身份服務的ISE和FirePOWER整合故障排除

目錄

簡介

本文檔介紹如何在思科下一代入侵防禦系統(NGIPS)上配置並排除TrustSec感知策略故障。NGIPS版本6.0支援與身份服務引擎(ISE)整合，允許構建基於身份感知的策略。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Adaptive Security Appliance(ASA)VPN配置
- Cisco AnyConnect Security Mobility Solution — 遠端存取
- Cisco FirePower管理中心基本配置
- Cisco ISE配置
- Cisco TrustSec解決方案

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7
- Microsoft Windows 2012證書頒發機構(CA)
- Cisco ASA版本9.3
- Cisco ISE軟體版本1.4
- Cisco AnyConnect安全行動化使用者端版本4.2
- Cisco FirePower管理中心(FMC)版本6.0
- Cisco FirePower NGIPS版本6.0

設定

FirePower管理中心(FMC)是FirePower的管理平台。與ISE整合相關的功能有兩種：

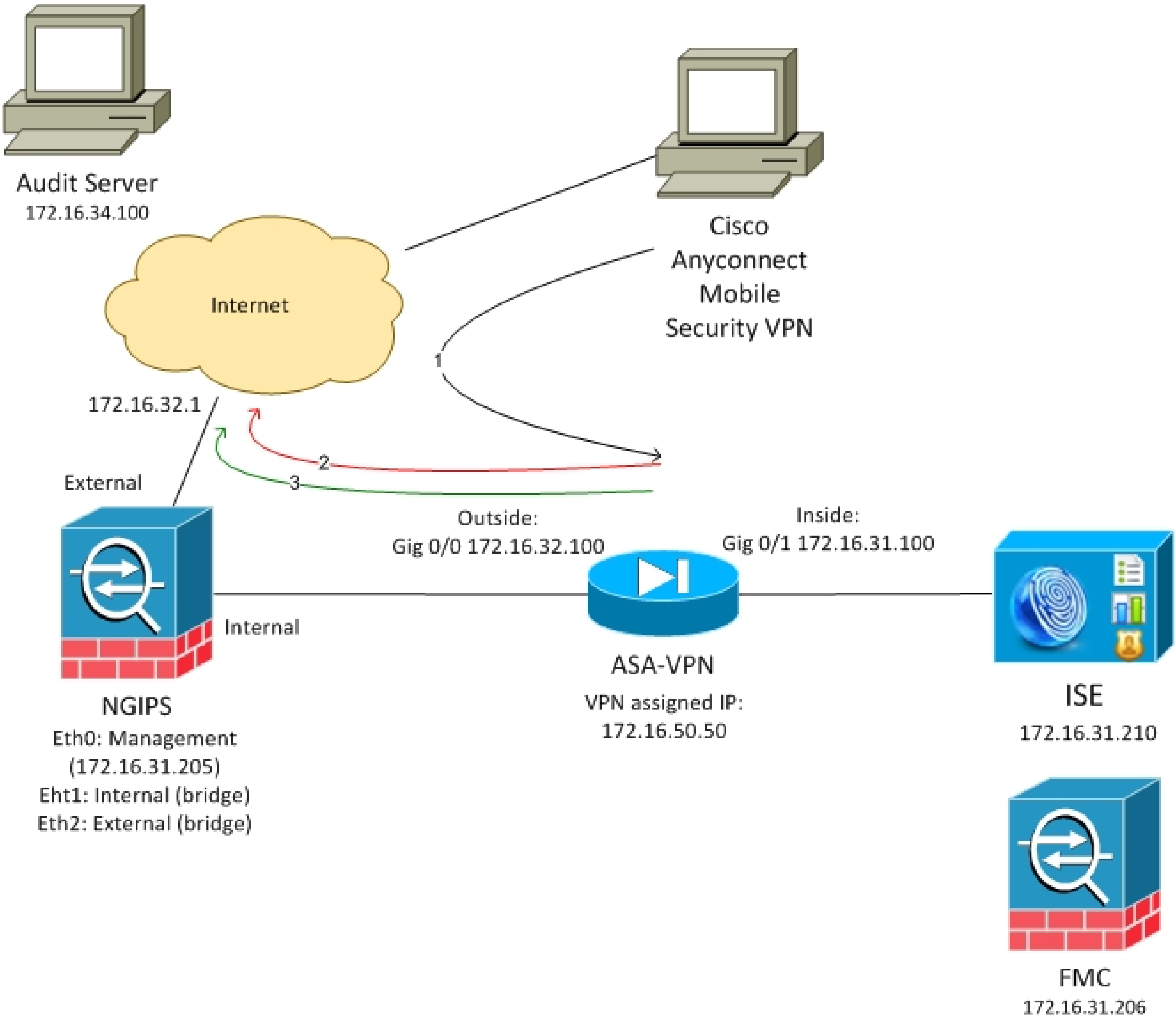
- 補救 — 允許FMC通過ISE隔離攻擊者，ISE動態更改訪問裝置的授權狀態，從而提供有限的網路訪問。此解決方案分為兩代：

1. 使用終端保護服務(EPS)API呼叫到ISE的傳統perl指令碼。
2. 使用對ISE的pxGrid協定呼叫的較新模組（此模組僅在5.4版中受支援 — 在6.0版中不受支援，在6.1版中規劃了本機支援）。

- 策略 — 允許FMC基於TrustSec安全組標籤(SGT)配置策略。

本文重點介紹第二個功能。有關補救示例，請閱讀參考部分

網路圖表



FMC配置了包含兩個規則的訪問控制策略：

- 使用自訂URL(attack-url)拒絕HTTP流量
- 允許具有自定義URL(attack-url)的HTTP流量，但前提是使用者由ISE分配到Audit(9)SGT標籤

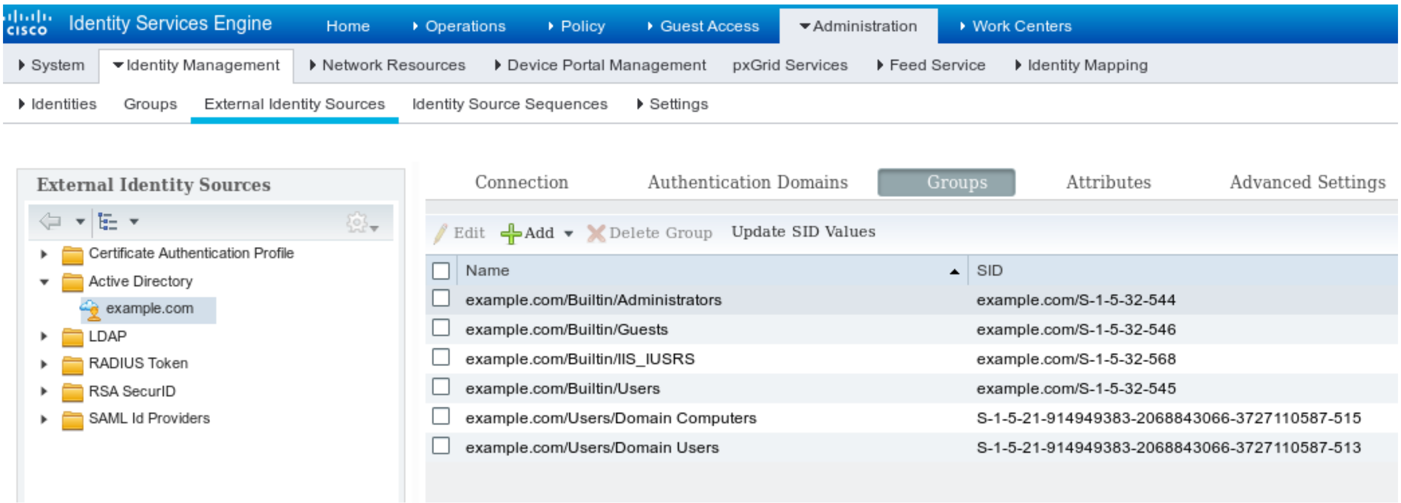
ISE決定為屬於管理員組並使用ASA-VPN裝置進行網路訪問的所有Active Directory使用者分配稽核標籤。

使用者通過ASA上的VPN連線訪問網路。然後，使用者嘗試使用URL攻擊URL訪問已稽核伺服器 — 但由於未將其分配給Audit SGT組而失敗。一旦修復，連線就會成功。

ISE

Active Directory

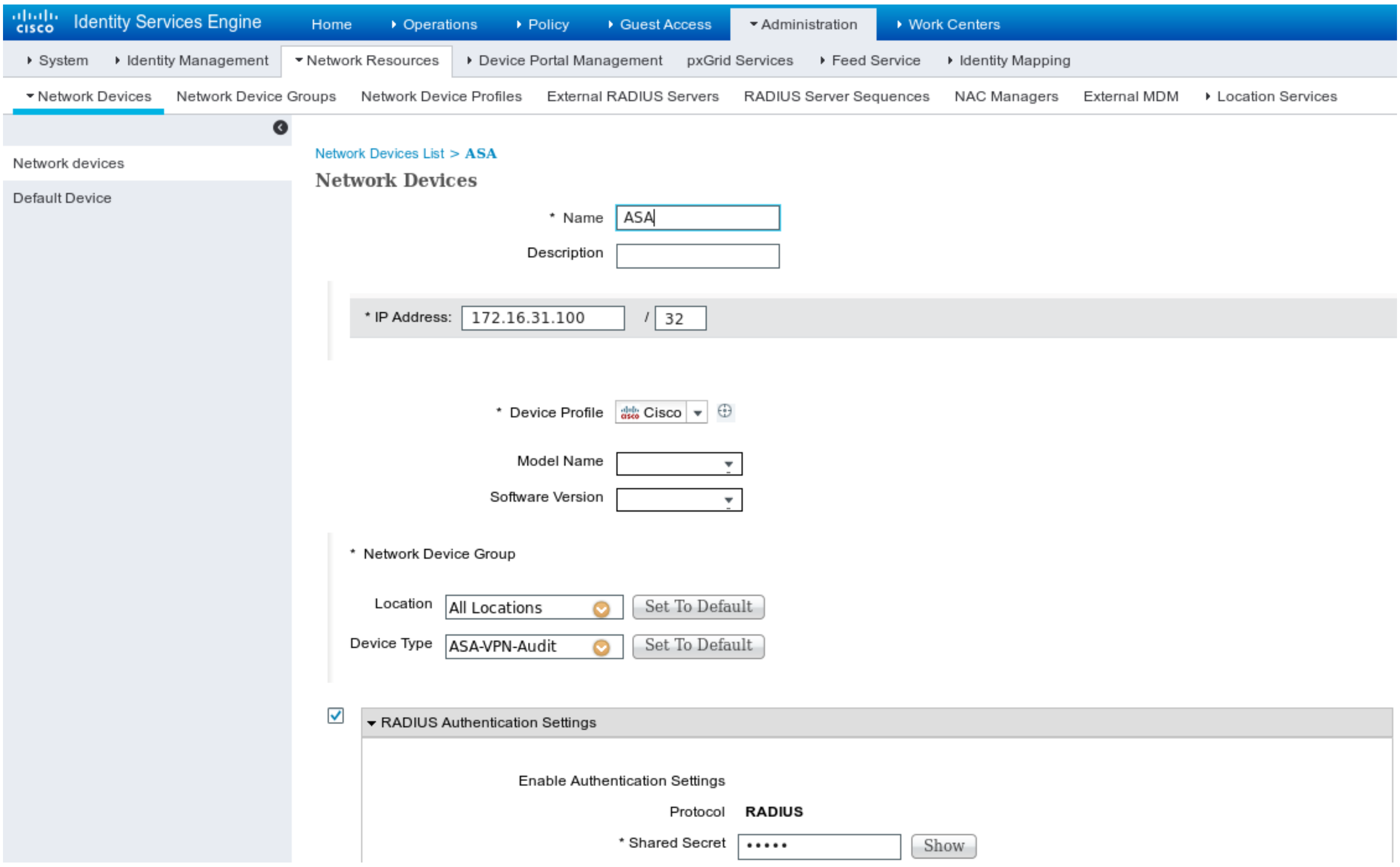
必須配置AD整合並提取正確的組（Administrators組用於授權規則條件）：



