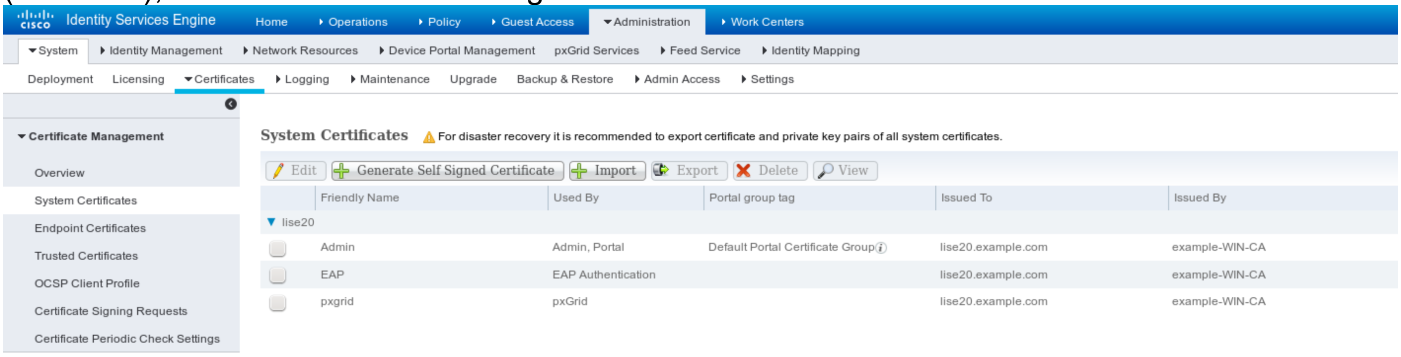
Certificate Template:

ISE-pxgrid

Additional Attributes:

Attributes:

Alla fine ISE deve avere i certificati Admin e pxGrid firmati dall'autorità di certificazione attendibile (Microsoft), come mostrato nell'immagine:

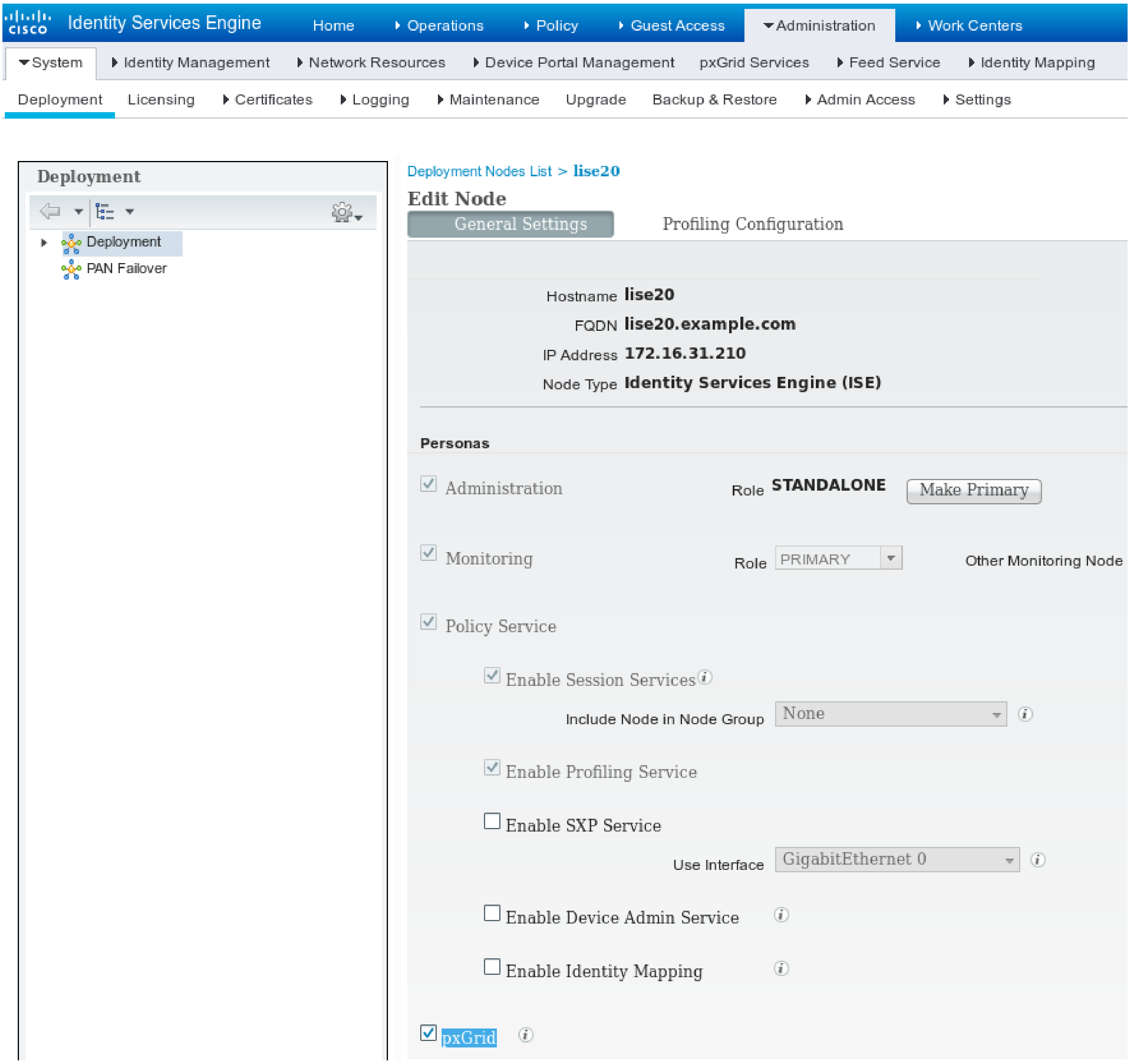


System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
▼ lise20					
□	Admin	Admin, Portal	Default Portal Certificate Group	lise20.example.com	example-WIN-CA
□	EAP	EAP Authentication		lise20.example.com	example-WIN-CA
□	pxgrid	pxGrid		lise20.example.com	example-WIN-CA

servizio pxGrid

Con i certificati corretti è necessario abilitare il ruolo pxGrid per un nodo specifico, come mostrato nell'immagine seguente:



Hostname lise20

FQDN lise20.example.com

IP Address 172.16.31.210

Node Type Identity Services Engine (ISE)

Personas

☑ Administration Role STANDALONE

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable SXP Service

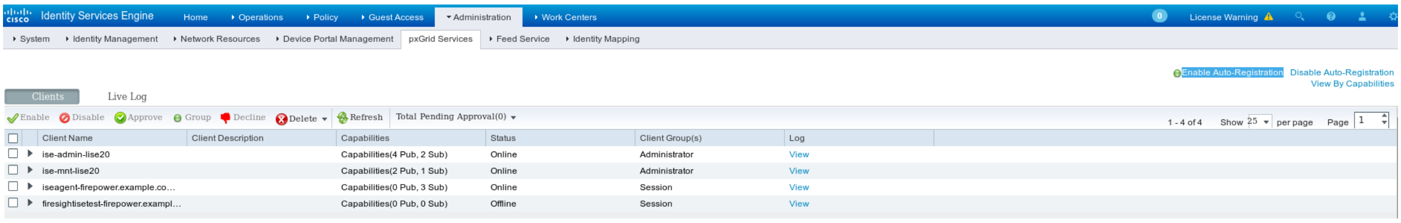
Use Interface GigabitEthernet 0

□ Enable Device Admin Service

□ Enable Identity Mapping

☑ pxGrid

L'approvazione automatica deve essere attivata:

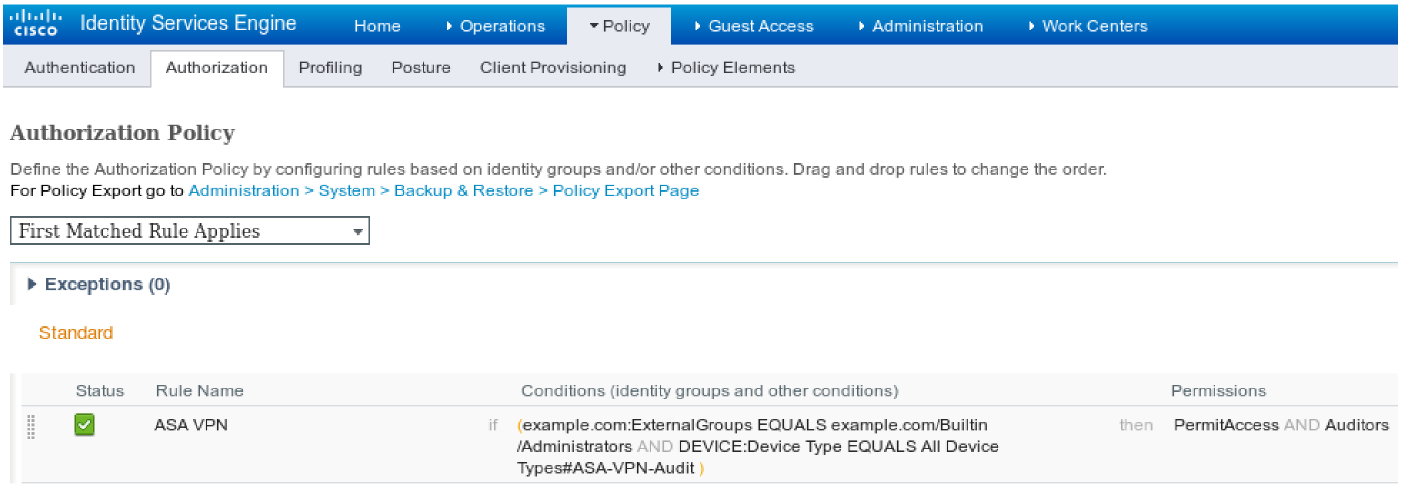


Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
ise-admin-lise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
ise-mnt-lise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
iseagent-firepower.example.co...		Capabilities(0 Pub, 3 Sub)	Online	Session	View
firesightisetest-firepower.exampl...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

Criteri di autorizzazione

Viene utilizzato il criterio di autenticazione predefinito (la ricerca di Active Directory viene eseguita se non viene trovato l'utente locale).

I criteri di autorizzazione sono stati configurati per fornire l'accesso completo alla rete (autorizzazione: PermitAccess) per gli utenti che eseguono l'autenticazione tramite ASA-VPN e appartengono al gruppo di Active Directory Administrators. Per questi utenti viene restituito il tag SGT Auditors:



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

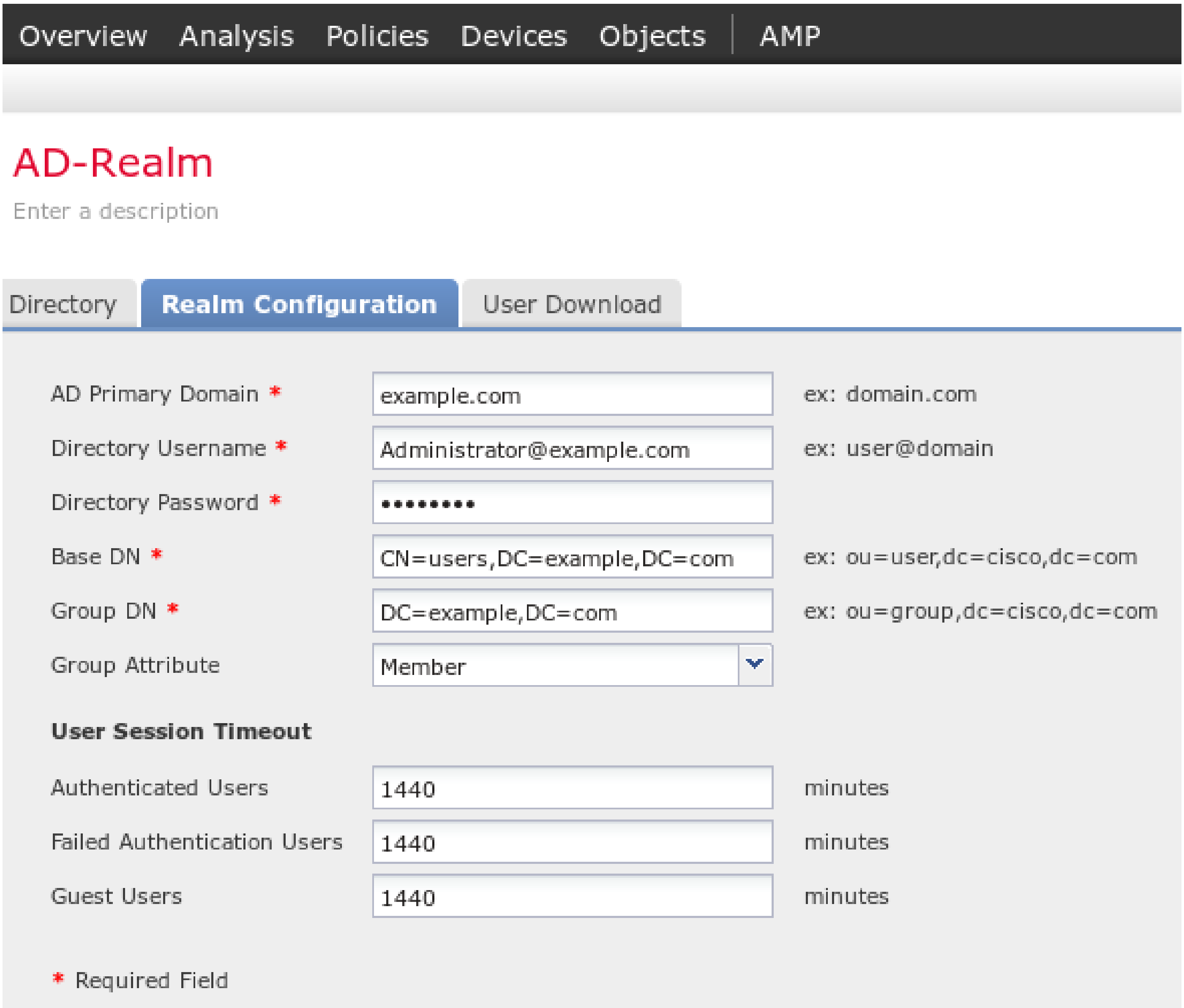
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	ASA VPN	if	(example.com:ExternalGroups EQUALS example.com/Builtin /Administrators AND DEVICE:Device Type EQUALS All Device Types#ASA-VPN-Audit)	then	PermitAccess AND Auditors

CCP

Area di autenticazione di Active Directory

La configurazione del realm è richiesta per l'integrazione con ISE (per usare le Identity Policies e recuperare l'appartenenza ai gruppi per gli utenti autenticati passivamente). È possibile configurare il realm per Active Directory o il protocollo LDAP (Lightweight Directory Access Protocol). In questo esempio viene utilizzato AD. Da **Sistema > Integrazione > Realm**:



AD-Realm

Enter a description

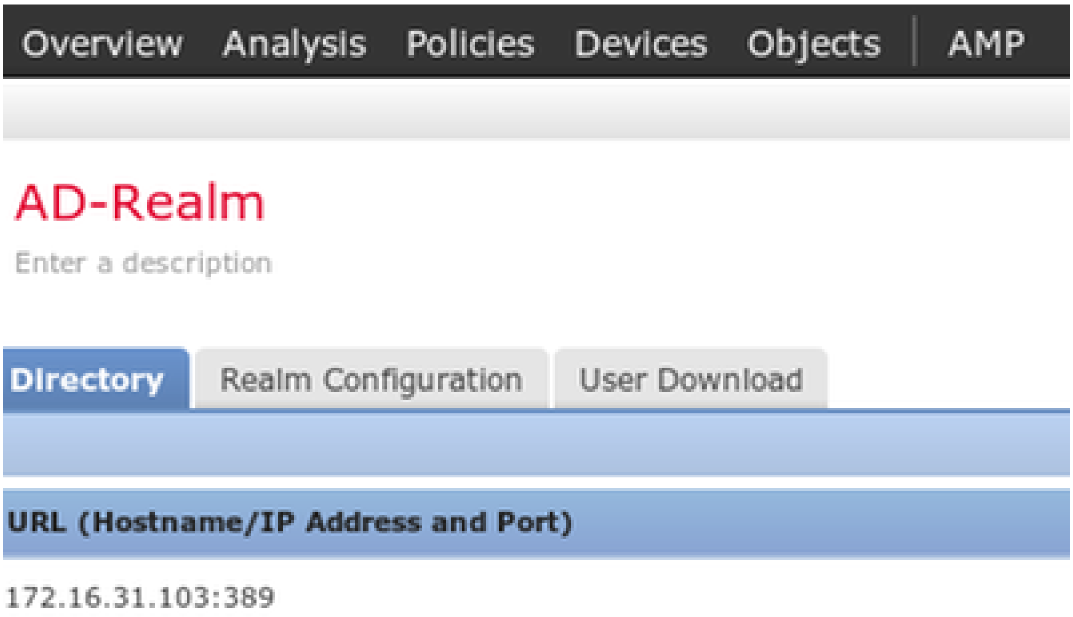
AD Primary Domain *	example.com	ex: domain.com
Directory Username *	Administrator@example.com	ex: user@domain
Directory Password *	•••••••••	
Base DN *	CN=users,DC=example,DC=com	ex: ou=user,dc=cisco,dc=com
Group DN *	DC=example,DC=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

User Session Timeout

Authenticated Users	1440	minutes
Failed Authentication Users	1440	minutes
Guest Users	1440	minutes

* Required Field

Vengono utilizzate le impostazioni di directory standard:



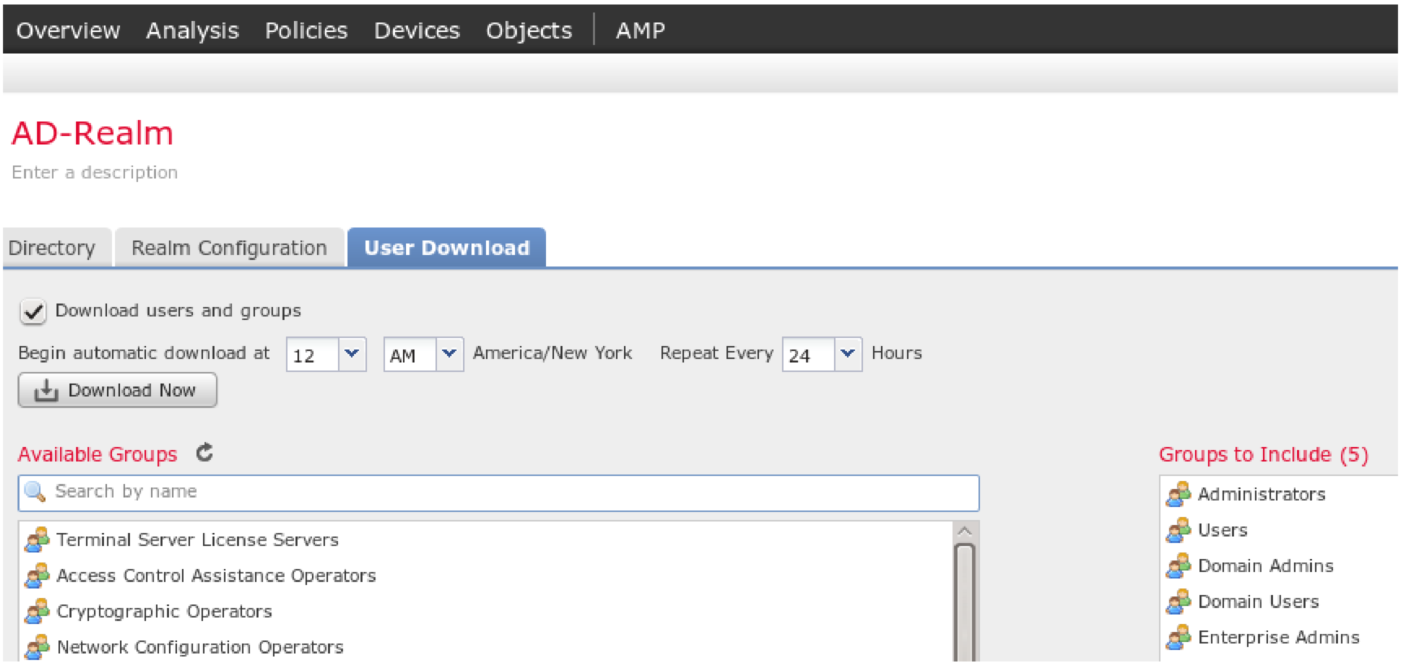
AD-Realm

Enter a description

URL (Hostname/IP Address and Port)

172.16.31.103:389

E alcuni dei gruppi AD vengono recuperati (da utilizzare come condizione aggiuntiva nelle regole di controllo di accesso):



AD-Realm

Enter a description

☑ Download users and groups

Begin automatic download at 12 AM America/New York Repeat Every 24 Hours

Available Groups

Search by name

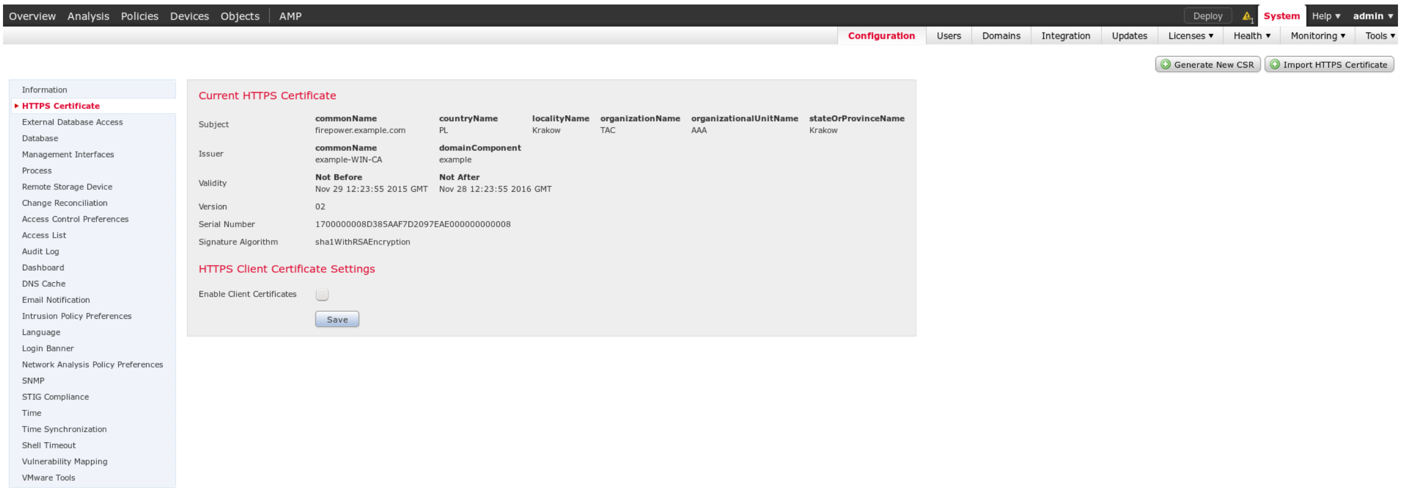
- Terminal Server License Servers
- Access Control Assistance Operators
- Cryptographic Operators
- Network Configuration Operators