	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

網路存取裝置

ASA新增為網路裝置。使用自定義組ASA-VPN-Audit，如下圖所示：



* 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: •••••

pxGrid和MnT的證書

FMC在ISE上使用兩種服務：

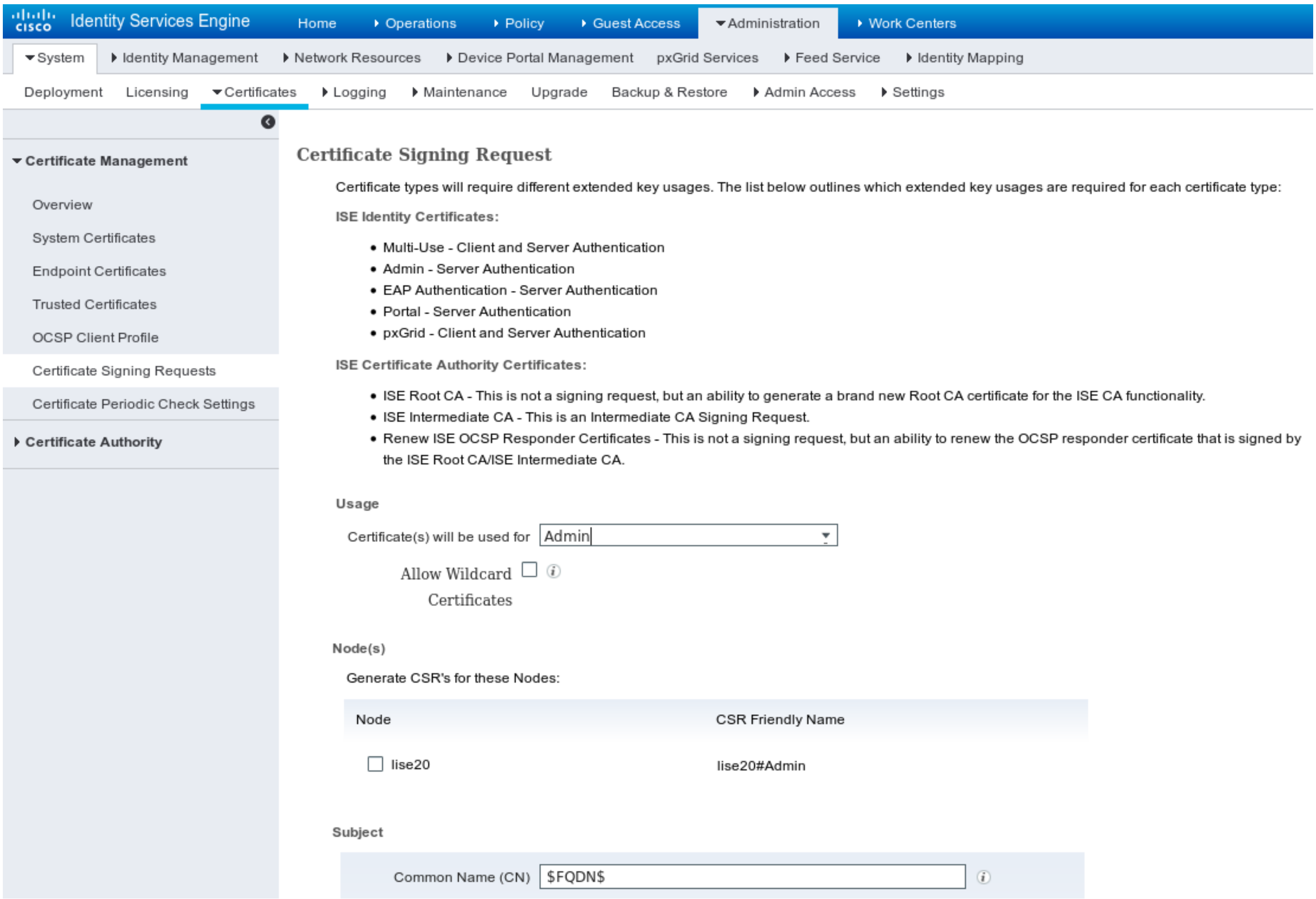
- 用於SGT和分析資料查詢的pxGrid
- 用於批次會話下載的監控和報告(MnT)

MnT可用性非常重要，因為通過這種方式通知FMC什麼是已驗證會話的IP地址，以及它的使用者名稱和SGT標籤。在此基礎上，可以應用正確的策略。請注意，NGIPS不像ASA一樣支援本地SGT標籤（內聯標籤）。但與ASA相反，它支援SGT名稱而非僅數字。

由於這些要求，ISE和FMC需要相互信任服務（證書）。 MnT僅使用伺服器端證書，pxGrid同時使用客戶端和伺服器端證書。

Microsoft CA用於對所有證書進行簽名。

對於MnT（管理員角色），ISE必須生成證書簽名請求(CSR)，如下圖所示：



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

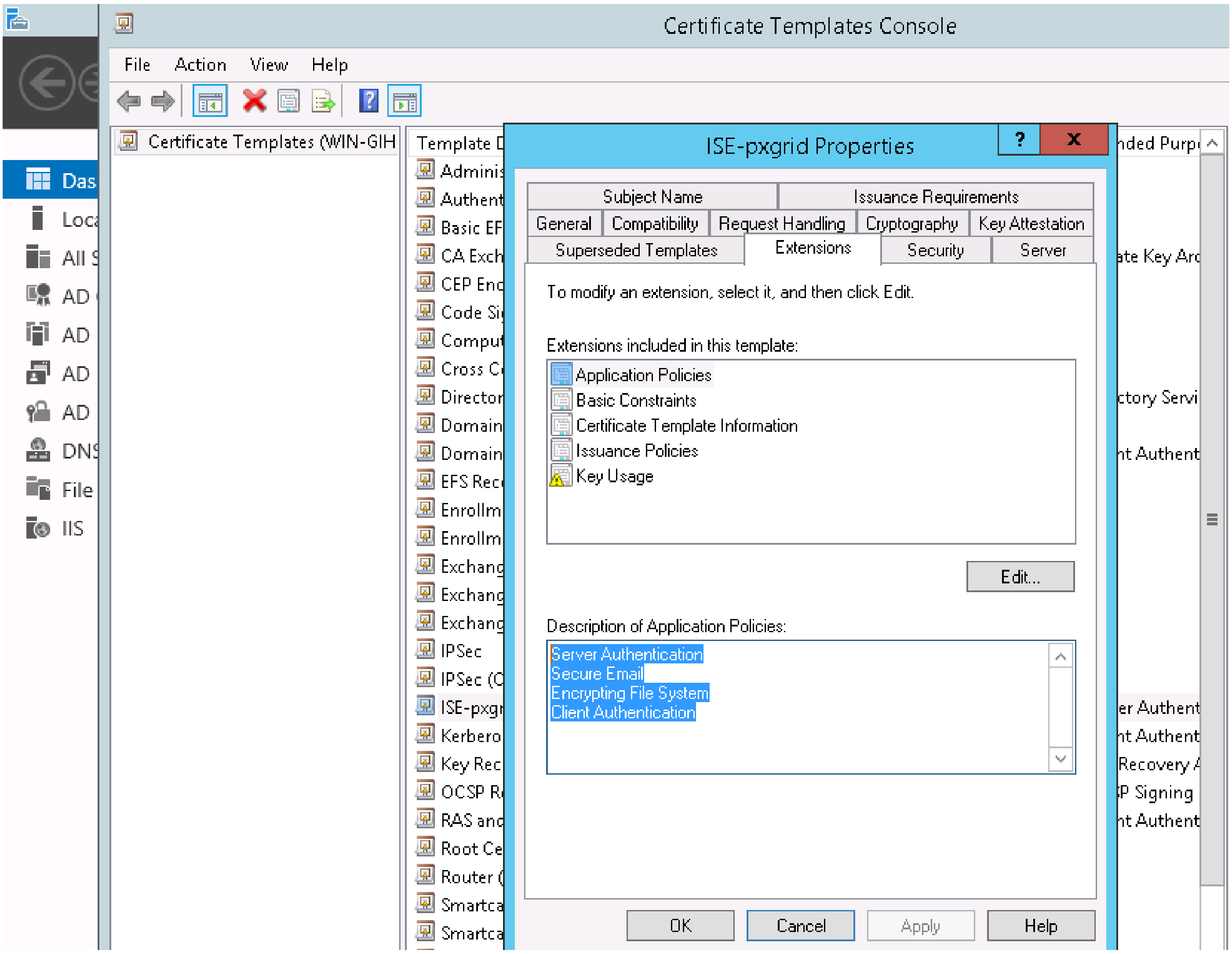
Subject

Common Name (CN): $FQDN$

經過Microsoft CA簽名後，必須通過「繫結證書」 **選項匯入**證書。
對於pxGrid服務必須遵循類似的過程。 **將用於pxGrid選項的**證書必須選中。
由於不能有兩個具有相同使用者名稱的證書，因此完全可以為OU或O部分新增不同的值（例如pxGrid）。

> **附註**：請確保為ISE和FMC的每個完全限定域名(FQDN)在DNS伺服器上配置正確的DNS記錄。

Admin證書和pxGrid證書的唯一區別在於簽名過程。因為pxGrid證書必須具有客戶端和伺服器身份驗證的擴展金鑰使用選項在Microsoft CA上的自定義模板可用於以下用途：



ISE-pxgrid Properties

Subject Name | Issuance Requirements | General | Compatibility | Request Handling | Cryptography | Key Attestation | Superseded Templates | Extensions | Security | Server

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

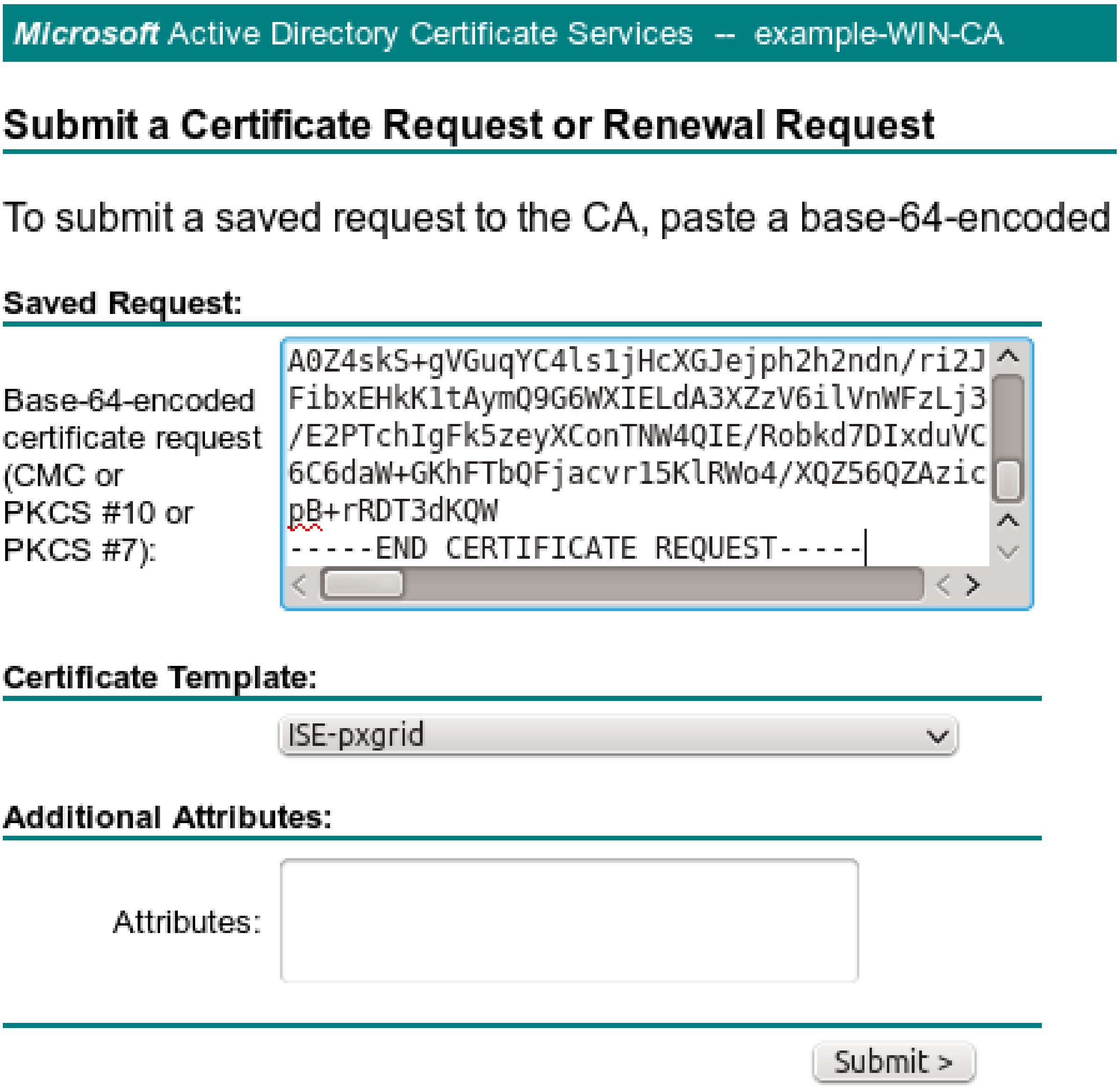
Edit...

Description of Application Policies:

Server Authentication
Secure Email
Encrypting File System
Client Authentication

OK Cancel Apply Help

如何使用Microsoft Web服務對pxGrid CSR進行簽名，如下圖所示：



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-----
```

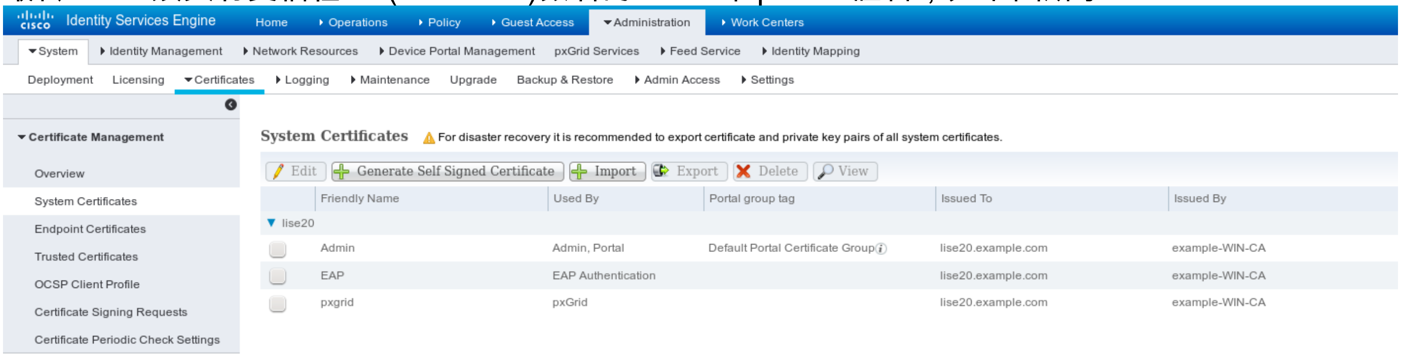
Certificate Template:

ISE-pxgrid

Additional Attributes:

Attributes:

最終ISE必須具有受信任CA(Microsoft)簽名的Admin和pxGrid證書，如下圖所示：

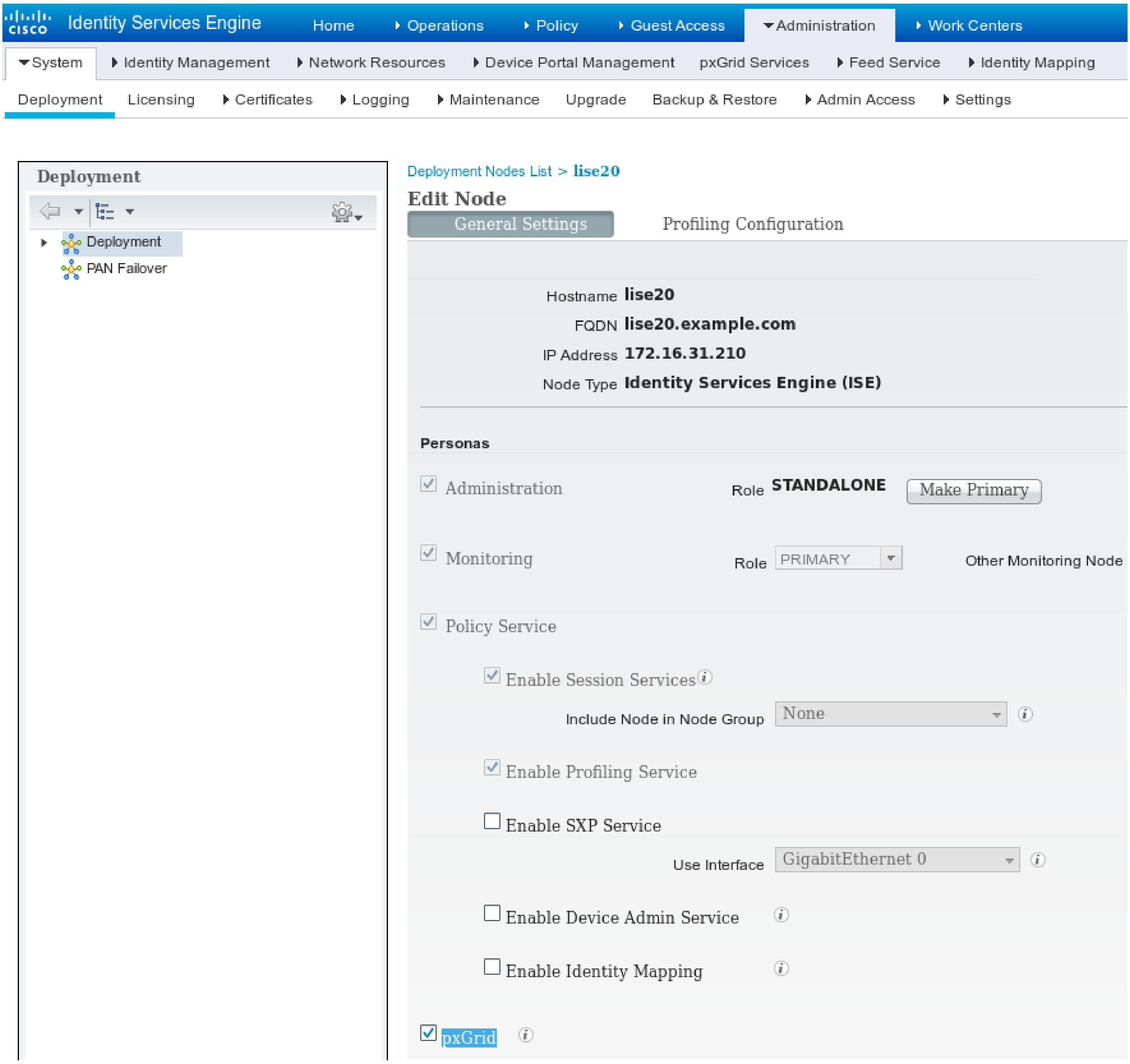


System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	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

pxGrid服務

必須啟用特定節點的正確證書pxGrid角色，如下圖所示：



Deployment Nodes List > lise20

Edit Node

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

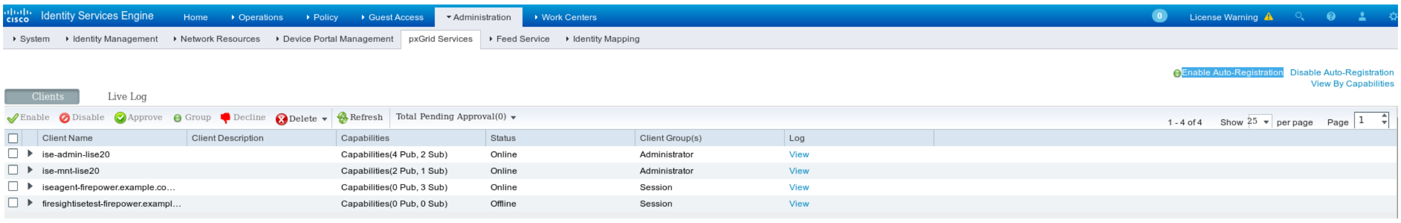
Use Interface GigabitEthernet 0

□ Enable Device Admin Service

□ Enable Identity Mapping

☑ pxGrid

並且自動批准必須設定為啟用：

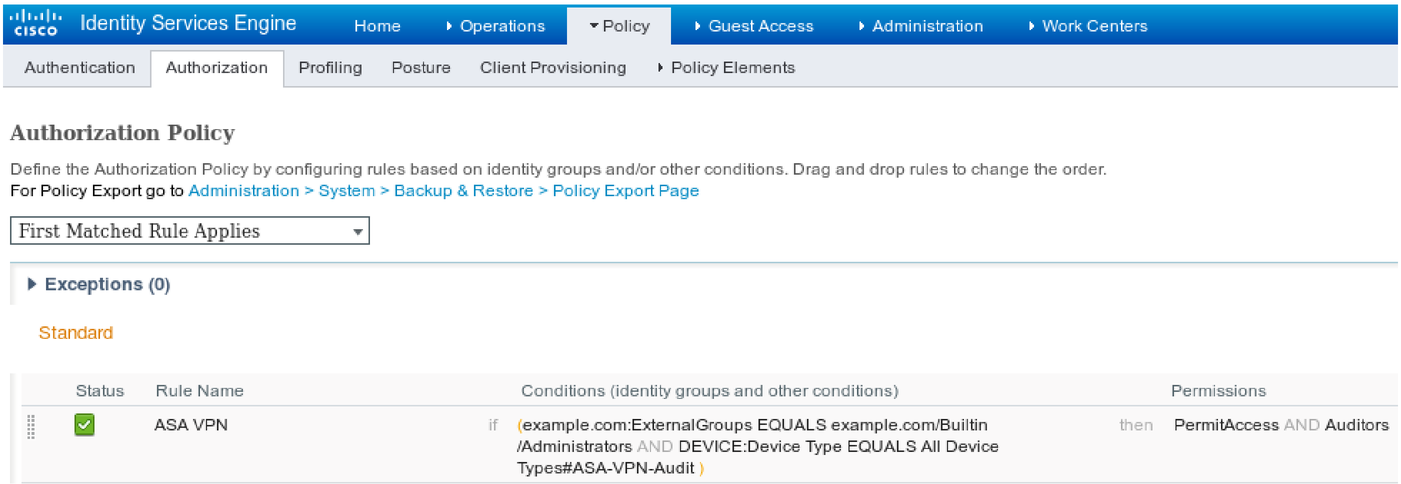


	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-lise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-lise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	iseagent-firepower.example.co...		Capabilities(0 Pub, 3 Sub)	Online	Session	View
□	firesightisetest-firepower.exampl...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

授權策略

使用預設身份驗證策略（如果找不到本地使用者，則執行AD查詢）。

授權策略已配置為提供完全網路訪問(許可權：PermitAccess)，用於通過ASA-VPN進行身份驗證並屬於Active Directory組管理員的使用者 — 對於這些使用者，返回SGT標籤審計器：



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)

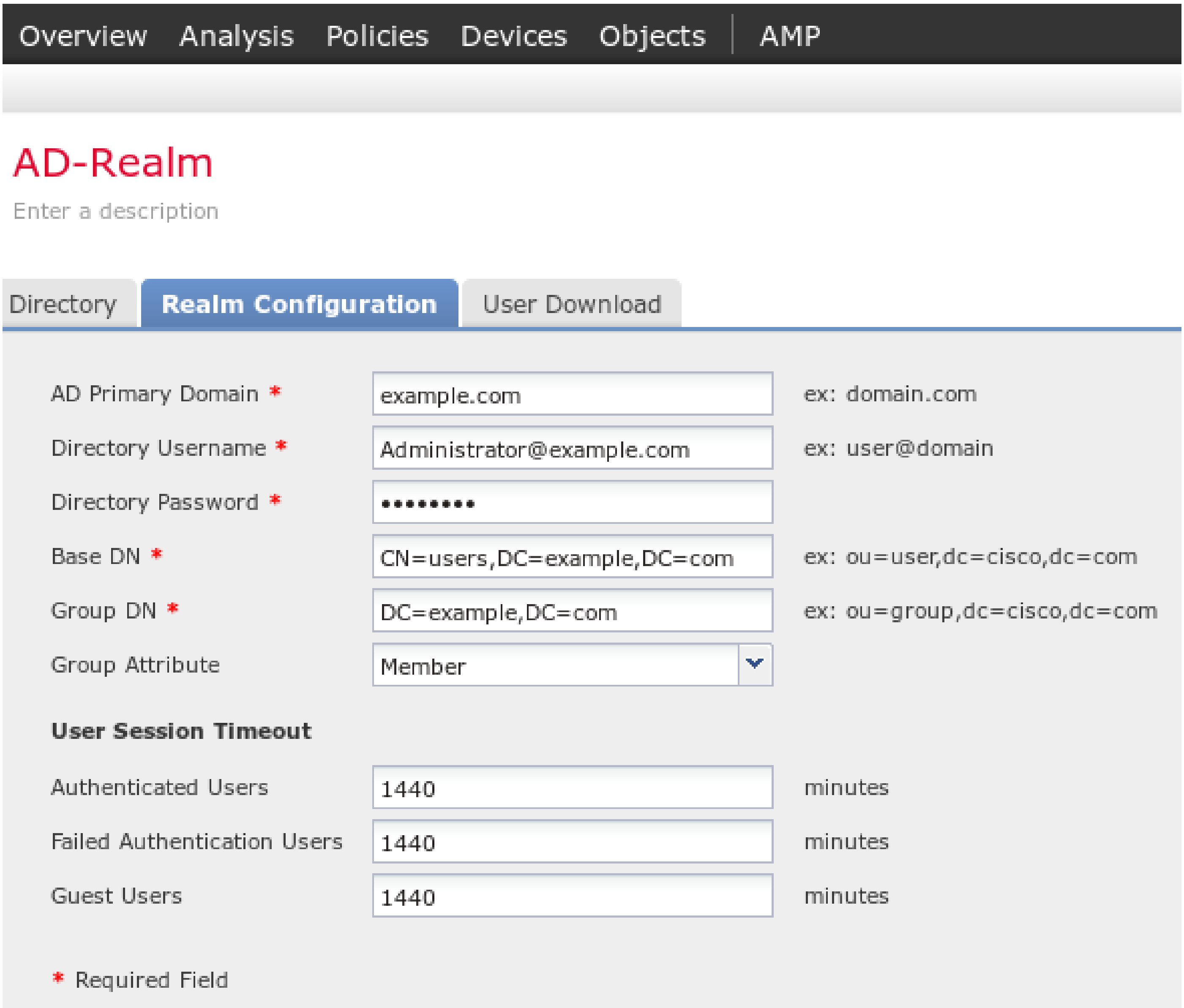