Groups to Include (5)

- Administrators
- Users
- Domain Admins
- Domain Users
- Enterprise Admins

Certificati per Admin e pxGrid

Sebbene non sia necessario, è buona norma generare una CSR per l'accesso degli amministratori. Firmare il CSR utilizzando Active Directory attendibile, reimportare il certificato firmato, come illustrato nell'immagine seguente:



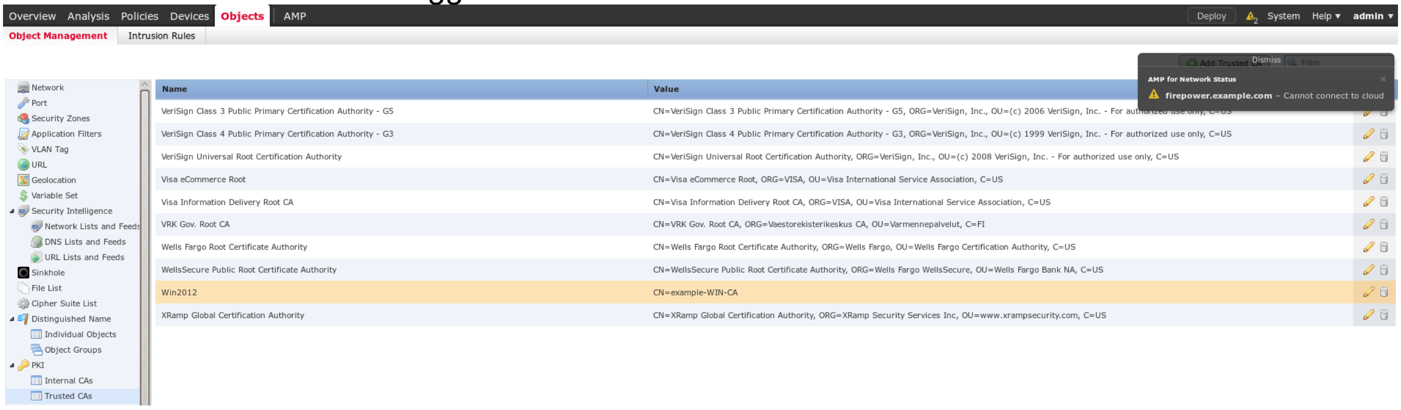
Current HTTPS Certificate

Subject	**commonName** firepower.example.com	**countryName** PL	**localityName** Krakow	**organizationName** TAC	**organizationalUnitName** AAA	**stateOrProvinceName** Krakow
Issuer	**commonName** example-WIN-CA	**domainComponent** example				
Validity	**Not Before** Nov 29 12:23:55 2015 GMT	**Not After** Nov 28 12:23:55 2016 GMT				
Version	02					
Serial Number	1700000008D385AAF7D2097EAE000000000008					
Signature Algorithm	sha1WithRSAEncryption					

HTTPS Client Certificate Settings

Enable Client Certificates □

Il certificato CA deve essere aggiunto a un archivio attendibile:



AMP for Network Status

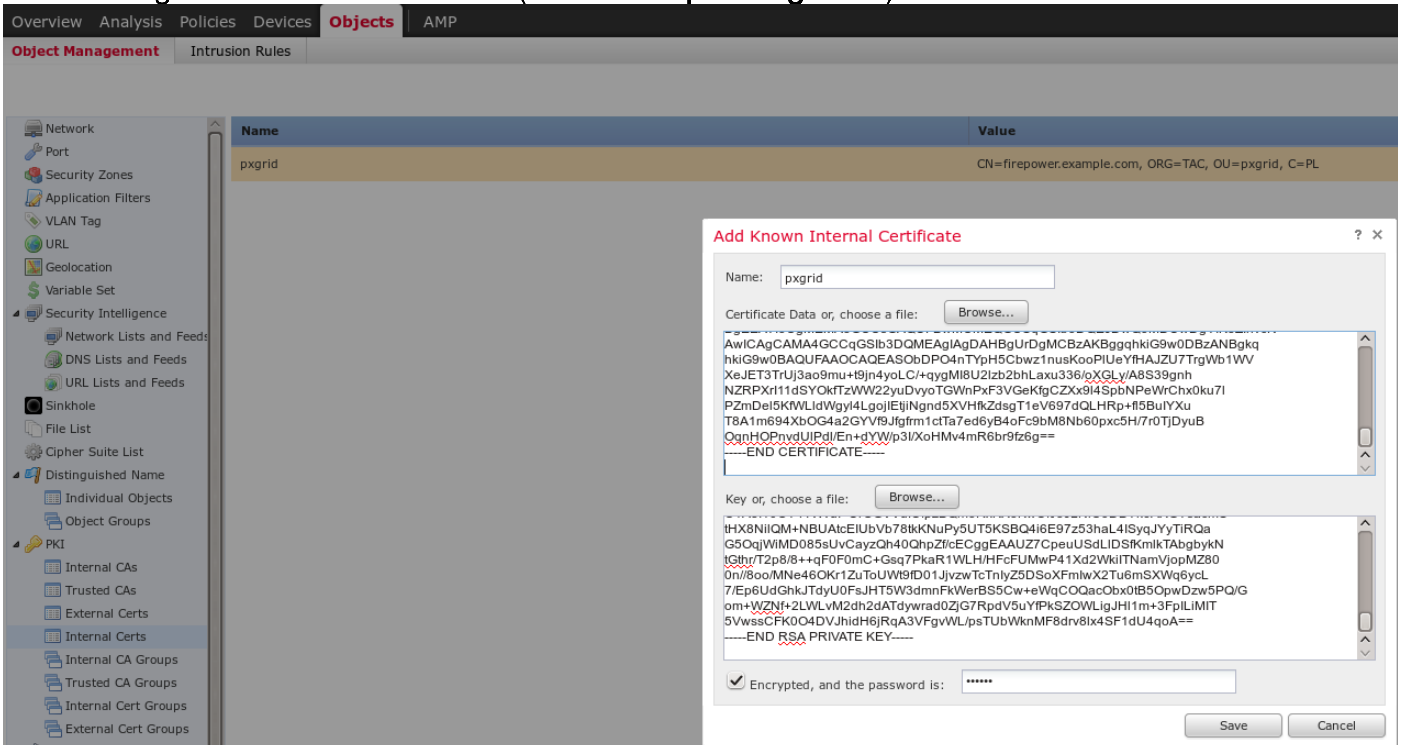
firepower.example.com – Cannot connect to cloud

Name	Value
VeriSign Class 3 Public Primary Certification Authority - G5	CN=VeriSign Class 3 Public Primary Certification Authority - G5, ORG=VeriSign, Inc., OU=(c) 2006 VeriSign, Inc. - For authorized use only, C=US
VeriSign Class 4 Public Primary Certification Authority - G3	CN=VeriSign Class 4 Public Primary Certification Authority - G3, ORG=VeriSign, Inc., OU=(c) 1999 VeriSign, Inc. - For authorized use only, C=US
VeriSign Universal Root Certification Authority	CN=VeriSign Universal Root Certification Authority, ORG=VeriSign, Inc., OU=(c) 2008 VeriSign, Inc. - For authorized use only, C=US
Visa eCommerce Root	CN=Visa eCommerce Root, ORG=VISA, OU=Visa International Service Association, C=US
Visa Information Delivery Root CA	CN=Visa Information Delivery Root CA, ORG=VISA, OU=Visa International Service Association, C=US
VRK Gov. Root CA	CN=VRK Gov. Root CA, ORG=Vaestorekisterikeskus CA, OU=Varmennepalvelut, C=FI
Wells Fargo Root Certificate Authority	CN=Wells Fargo Root Certificate Authority, ORG=Wells Fargo, OU=Wells Fargo Certification Authority, C=US
WellsSecure Public Root Certificate Authority	CN=WellsSecure Public Root Certificate Authority, ORG=Wells Fargo WellsSecure, OU=Wells Fargo Bank NA, C=US
Win2012	CN=example-WIN-CA
XRamp Global Certification Authority	CN=XRamp Global Certification Authority, ORG=XRamp Security Services Inc, OU=www.xrampsecurity.com, C=US

L'ultimo passaggio consiste nel generare il certificato pxGrid utilizzato da FMC per autorizzare il servizio ISE pxGrid. Per generare CSR è necessario utilizzare CLI (o qualsiasi altra macchina esterna con lo strumento 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:~#
```

Una volta generato fire.csr, firmarlo utilizzando Microsoft CA (modello pxGrid). Importare nuovamente la chiave privata (fire.key) e il certificato firmato (fire.pem) nell'archivio certificati interni di Gestione risorse file server. Per la chiave privata utilizzare la password impostata durante la generazione della chiave (comando **openssl genrsa**):



Name	Value
pxgrid	CN=firepower.example.com, ORG=TAC, OU=pxgrid, C=PL

Add Known Internal Certificate

Name: pxgrid

Certificate Data or, choose a file:

AwICAgCAMA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMCBzAKBggqhkiG9w0DBzANBgkq
hkiG9w0BAQUFAAOCAQEASObDPO4nTYpH5Cbwz1nusKooPlUeYfHAJZU7TrgWb1WV
XeJET3TrUj3ao9mu+t9jn4yoLC/+qygMI8U2lzb2bhLaxu336/oXGLy/A8S39gnh
NZRPXrl11dSYOkfTzWW22yuDvyoTGWnPxF3VGeKfgCZXx9l4SpbNPeWrChx0ku7I
PZmDel5KfWLldWgyl4LgojlEtjiNgnd5XVHfkZdsgT1eV697dQLHRp+fl5BuIYXu
T8A1m694XbOG4a2GYVf9Jfgfrm1ctTa7ed6yB4oFc9bM8Nb60pxc5H/7r0TjDyuB
OqnHOPnvdUIPdl/En+dYW/p3I/XoHMv4mR6br9fz6g==
-----END CERTIFICATE-----

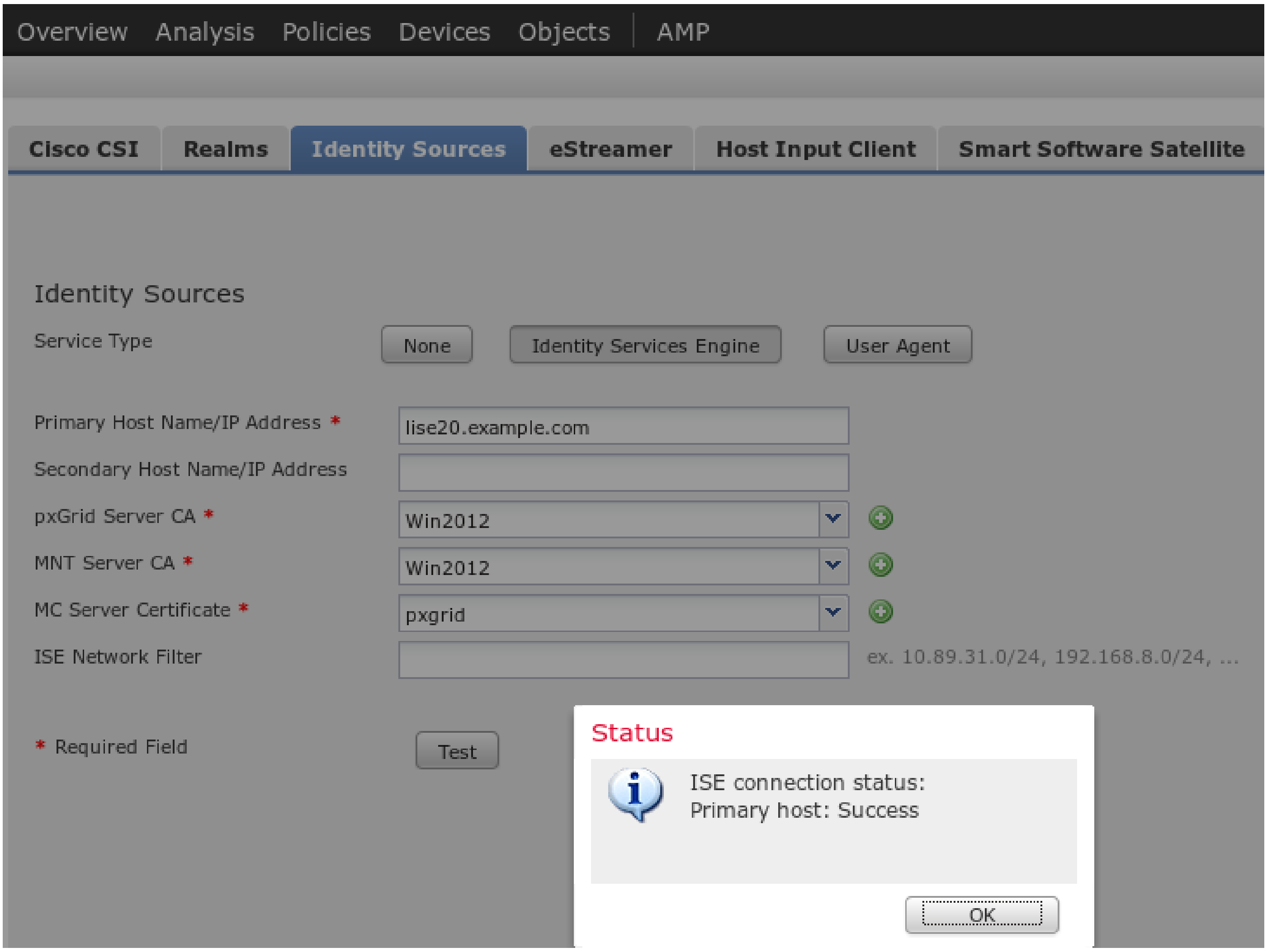
Key or, choose a file:

tHX8NiIQM+NBUAtcElUbVb78tkKNuPy5UT5KSBQ4i6E97z53haL4ISyqJYyTiRQa
G5OqjWiMD085sUvCayzQh40QhpZf/cECggEAAUZ7CpeuUSdLIDSfKmlkTAbgbykN
tGthr/T2p8/8++qF0F0mC+Gsq7PkaR1WLH/HFcFUMwP41Xd2WkiITNamVjopMZ80
0n//8oo/MNe46OKr1ZuToUWt9fD01JjvzwTcTnlyZ5DSoXFmlwX2Tu6mSXWq6ycL
7/Ep6UdGhkJTdyU0FsJHT5W3dmnFkWerBS5Cw+eWqCOQacObx0tB5OpwDzw5PQ/G
om+WZNf+2LWLvM2dh2dATdywrad0ZjG7RpdV5uYfPkSZOWLigJHl1m+3FpILiMIT
5VwssCFK0O4DVJhidH6jRqA3VFgvWL/psTUbWknMF8drv8lx4SF1dU4qoA==
-----END RSA PRIVATE KEY-----

☑ Encrypted, and the password is: •••••••

Integrazione con ISE

Una volta installati tutti i certificati, configurare l'integrazione ISE da **System > Integration**:



Identity Sources

Service Type: None | Identity Services Engine | User Agent

Primary Host Name/IP Address *: lise20.example.com

Secondary Host Name/IP Address:

pxGrid Server CA *: Win2012

MNT Server CA *: Win2012

MC Server Certificate *: pxgrid

ISE Network Filter: ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

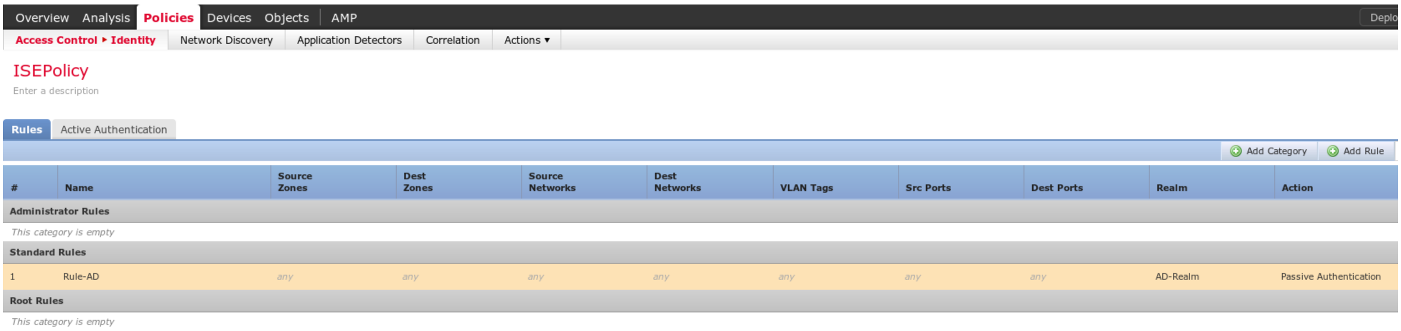
Status

ISE connection status:
Primary host: Success

Utilizzare la CA importata per la convalida dei certificati dei servizi PxGrid e MnT. Per Management Console (MC) utilizzare il certificato interno generato per pxGrid.

Criteri di identità

Configurare i criteri di identità che utilizzano il realm AD configurato in precedenza per l'autenticazione passiva:



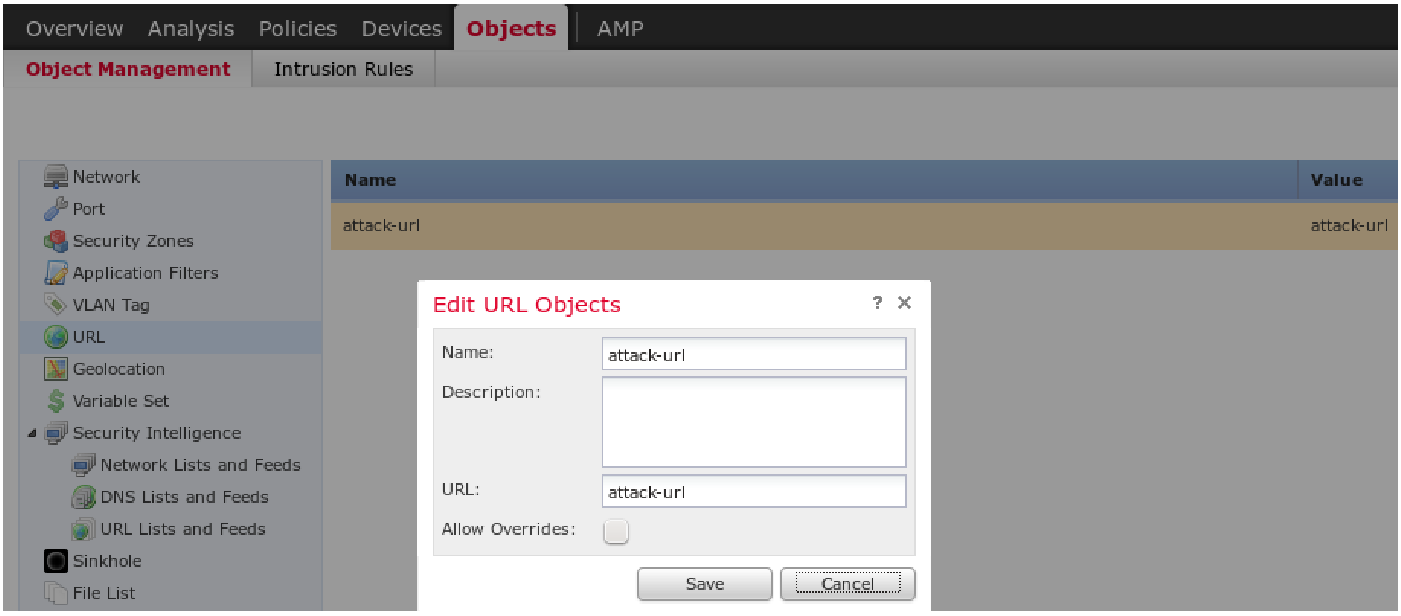
ISEPolicy

Enter a description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Src Ports	Dest Ports	Realm	Action
Administrator Rules										
This category is empty										
Standard Rules										
1	Rule-AD	any	any	any	any	any	any	any	AD-Realm	Passive Authentication
Root Rules										
This category is empty										

Policy di controllo dell'accesso

Per questo esempio è stato creato l'URL personalizzato:

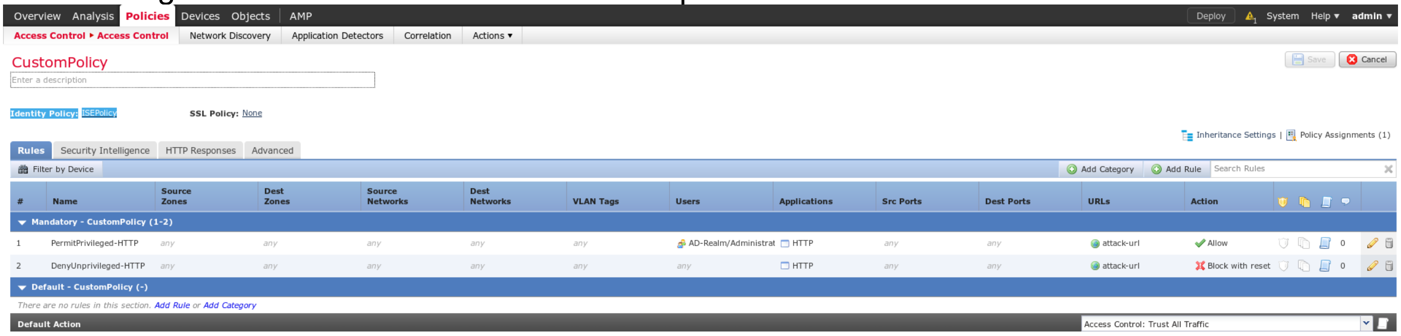


Name	Value
attack-url	attack-url

Edit URL Objects

Name:	attack-url
Description:	
URL:	attack-url
Allow Overrides:	□

E le due regole dei criteri di controllo d'accesso personalizzati:



CustomPolicy

Enter a description

Identity Policy: ISEPolicy SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action				
Mandatory - CustomPolicy (1-2)																
1	PermitPrivileged-HTTP	any	any	any	any	any	AD-Realm/Administrat	HTTP	any	any	attack-url	Allow				0
2	DenyUnprivileged-HTTP	any	any	any	any	any	any	HTTP	any	any	attack-url	Block with reset				0
Default - CustomPolicy (-)																

There are no rules in this section. Add Rule or Add Category

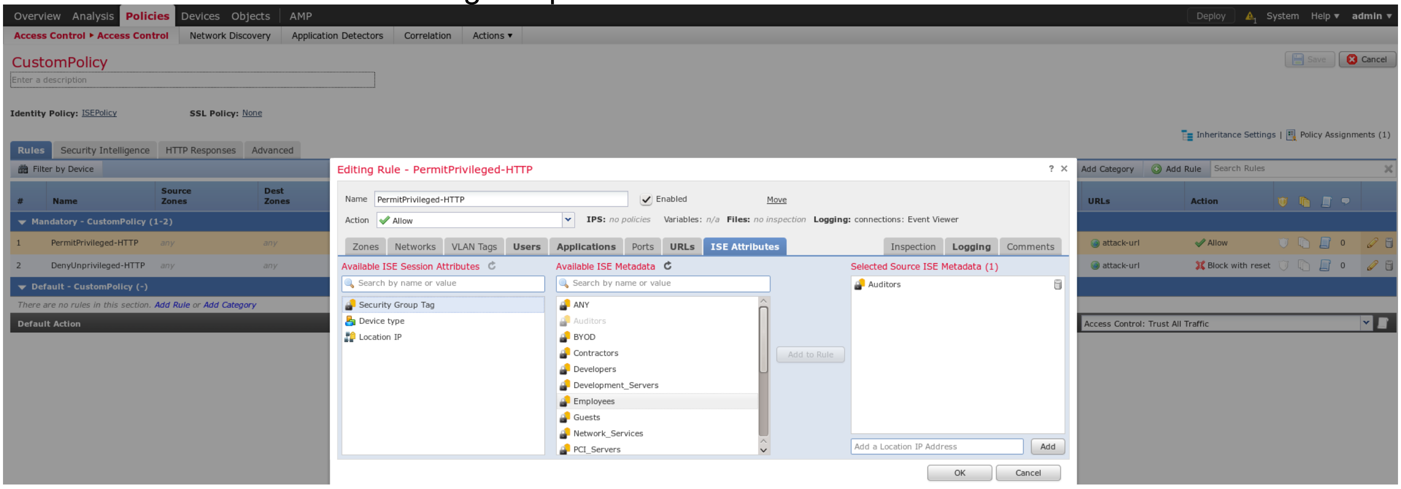
Default Action: Access Control: Trust All Traffic