Standard

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

FMC

Active Directory領域

領域配置是使用ISE整合的必要條件（使用身份策略並為被動身份驗證使用者檢索組成員身份）。可以為Active Directory或輕型目錄訪問協定(LDAP)配置領域。 在此示例中，正在使用AD。在**系統>整合>領域**中：



AD-Realm

Enter a description

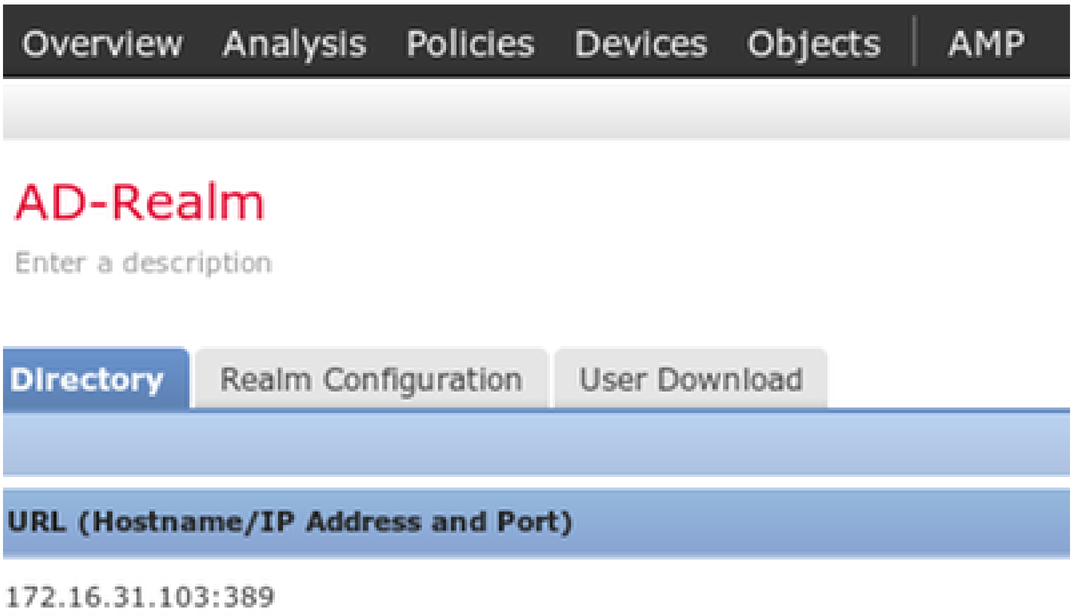
AD Primary Domain *	example.com	ex: domain.com
Directory Username *	Administrator@example.com	ex: user@domain
Directory Password *	••••••••	
Base DN *	CN=users,DC=example,DC=com	ex: ou=user,dc=cisco,dc=com
Group DN *	DC=example,DC=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

User Session Timeout

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

* Required Field

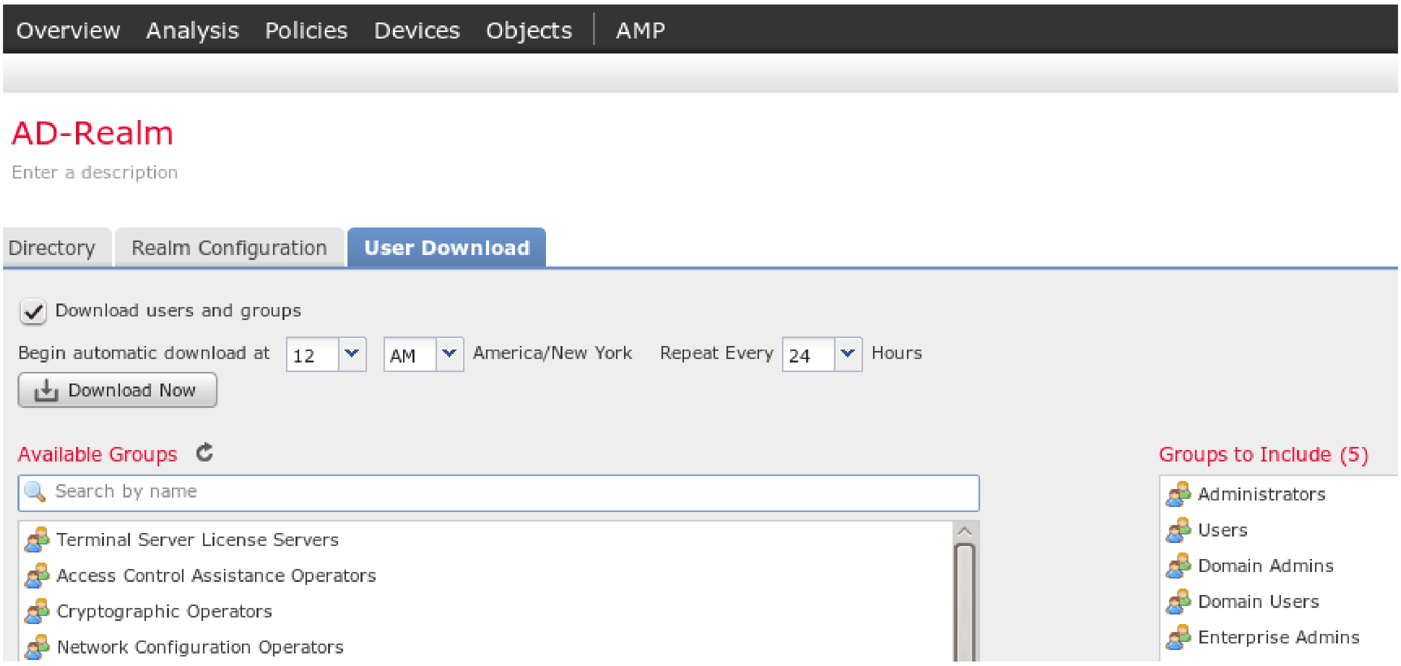
使用標準目錄設定：



URL (Hostname/IP Address and Port)

172.16.31.103:389

並檢索一些AD組（在訪問控制規則中用作附加條件）：



☑ Download users and groups

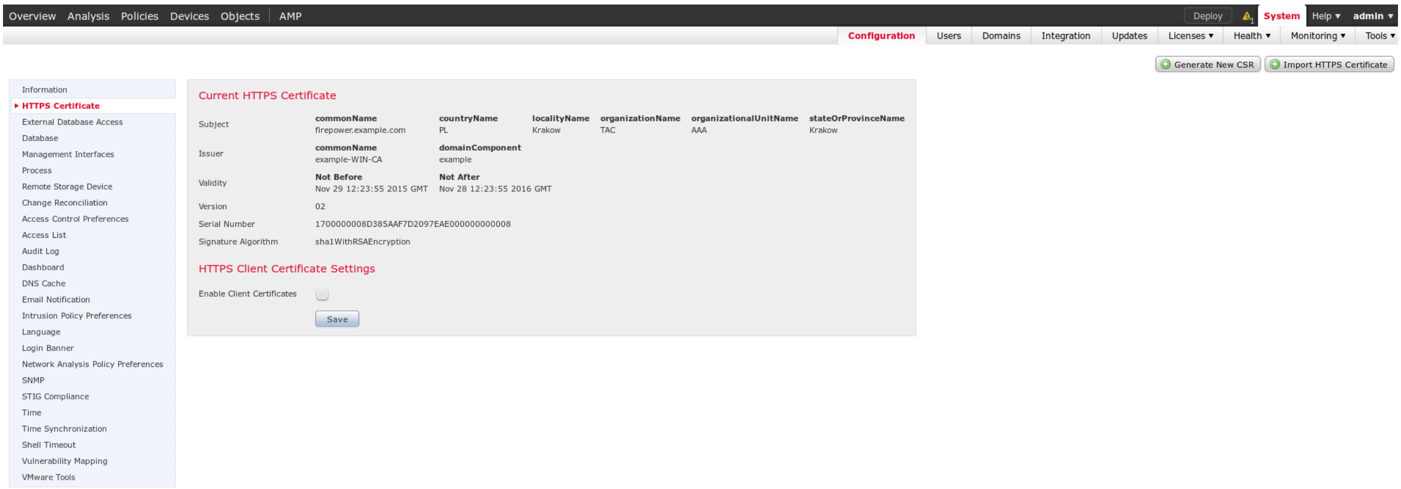
Begin automatic download at 12 AM America/New York Repeat Every 24 Hours

Available Groups:
- 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

Admin和pxGrid的證書

雖然不是必需的，但為管理員存取產生CSR是很好的作法。使用受信任AD對CSR進行簽名，然後匯入回已簽名的證書，如下圖所示：



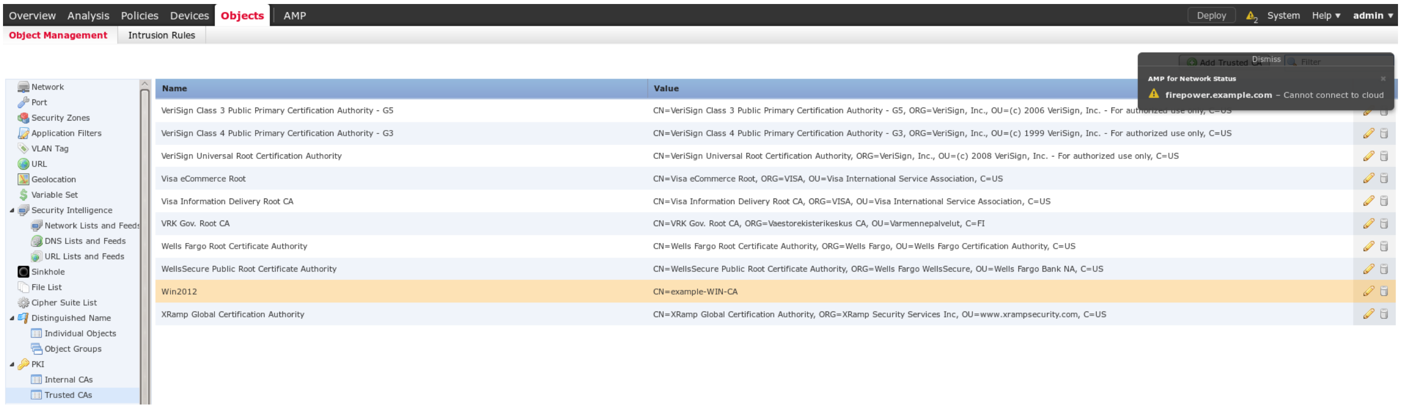
Current HTTPS Certificate

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 □

需要將CA證書新增到受信任的儲存：



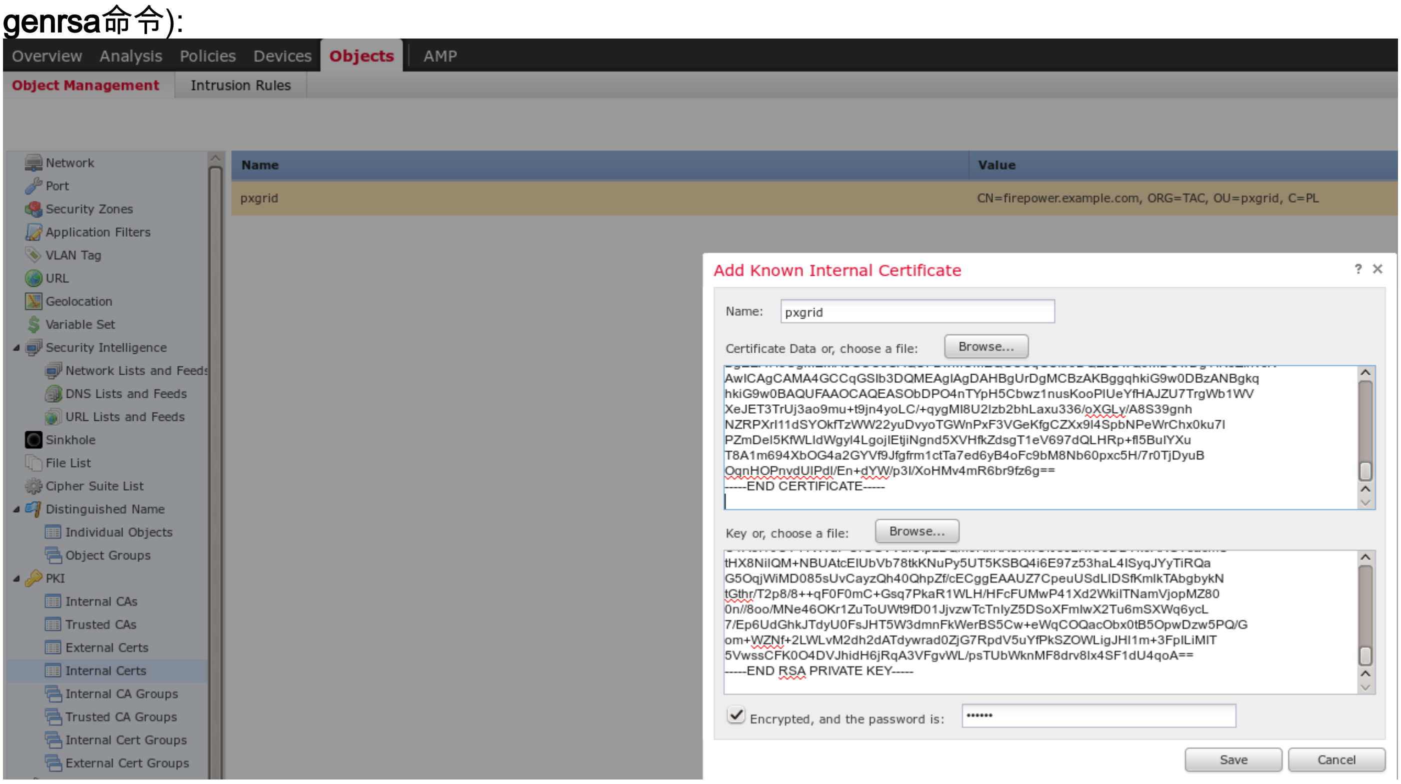
firepower.example.com – Cannot connect to cloud

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

最後一步是生成FMC使用的pxGrid證書以授權給ISE pxGrid服務。若要產生CSR，需要使用CLI（或任何其他使用openssl工具的外部機器）。