La regola PermitPrivileged-HTTP consente a tutti gli utenti appartenenti al gruppo AD Administrators ai quali è stato assegnato il tag SGT. gli auditor per eseguire l'attacco HTTP su tutti gli oggetti.

DenyUnprivileged-HTTP nega tale azione a tutti gli altri utenti.

Si noti inoltre che i criteri di identità creati in precedenza sono stati assegnati a questi criteri di controllo di accesso.

In questa scheda non è possibile visualizzare i tag SGT, ma questi sono visibili durante la creazione o la modifica di una regola specifica:



Editing Rule - PermitPrivileged-HTTP

Name: PermitPrivileged-HTTP ☑ Enabled Move

Action: Allow IPS: *no policies* Variables: *n/a* Files: *no inspection* Logging: connections: Event Viewer

Available ISE Session Attributes

- Security Group Tag
- Device type
- Location IP

Available ISE Metadata

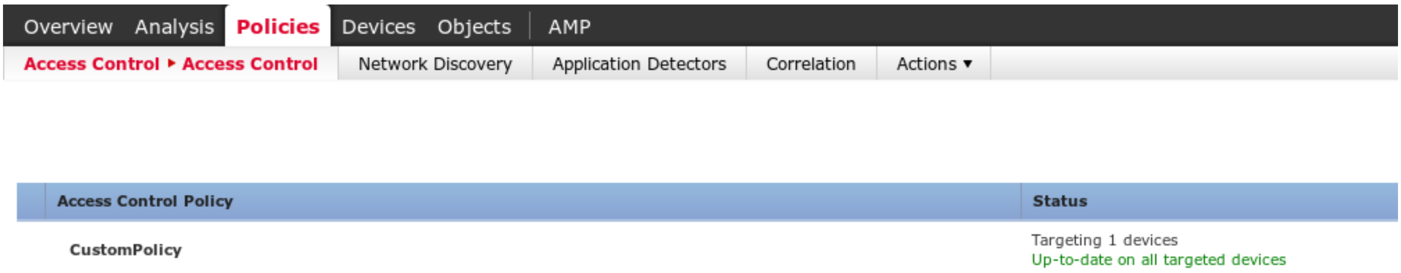
- ANY
- Auditors
- BYOD
- Contractors
- Developers
- Development_Servers
- Employees
- Guests
- Network_Services
- PCI_Servers

Selected Source ISE Metadata (1)

- Auditors

Add a Location IP Address

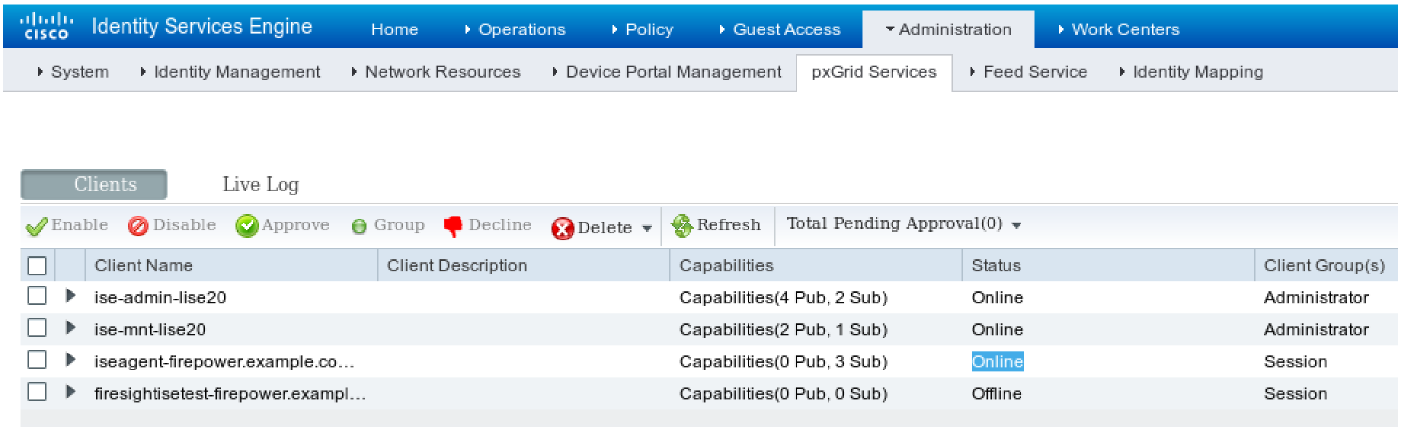
Verificare che il criterio sia assegnato al Server dei criteri di rete e che tutte le modifiche siano distribuite:



Access Control Policy	Status
CustomPolicy	Targeting 1 devices Up-to-date on all targeted devices

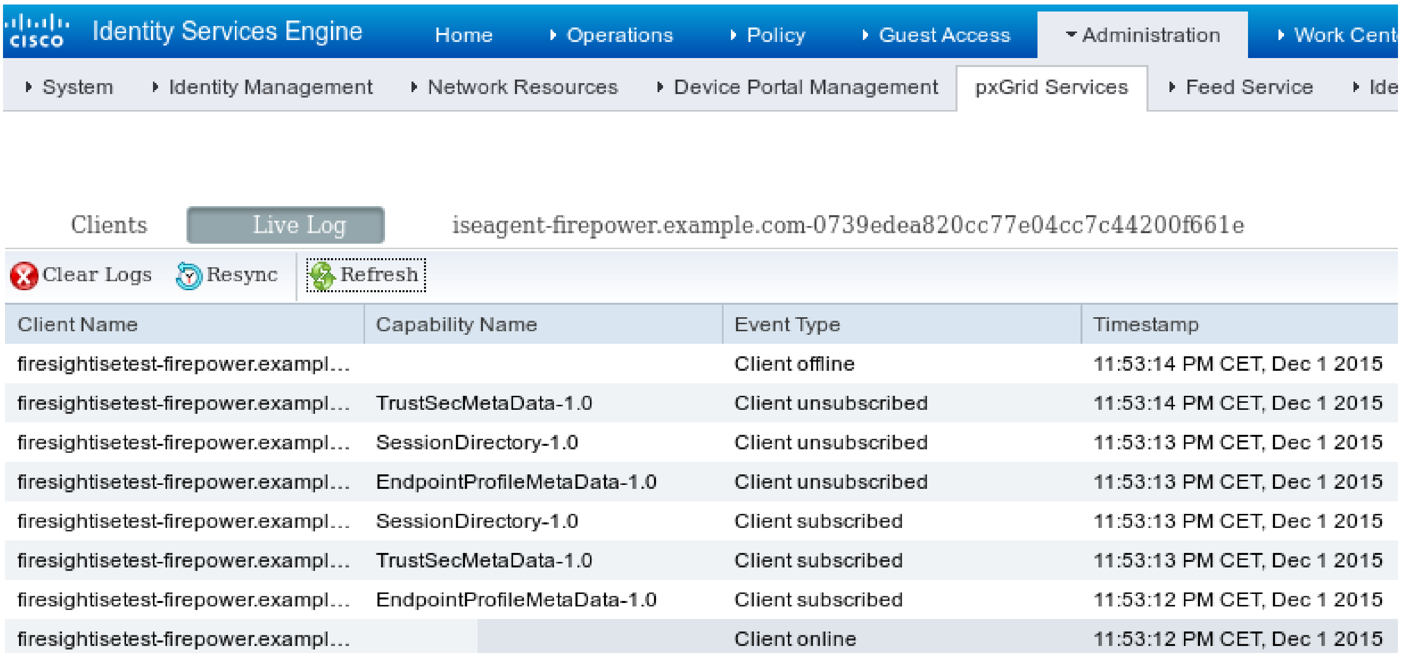
Verifica

Dopo aver configurato correttamente tutti gli elementi, ISE dovrebbe vedere il client pxGrid che si sta abbonando a un servizio di sessione (stato Online).



□	Client Name	Client Description	Capabilities	Status	Client Group(s)
□	ise-admin-lise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator
□	ise-mnt-lise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator
□	iseagent-firepower.example.co...		Capabilities(0 Pub, 3 Sub)	Online	Session
□	firesightisetest-firepower.exampl...		Capabilities(0 Pub, 0 Sub)	Offline	Session

Dai log è inoltre possibile confermare che FMC ha sottoscritto il servizio TrustSecMetaData (tag SGT) - ha ottenuto tutti i tag e ha annullato la sottoscrizione.

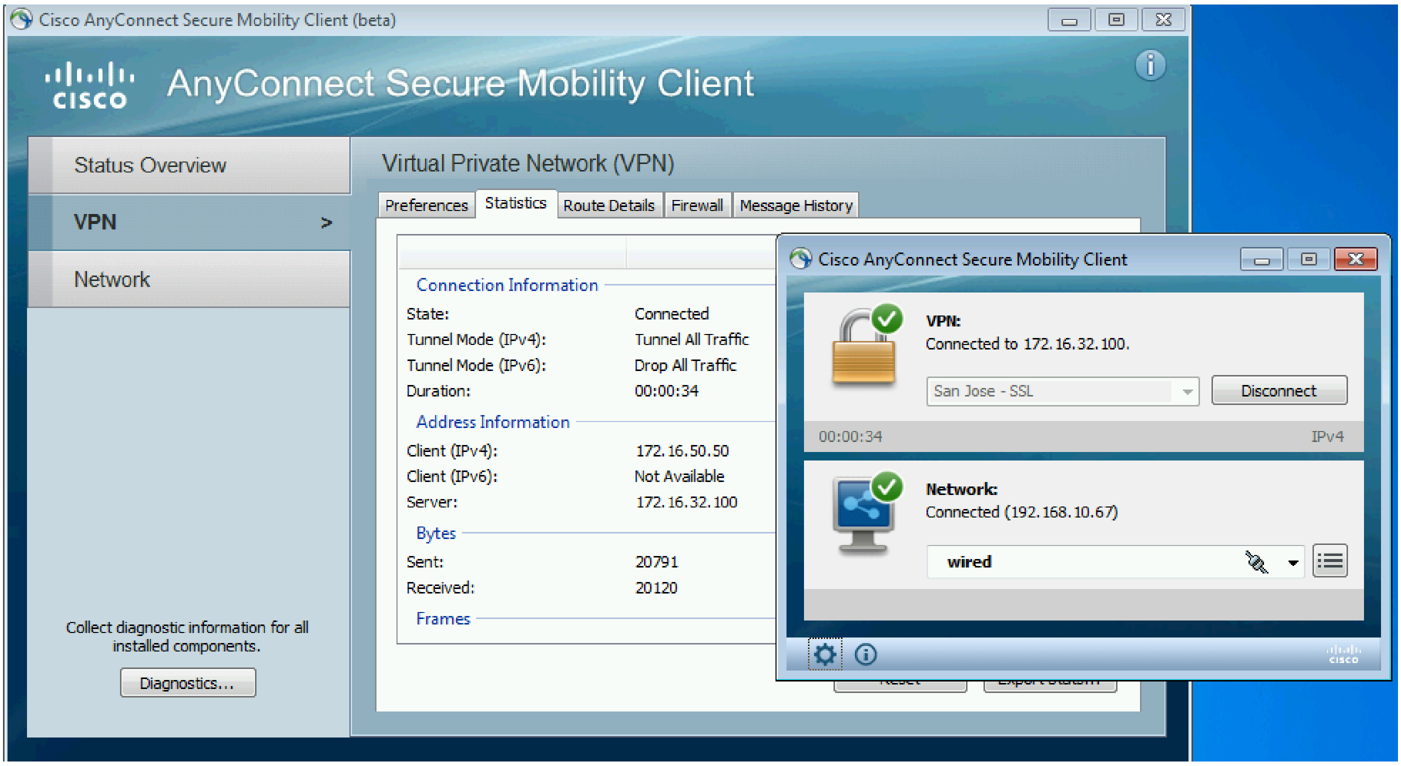


Client Name	Capability Name	Event Type	Timestamp
firesightisetest-firepower.exampl...		Client offline	11:53:14 PM CET, Dec 1 2015
firesightisetest-firepower.exampl...	TrustSecMetaData-1.0	Client unsubscribed	11:53:14 PM CET, Dec 1 2015
firesightisetest-firepower.exampl...	SessionDirectory-1.0	Client unsubscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl...	EndpointProfileMetaData-1.0	Client unsubscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl...	SessionDirectory-1.0	Client subscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl...	TrustSecMetaData-1.0	Client subscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl...	EndpointProfileMetaData-1.0	Client subscribed	11:53:12 PM CET, Dec 1 2015
firesightisetest-firepower.exampl...		Client online	11:53:12 PM CET, Dec 1 2015

Impostazione sessione VPN

Il primo test viene eseguito per uno scenario in cui l'autorizzazione su ISE non restituisce il tag SGT corretto (NGIPS non consente test di controllo).

Quando la sessione VPN è attiva, l'interfaccia utente di AnyConnect può fornire ulteriori dettagli:


Cisco AnyConnect Secure Mobility Client (beta)
AnyConnect Secure Mobility Client
Status Overview
VPN >
Network
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Diagnostics...
Cisco AnyConnect Secure Mobility Client
Disconnect

Collect diagnostic information for all installed components.

Connection Information

State: Connected
Tunnel Mode (IPv4): Tunnel All Traffic
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:00:34

Address Information

Client (IPv4): 172.16.50.50
Client (IPv6): Not Available
Server: 172.16.32.100

Bytes

Sent: 20791
Received: 20120

Frames

VPN:
Connected to 172.16.32.100.
San Jose - SSL
00:00:34 IPv4

Network:
Connected (192.168.10.67)
wired

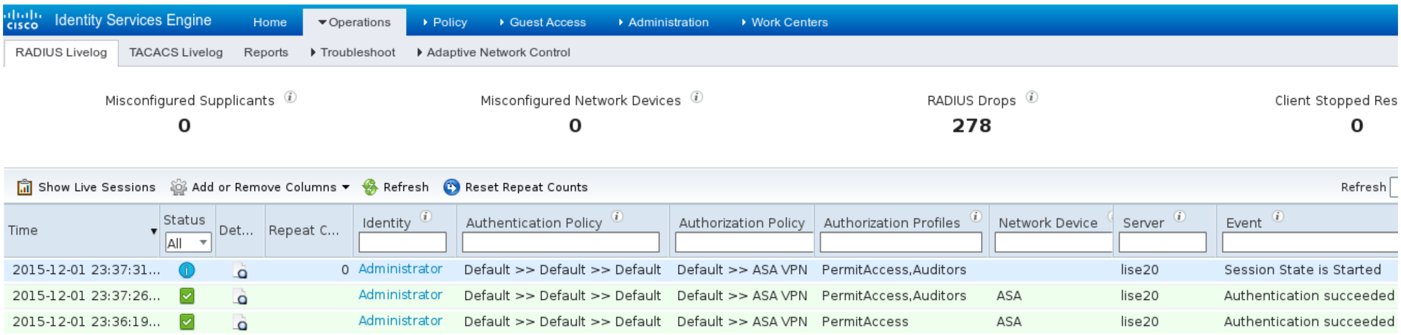
L'appliance ASA può confermare che la sessione è stata stabilita:

```
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
```

Si noti che ASA non vede alcun tag SGT restituito per questa autenticazione. L'appliance ASA non è configurata per TrustSec, quindi le informazioni verranno comunque ignorate.

Anche ISE ha reso nota la riuscita dell'autorizzazione (registro alle 23:36:19) - non è stato restituito alcun tag SGT:



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 278

Client Stopped Res 0

Time	Status All	Det...	Repeat C...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Server	Event
2015-12-01 23:37:31...	ⓘ	🔍	0	Administrator	Default >> Default >> Default	Default >> ASA VPN	PermitAccess,Auditors		lise20	Session State is Started
2015-12-01 23:37:26...	✓	🔍		Administrator	Default >> Default >> Default	Default >> ASA VPN	PermitAccess,Auditors	ASA	lise20	Authentication succeeded
2015-12-01 23:36:19...	✓	🔍		Administrator	Default >> Default >> Default	Default >> ASA VPN	PermitAccess	ASA	lise20	Authentication succeeded

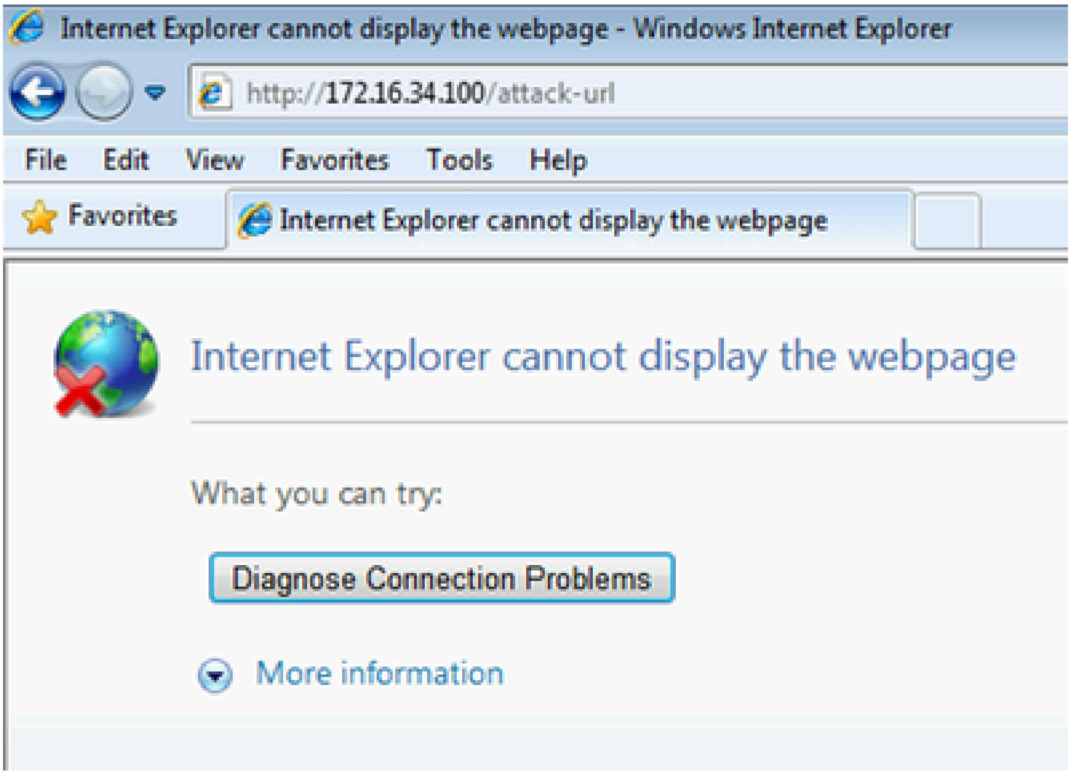
FMC: recupero dati sessione da MnT

In questa fase FMC in /var/log/messages segnala una nuova sessione (ricevuta come sottoscrittore per il servizio pxGrid) per il nome utente dell'amministratore ed esegue una ricerca AD per l'appartenenza ai gruppi:

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

Accesso di rete privilegiato e senza privilegi

Quando in questa fase l'utente tenta di aprire il browser Web e di accedere al server controllato, la connessione verrà terminata:

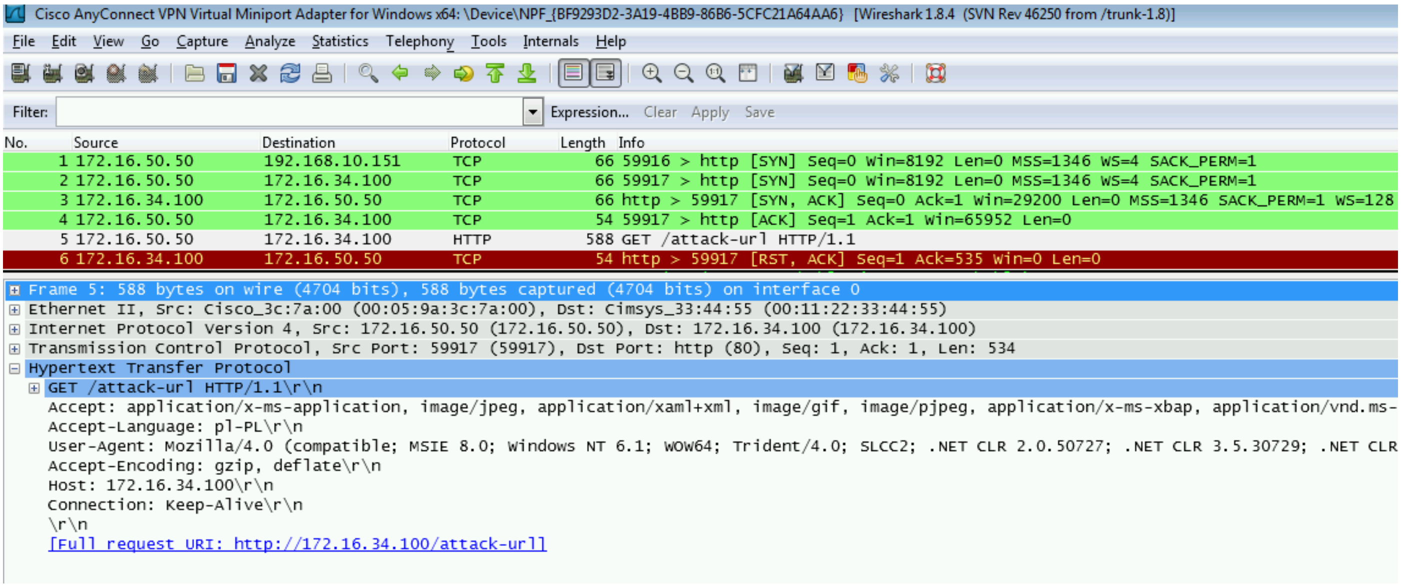

Internet Explorer cannot display the webpage - Windows Internet Explorer
http://172.16.34.100/attack-url
File
Edit
View
Favorites
Tools
Help
Favorites
Internet Explorer cannot display the webpage

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems
More information

Può essere confermato dalle acquisizioni dei pacchetti prese dal client (invio RST TCP in base alla configurazione FMC):

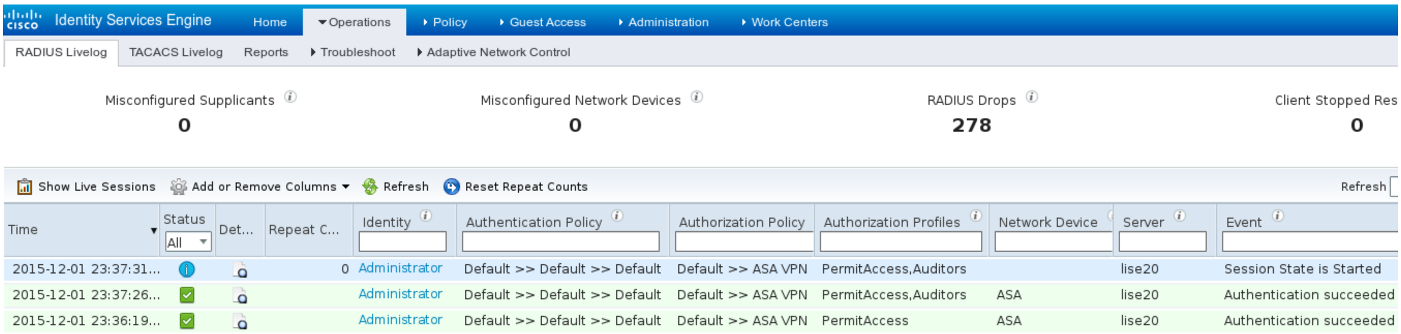

Cisco AnyConnect VPN Virtual Miniport Adapter for Windows x64: \Device\NPF_{BF9293D2-3A19-4BB9-86B6-5CFC21A64AA6} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.     Source          Destination      Protocol   Length Info
      1 172.16.50.50    192.168.10.151   TCP            66 59916 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1346 WS=4 SACK_PERM=1
      2 172.16.50.50    172.16.34.100    TCP            66 59917 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1346 WS=4 SACK_PERM=1
      3 172.16.34.100   172.16.50.50     TCP            66 http > 59917 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1346 SACK_PERM=1 WS=128
      4 172.16.50.50    172.16.34.100    TCP            54 59917 > http [ACK] Seq=1 Ack=1 Win=65952 Len=0
      5 172.16.50.50    172.16.34.100    HTTP          588 GET /attack-url HTTP/1.1
      6 172.16.34.100   172.16.50.50     TCP            54 http > 59917 [RST, ACK] Seq=1 Ack=535 Win=0 Len=0

⊞ Frame 5: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface 0
⊞ Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
⊞ Internet Protocol Version 4, Src: 172.16.50.50 (172.16.50.50), Dst: 172.16.34.100 (172.16.34.100)
⊞ Transmission Control Protocol, Src Port: 59917 (59917), Dst Port: http (80), Seq: 1, Ack: 1, Len: 534
⊟ Hypertext Transfer Protocol
  ⊞ GET /attack-url HTTP/1.1\r\n
    Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-
    Accept-Language: pl-PL\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
    Accept-Encoding: gzip, deflate\r\n
    Host: 172.16.34.100\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://172.16.34.100/attack-url]
```