```
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:~#
```

生成fire.csr後，使用Microsoft CA（pxGrid模板）對其進行簽名。 將私密金鑰(fire.key)和簽署憑證(fire.pem)匯回到FMC內部憑證庫中。對於私鑰，請使用在生成金鑰期間設定的密碼(**openssl** genrsa命令):



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/+qygMI8U2Izb2bhLaxu336/oXGLy/A8S39gnh
NZRPXrl11dSYOkfTzWW22yuDvyoTGWnPxF3VGeKfgCZXx9l4SpbNPeWrChx0ku7I
PZmDel5KfWLIdWgyl4LgojIEtjiNgnd5XVHfkZdsgT1eV697dQLHRp+fl5BuIYXu
T8A1m694XbOG4a2GYVf9Jfgfrm1ctTa7ed6yB4oFc9bM8Nb60pxc5H/7r0TjDyuB
OgnHOPnvdUIPdl/En+dYW/p3l/XoHMv4mR6br9fz6g==
-----END CERTIFICATE-----
```

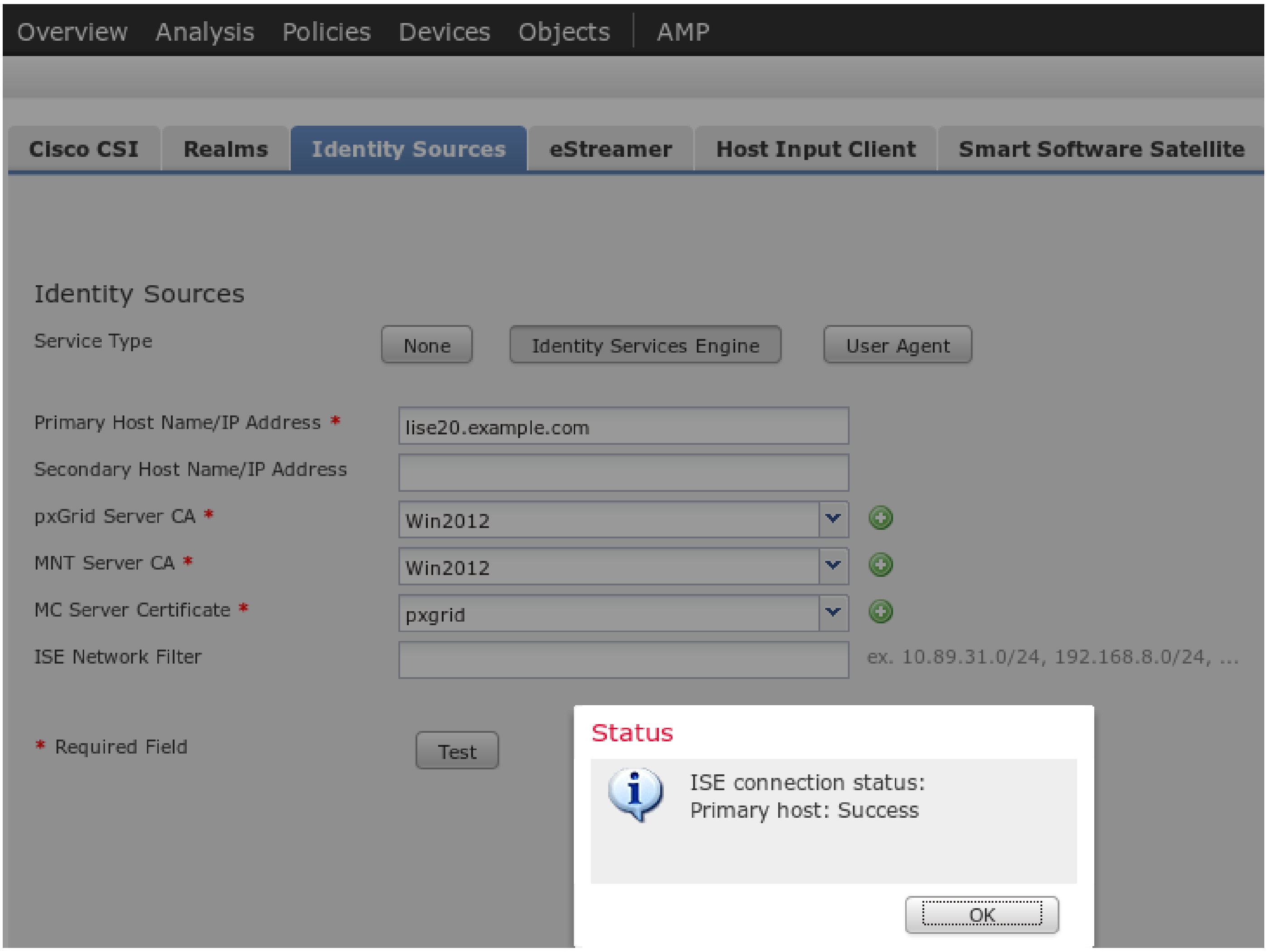
Key or, choose a file:

```
tHX8NiIQM+NBUAtcElUbVb78tkKNuPy5UT5KSBQ4i6E97z53haL4ISyqJYyTiRQa
G5OqjWiMD085sUvCayzQh40QhpZf/cECggEAAUZ7CpeuUSdLIDSfKmlkTAbgbykN
tGthr/T2p8/8++qF0F0mC+Gsq7PkaR1WLH/HFcFUMwP41Xd2WkiITNamVjopMZ80
0n//8oo/MNe46OKr1ZuToUWt9fD01JjvzwTcTnlyZ5DSoXFmlwX2Tu6mSXWq6ycL
7/Ep6UdGhkJTdyU0FsJHT5W3dmnFkWerBS5Cw+eWqCOQacObx0tB5OpwDzw5PQ/G
om+WZNf+2LWLvM2dh2dATdywrad0ZjG7RpdV5uYfPkSZOWLigJHI1m+3FpILiMIT
5VwssCFK0O4DVJhidH6jRqA3VFgvWL/psTUbWknMF8drv8lx4SF1dU4qoA==
-----END RSA PRIVATE KEY-----
```