Una volta che ISE è configurato per la restituzione, la sessione ASA con tag di revisione riporta:

```
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
```

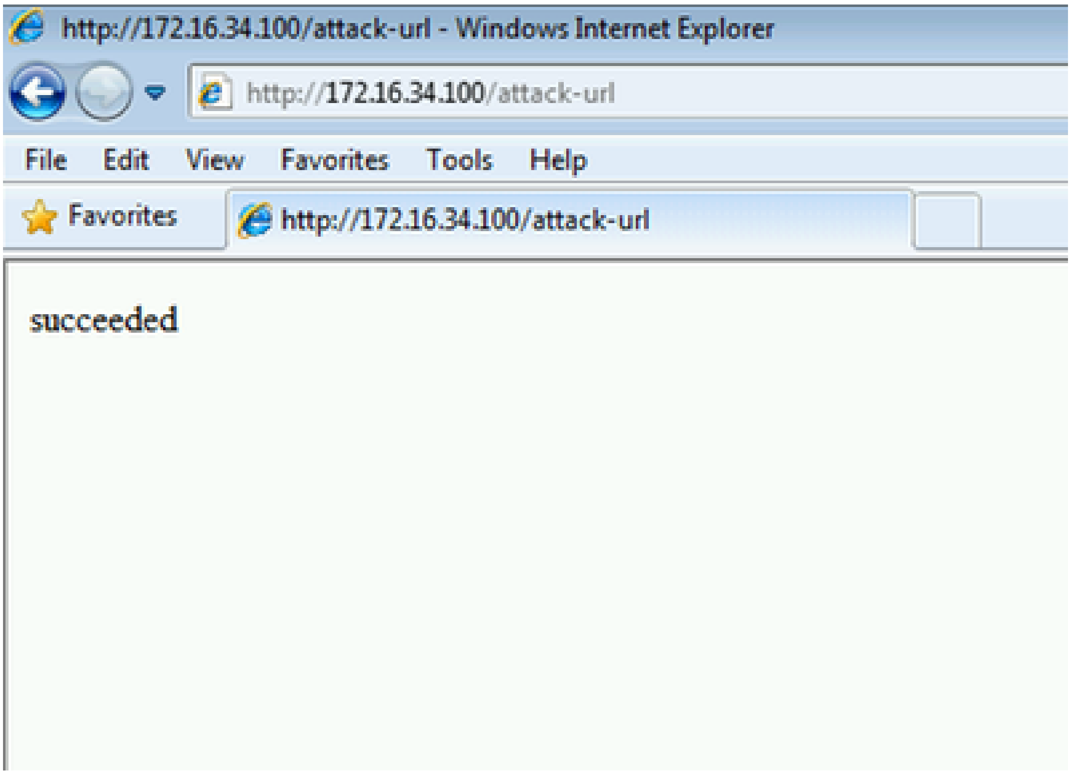
Anche ISE segnala un'autorizzazione riuscita (il log alle 23:37:26) - SGT tag Auditor viene restituito:



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Res
0	0	278	0

Time	Status	Det...	Repeat C...	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Server	Event
	All									
2015-12-01 23:37:31...	ⓘ		0	Administrator	Default >> Default >> Default	Default >> ASA VPN	PermitAccess,Auditors		lise20	Session State is Started
2015-12-01 23:37:26...	✓			Administrator	Default >> Default >> Default	Default >> ASA VPN	PermitAccess,Auditors	ASA	lise20	Authentication succeeded
2015-12-01 23:36:19...	✓			Administrator	Default >> Default >> Default	Default >> ASA VPN	PermitAccess	ASA	lise20	Authentication succeeded

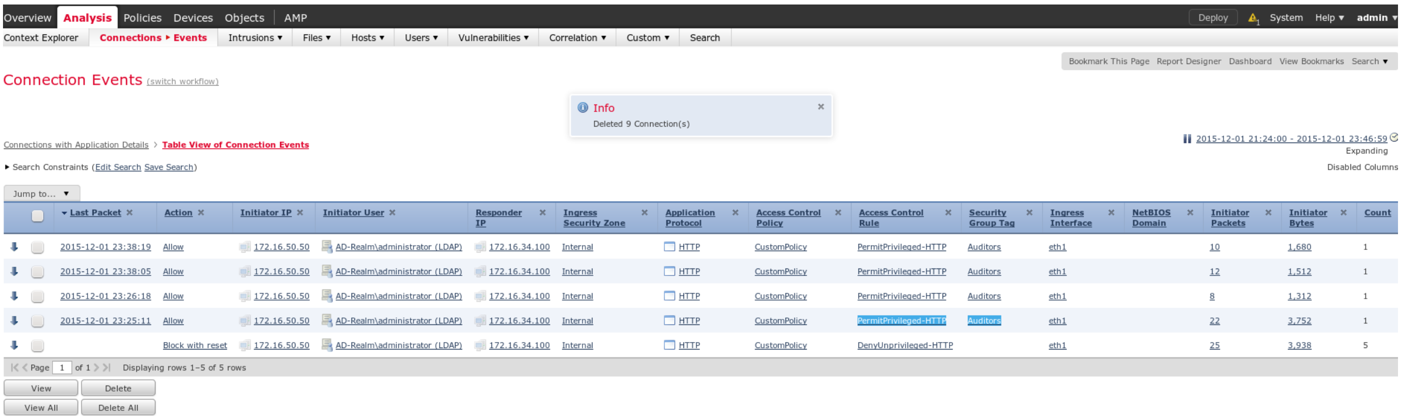
L'utente può accedere al servizio:


http://172.16.34.100/attack-url - Windows Internet Explorer
http://172.16.34.100/attack-url
File
Edit
View
Favorites
Tools
Help
Favorites
http://172.16.34.100/attack-url

succeeded

Accesso registrazione FMC

Questa attività può essere confermata dal report Evento di connessione:



Connection Events (switch workflow)

Info
Deleted 9 Connection(s)

Connections with Application Details > Table View of Connection Events

2015-12-01 21:24:00 - 2015-12-01 23:46:59
Expanding

▸ Search Constraints (Edit Search Save Search)

Disabled Columns

	□	Last Packet	Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Application Protocol	Access Control Policy	Access Control Rule	Security Group Tag	Ingress Interface	NetBIOS Domain	Initiator Packets	Initiator Bytes	Count
⬇	□	2015-12-01 23:38:19	Allow	172.16.50.50	AD-Realm\administrator (LDAP)	172.16.34.100	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors	eth1		10	1,680	1
⬇	□	2015-12-01 23:38:05	Allow	172.16.50.50	AD-Realm\administrator (LDAP)	172.16.34.100	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors	eth1		12	1,512	1
⬇	□	2015-12-01 23:26:18	Allow	172.16.50.50	AD-Realm\administrator (LDAP)	172.16.34.100	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors	eth1		8	1,312	1
⬇	□	2015-12-01 23:25:11	Allow	172.16.50.50	AD-Realm\administrator (LDAP)	172.16.34.100	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors	eth1		22	3,752	1
⬇	□		Block with reset	172.16.50.50	AD-Realm\administrator (LDAP)	172.16.34.100	Internal	HTTP	CustomPolicy	DenyUnprivileged-HTTP		eth1		25	3,938	5

Page 1 of 1 Displaying rows 1–5 of 5 rows

Innanzitutto, all'utente non è stato assegnato alcun tag SGT ed è stata raggiunta la regola DenyUnprivileged-HTTP. Dopo che il tag del revisore è stato assegnato dalla regola ISE (e recuperato dalla FMC), viene utilizzato PermitPrivileged-HTTP e l'accesso è consentito.

Si noti inoltre che, per visualizzare la barra, sono state rimosse più colonne, in quanto normalmente la regola di controllo di accesso e il tag del gruppo di protezione vengono visualizzati come una delle ultime colonne (è necessario utilizzare una barra di scorrimento orizzontale). La vista personalizzata può essere salvata e riutilizzata in futuro.

Risoluzione dei problemi

Debug FMC

Per controllare i log del componente adi responsabile dei servizi di identità, controllare il file /var/log/messages:

```
[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
```

Per ottenere debug più dettagliati, è possibile terminare il processo adi (dalla radice dopo sudo) ed eseguirlo con l'argomento debug:

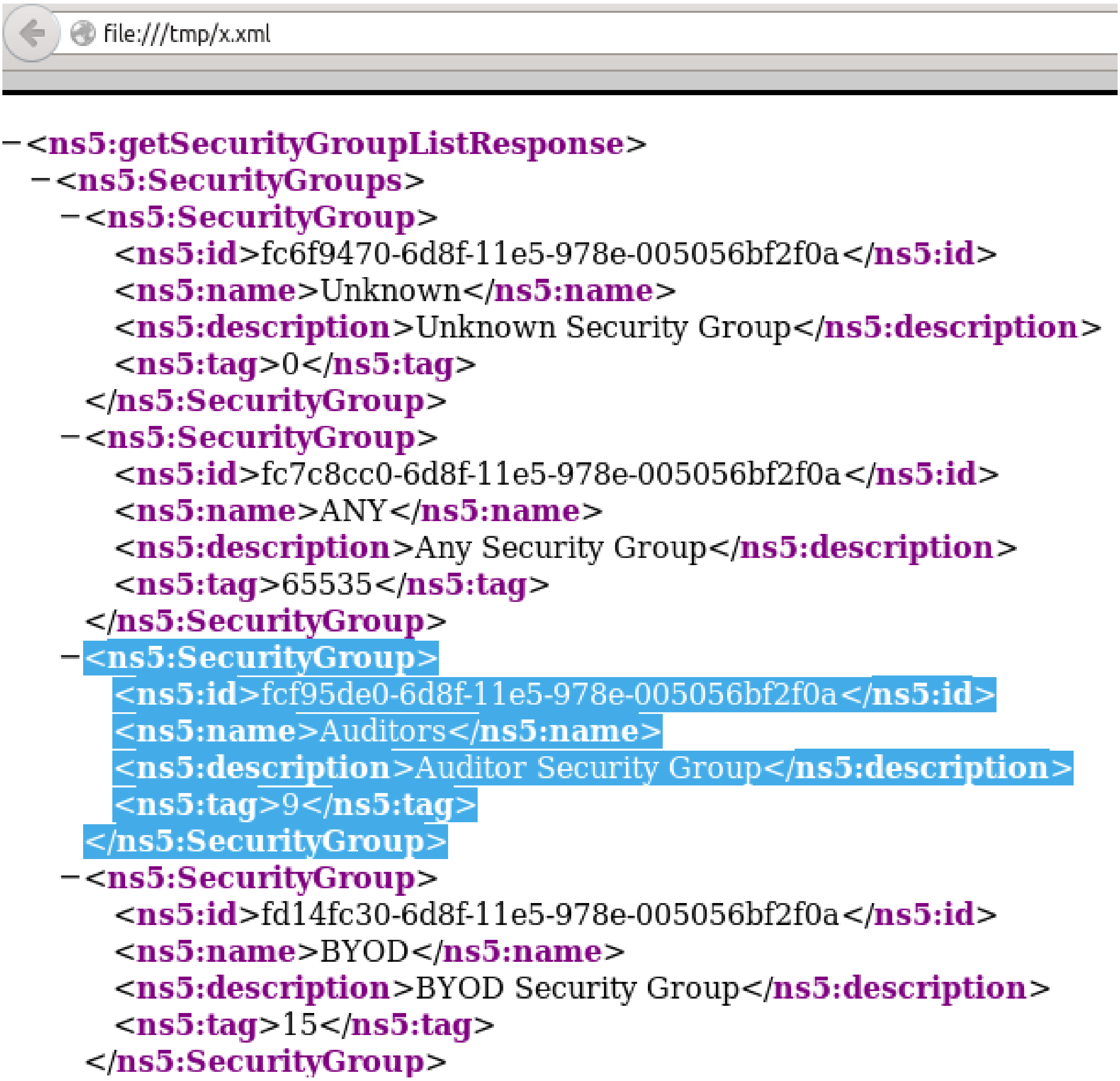
```
root@firepower:/var/log# ps ax | grep adi
24047 ?        Sl     0:00 /usr/local/sf/bin/adi
24090 pts/0    S+     0:00 grep adi
root@firepower:/var/log# kill -9 24047
root@firepower:/var/log# /usr/local/sf/bin/adi --debug
Dec 01 23:14:34 firepower SF-IMS[24106]: [24106] ADI:adi.Adi [DEBUG] adi.cpp:319:HandleLog():
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.......>
```

Query SGT tramite pxGrid

L'operazione viene eseguita quando si fa clic sul pulsante **Test** nella sezione **ISE Integration** o quando l'elenco SGT viene aggiornato, durante l'aggiunta della regola in Access Control Policy.

```
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>]
```

Per una migliore visualizzazione, il contenuto XML di tale registro può essere copiato nel file xml e aperto da un browser Web. È possibile confermare la ricezione di un SGT (audit) specifico e di tutti gli altri SGT definiti su 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>
```

Query di sessione su MnT tramite API REST

Anche questo fa parte dell'operazione di test (notare che il nome host e la porta MnT vengono passati tramite pxGrid). Viene utilizzato il download in blocco della sessione:

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK, p_node*:0x7f0ea6ffa8a8(<session
xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime
xmlns='http://www.cisco.com/pxgrid'>2015-12-
01T23:37:31.191+01:00</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt
tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-
Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E
6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceMgmtIntfID></deviceAttachPt
></interface><user><name
xmlns='http://www.cisco.com/pxgrid'>Administrator</name><ADUserDNSDomain>example.com</ADUserDNSD
omain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfi
le>Windows7-Workstation</endpointProfile><securityGroup>Auditors</securityGroup></session>)]
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.ISEConnection [DEBUG]
adi.cpp:319:HandleLog(): bulk download invoking callback on entry# 1
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.ISESessionEntry [DEBUG]
adi.cpp:319:HandleLog(): parsing Session Entry with following text:<session
xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime
xmlns='http://www.cisco.com/pxgrid'>2015-12-
01T23:37:31.191+01:00</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt
tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-
Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E
6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceMgmtIntfID></deviceAttachPt
></interface><user><name
xmlns='http://www.cisco.com/pxgrid'>Administrator</name><ADUserDNSDomain>example.com</ADUserDNSD
omain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfi
le>Windows7-Workstation</endpointProfile><securityGroup>Auditors</securityGroup></session>
```

Risultato analizzato (1 sessione attiva ricevuta):

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.ISESessionEntry [DEBUG]
adi.cpp:319:HandleLog(): Parsing incoming DOM resulted in following ISESessionEntry:
{gid = ac101f6400007000565d597f, timestamp = 2015-12-01T23:37:31.191+01:00,
state = Started, session_id = 91200007, nas_ip = 172.16.31.100,
mac_addr = 08:00:27:23:E6:F2, ip = 172.16.50.50, user_name = Administrator,
sgt = Auditors, domain = example.com, device_name = Windows7-Workstation}
```

In questa fase NGIPS tenta di correlare il nome utente (e il dominio) con il nome utente Realm-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
```

LDAP viene utilizzato per trovare l'appartenenza di un utente e di un gruppo:

```
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.
```

Debug ISE

Dopo aver abilitato il debug a livello di TRACCIA per il componente pxGrid, è possibile controllare ogni operazione (ma senza payload/dati come su FMC).

Esempio di recupero del tag 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

CSCuv3295 - ISE potrebbe inviare informazioni sul dominio nei campi del nome utente

CSCus53796 - Impossibile ottenere il nome di dominio completo dell'host per la query di massa REST

CSCuv43145 - Riavvio del servizio di mapping PXGRID & Identity, importazione/eliminazione dell'archivio trust

Riferimenti

- Configurazione dei servizi di monitoraggio e aggiornamento con ISE e FirePower Integration
- Configurazione di pxGrid in un ambiente ISE distribuito
- Procedure relative alla distribuzione dei certificati con Cisco PxGrid: Configurazione di ISE pxGrid Node e client pxGrid con firma CA
- Integrazione di ISE versione 1.3 pxGrid con l'applicazione IPS pxLog
- Guida dell'amministratore di Cisco Identity Services Engine, versione 2.0
- Guida di riferimento all'API Cisco Identity Services Engine, versione 1.2 - Introduzione al servizio RESTful...
- Guida di riferimento all'API di Cisco Identity Services Engine, versione 1.2 - Introduzione alla risoluzione dei problemi di monitoraggio...
- Guida dell'amministratore di Cisco Identity Services Engine, versione 1.3
- Documentazione e supporto tecnico - Cisco Systems