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

ISE整合

安裝所有證書後，從**System > Integration**配置ISE整合：



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

Test

Status

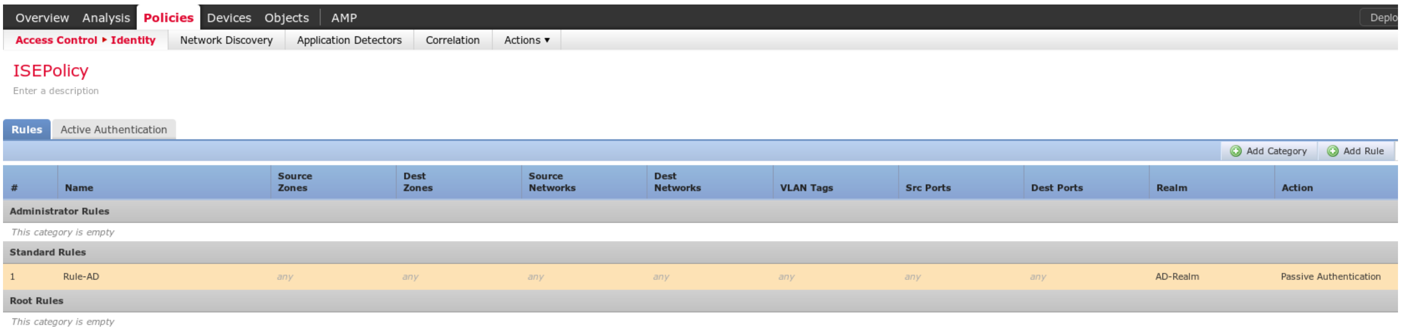
ISE connection status:
Primary host: Success

OK

將匯入的CA用於pxGrid和MnT服務證書驗證。對於管理控制檯(MC)，使用為pxGrid生成的內部證書
。

身份策略

配置身份策略，該策略利用以前配置的AD領域進行被動身份驗證：



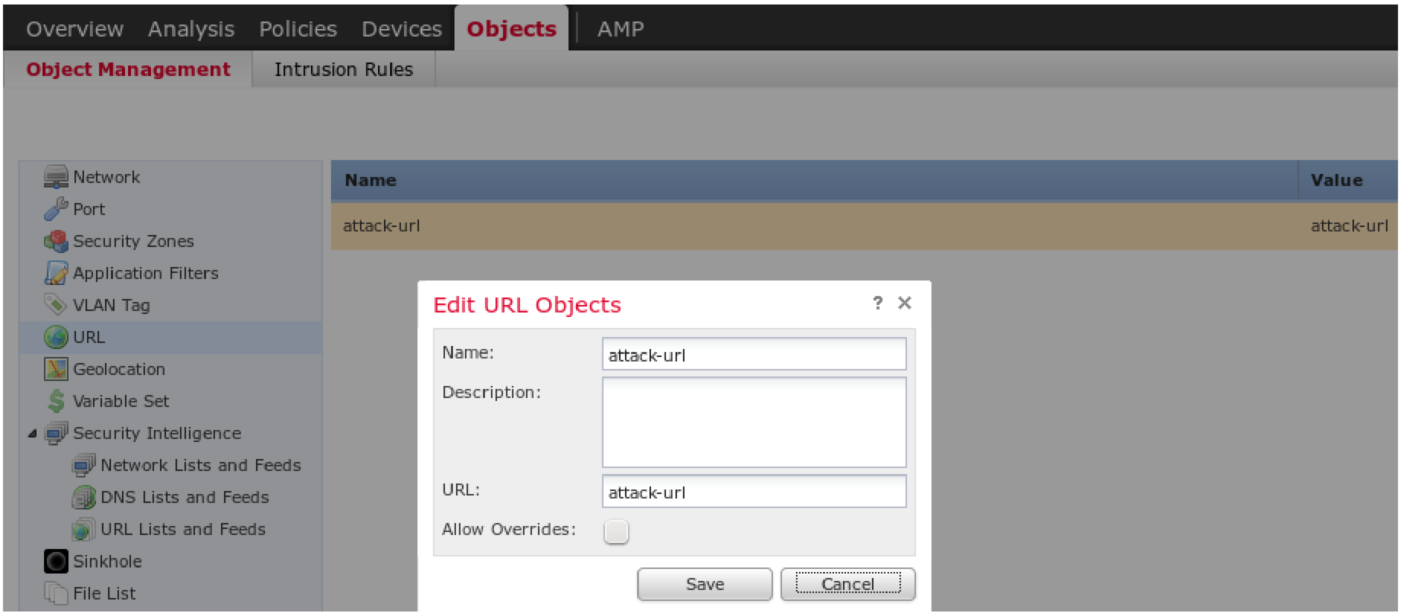
ISEPolicy

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										

訪問控制策略

在此範例中，自訂URL已建立：

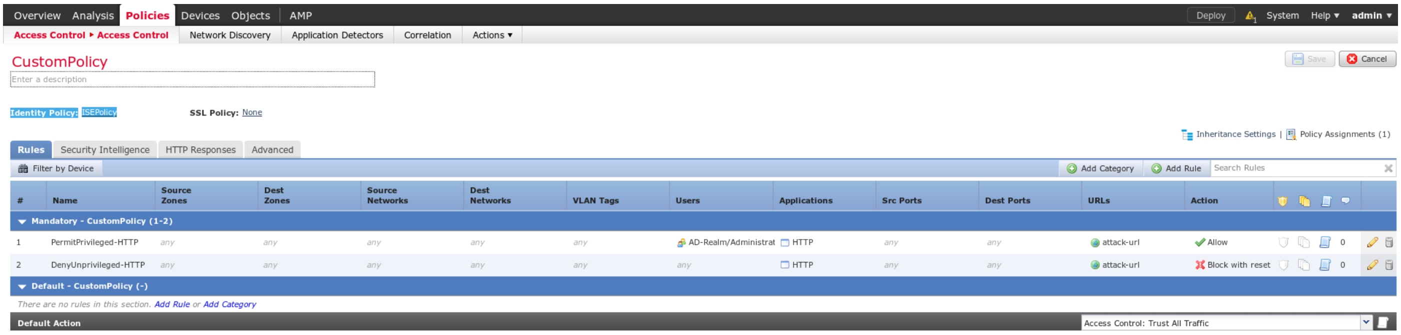


Name	Value
attack-url	attack-url

Edit URL Objects

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

以及自定義訪問控制策略中的兩個規則：



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
2	DenyUnprivileged-HTTP	any	any	any	any	any	any	HTTP	any	any	attack-url	✗ Block with reset
Default - CustomPolicy (-)												

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

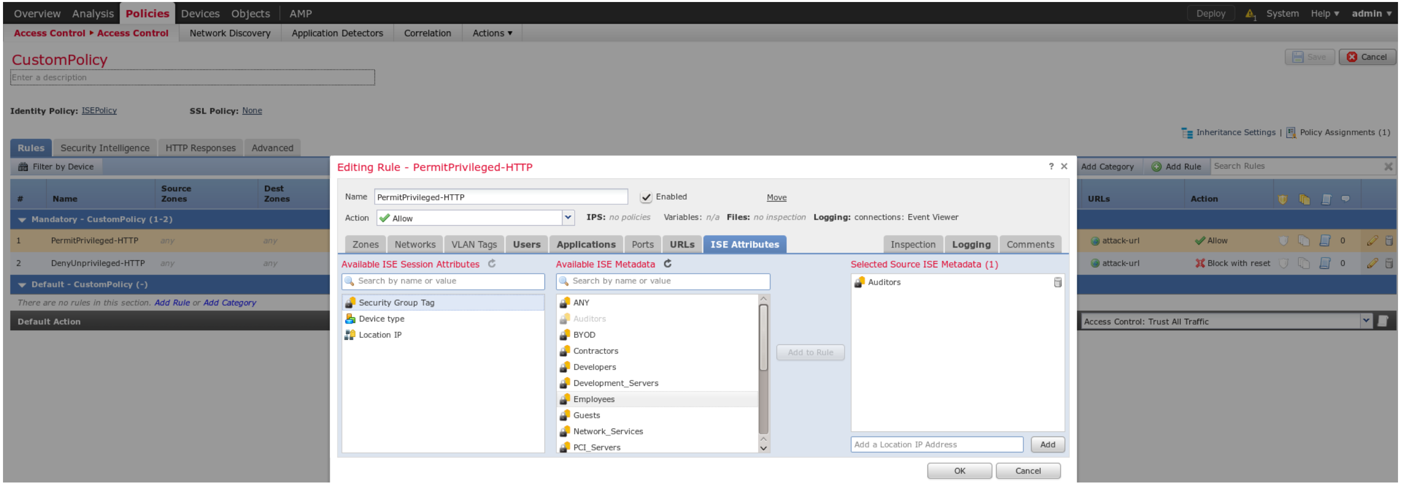
Default Action: Access Control: Trust All Traffic

PermitPrivileged-HTTP規則允許屬於已分配SGT標籤的AD Administrators組的所有使用者。審計者對所有目標執行HTTP攻擊。

DenyUnprivileged-HTTP拒絕將此操作用於所有其他使用者。

另請注意，以前建立的身份策略已分配給此訪問控制策略。

在此頁籤上，無法檢視SGT標籤，但在建立或編輯特定規則時，可以看到這些標籤：



Editing Rule - PermitPrivileged-HTTP

Name: PermitPrivileged-HTTP   ☑ Enabled   Move

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

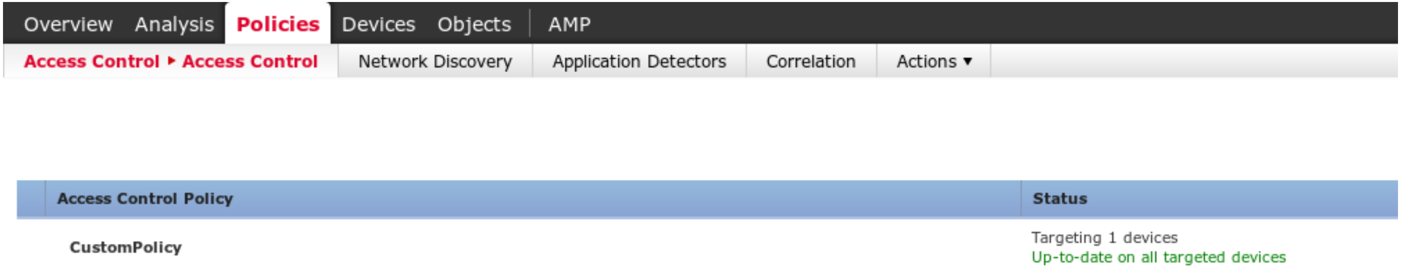
Available ISE Session Attributes: Security Group Tag, Device type, Location IP

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

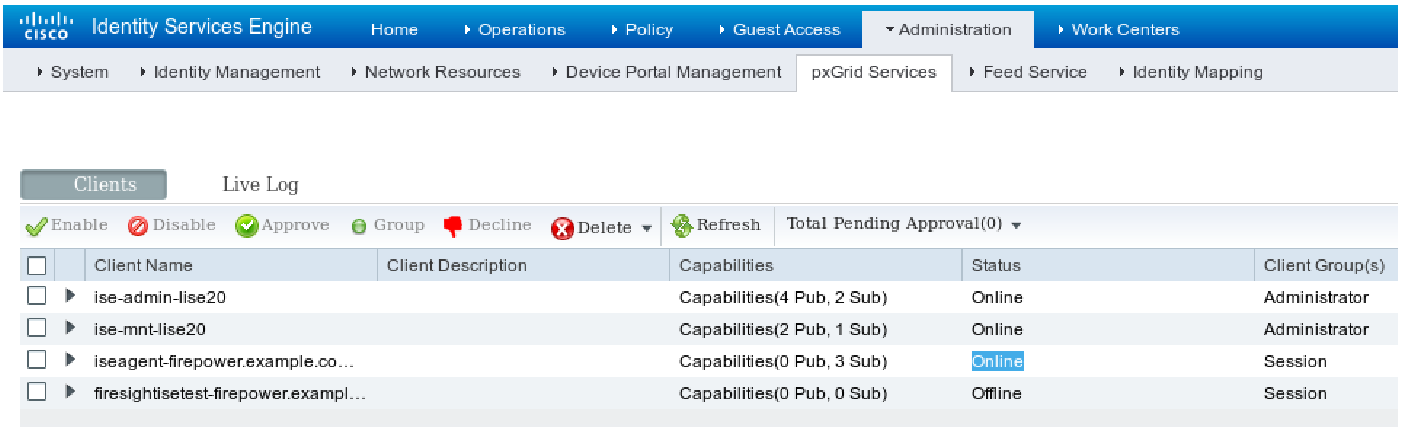
確保將策略分配給NGIPS，並且部署所有更改：



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

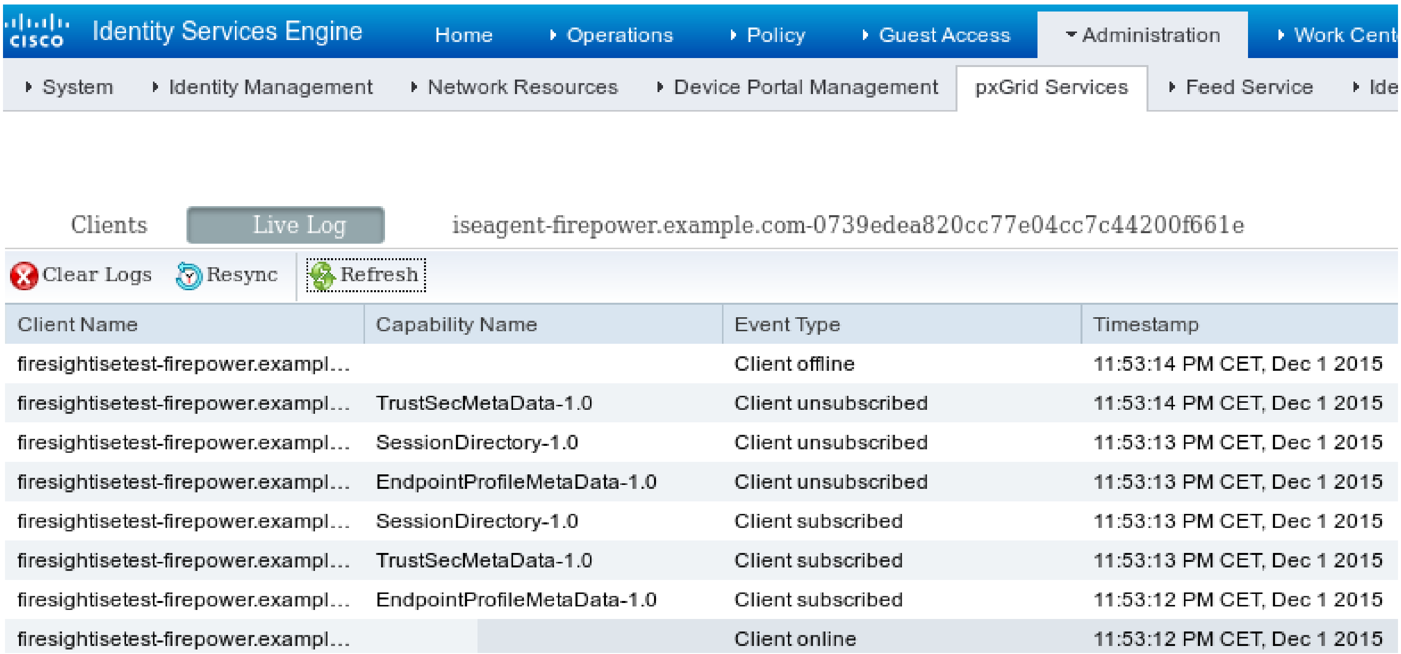
驗證

在正確配置所有內容後，ISE應看到pxGrid客戶端訂閱會話服務（狀態線上）。



□		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

從日誌中，您還可以確認FMC已訂閱TrustSecMetaData（SGT標籤）服務 — 已獲取所有標籤並取消訂閱。



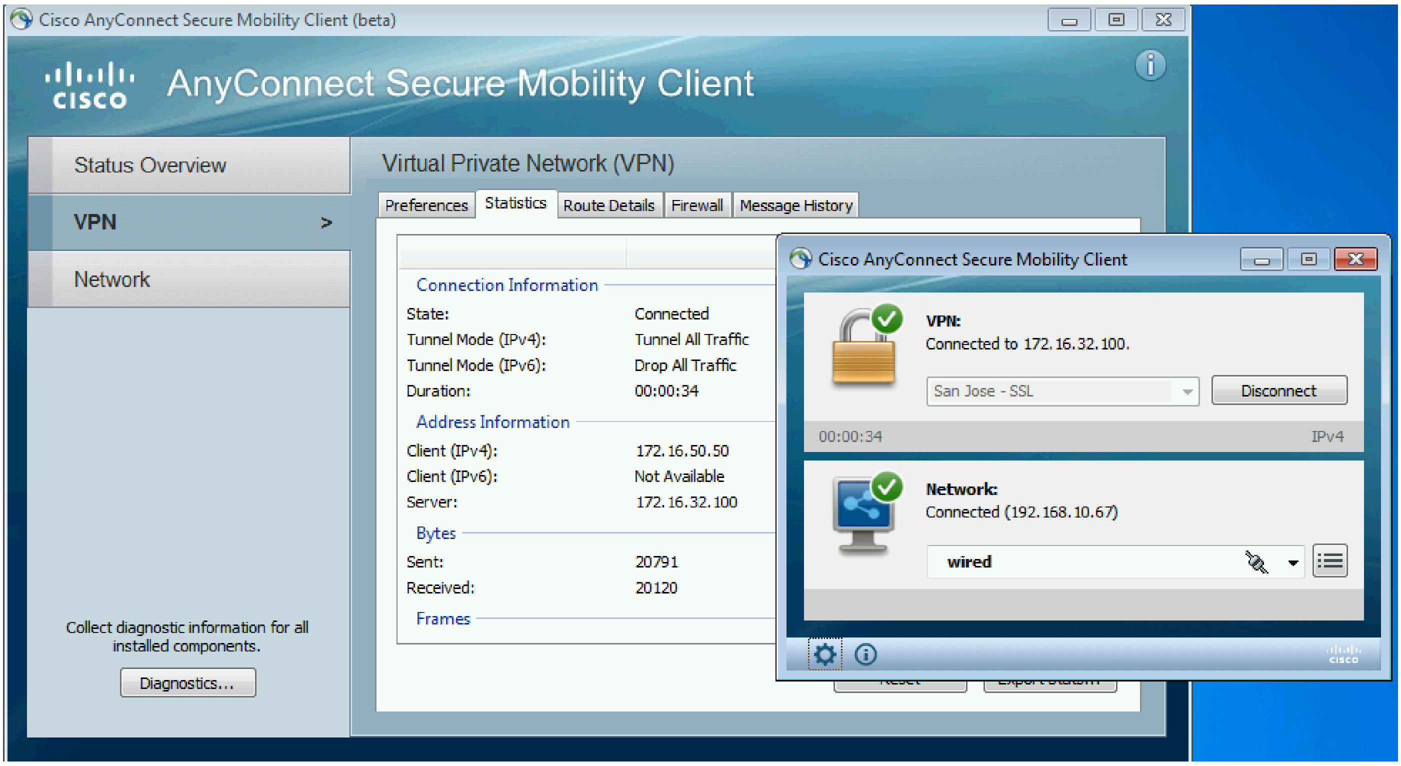
iseagent-firepower.example.com-0739edea820cc77e04cc7c44200f661e

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

VPN會話建立

當ISE上的授權沒有返回正確的SGT標籤（NGIPS不允許稽核測試）時，會為場景執行第一個測試。

VPN會話啟動後，AnyConnect使用者介面(UI)可提供更多詳細資訊：


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

Virtual Private Network (VPN)

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

Collect diagnostic information for all installed components.

VPN:
Connected to 172.16.32.100.

San Jose - SSL

00:00:34 IPv4

Network:
Connected (192.168.10.67)

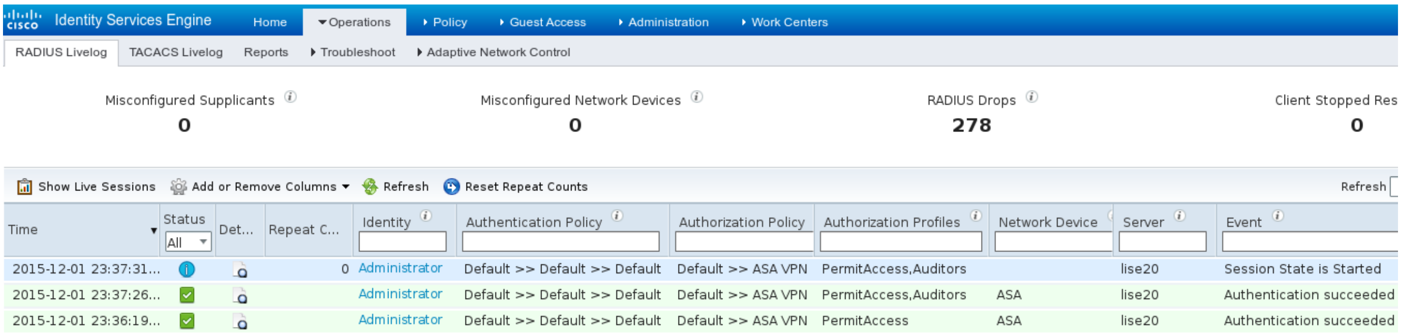
wired

ASA可以確認會話已建立：

```
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
```

請注意，ASA確實看到為此身份驗證返回的任何SGT標籤。未為TrustSec配置ASA — 因此無論如何都會跳過資訊。

ISE還報告成功的授權（23:36:19處的日誌）— 未返回SGT標籤：



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

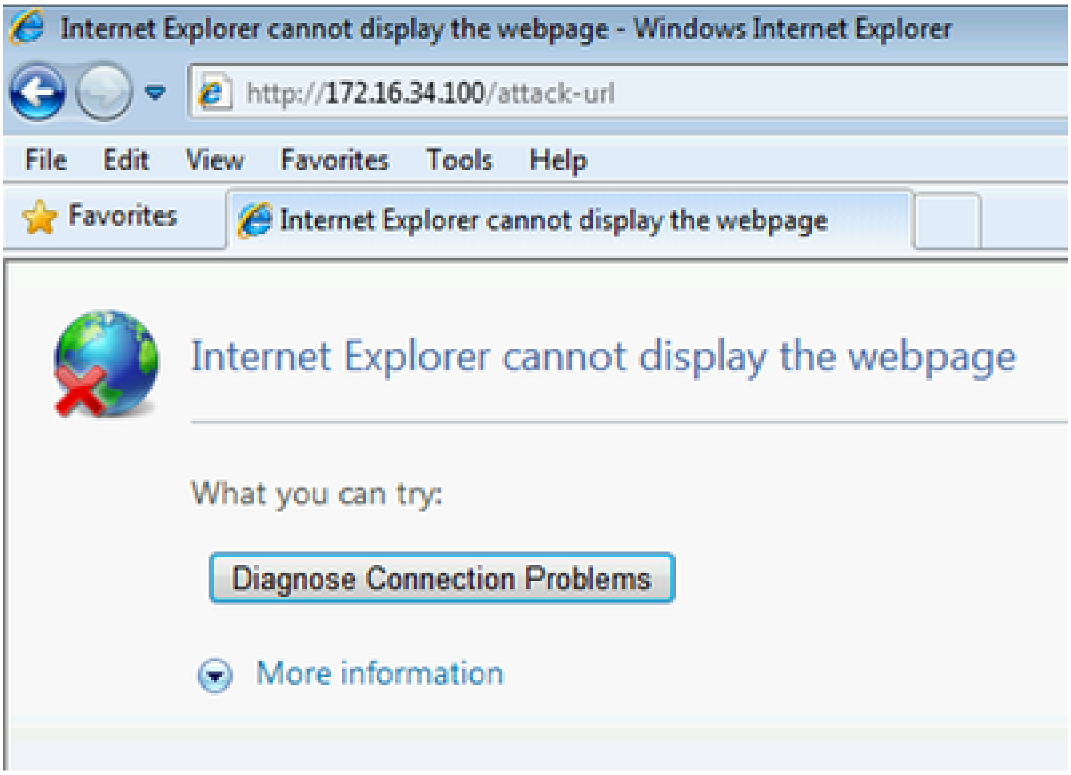
FMC從MnT獲取會話資料

在此階段，/var/log/messages中的FMC報告管理員使用者名稱的新會話（作為pxGrid服務的訂閱者接收），並對組成員身份執行AD查詢：

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

無許可權和特權網路訪問

在此階段，當使用者嘗試開啟Web瀏覽器並訪問稽核伺服器時，連線將終止：

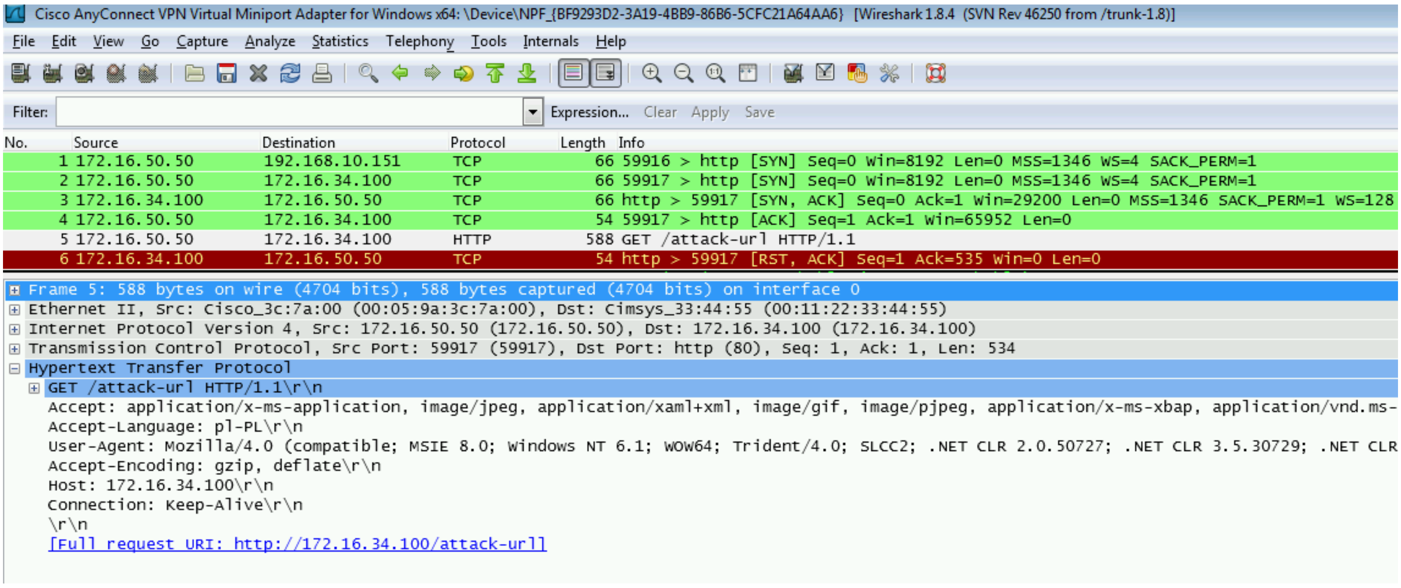

Internet Explorer cannot display the webpage - Windows Internet Explorer
http://172.16.34.100/attack-url
File
Edit
View
Favorites
Tools
Help
Favorites
Internet Explorer cannot display the webpage

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems
More information

可從使用者端擷取封包擷取（依照FMC設定傳送的TCP RST）確認這點：

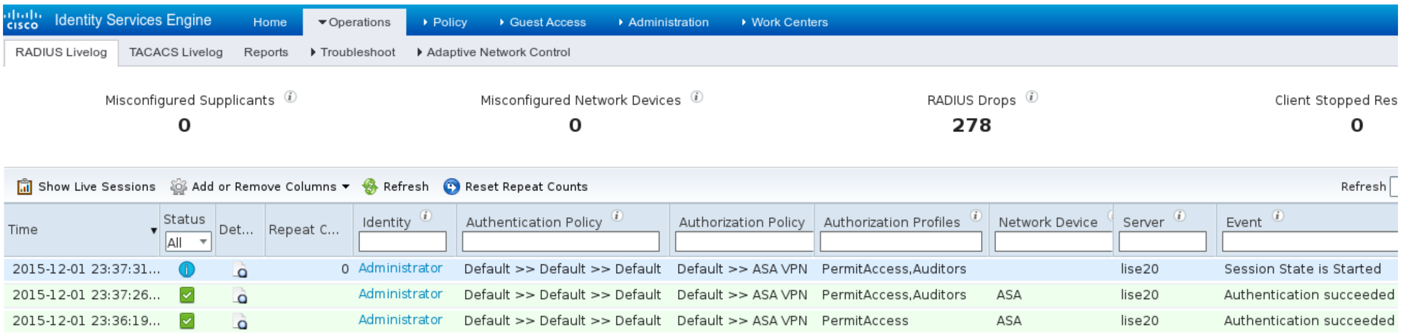

Cisco AnyConnect VPN Virtual Miniport Adapter for Windows x64: \Device\NPF_{BF9293D2-3A19-4BB9-86B6-5CFC21A64AA6} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
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]
```

ISE配置為返回後，稽核標籤ASA會話報告：

```
asav# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Administrator          Index        : 1
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.67
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel:
(1)AES128

Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel:
(1)SHA1

Bytes Tx     : 11428                  Bytes Rx     :
24604

Group Policy : POLICY                 Tunnel Group :
SSLVPN

Login Time   : 12:22:59 UTC Wed Dec 2
2015

Duration     :
0h:01m:49s


Inactivity   :
0h:00m:00s


VLAN Mapping : N/A                    VLAN         :
none

Audt Sess ID : ac101f6400001000565ee2a3
Security Grp : 9
```

ISE還會報告成功的授權（23:37:26的日誌）— 返回SGT標籤審計器：



Identity Services Engine | Home | ▾Operations | ▸ Policy | ▸ Guest Access | ▸ Administration | ▸ Work Centers

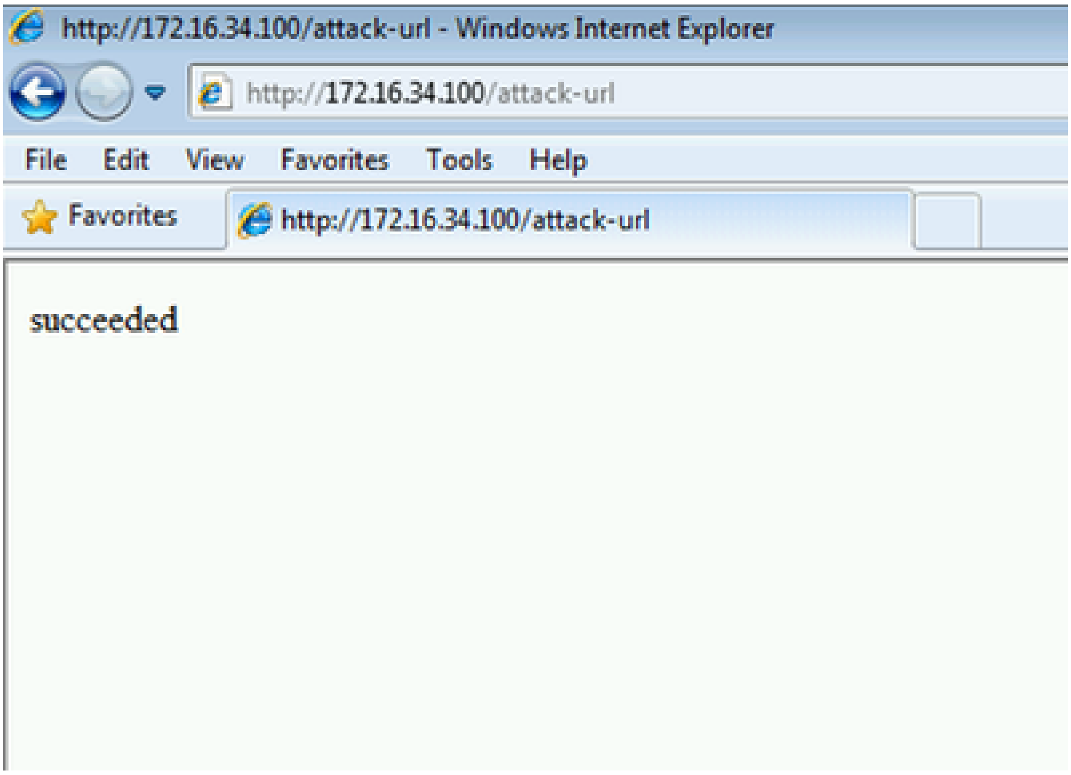
RADIUS Livelog | TACACS Livelog | Reports | ▸ Troubleshoot | ▸ Adaptive Network Control

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

Show Live Sessions | Add or Remove Columns ▾ | Refresh | Reset Repeat Counts | Refresh

Time	Status	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

使用者可以訪問上述服務：



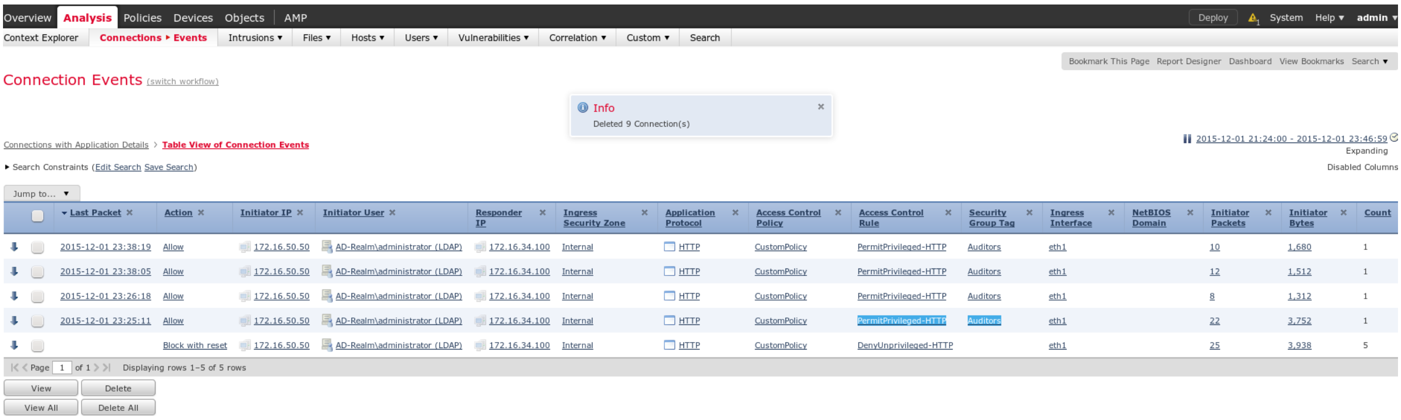
http://172.16.34.100/attack-url - Windows Internet Explorer

http://172.16.34.100/attack-url

succeeded

FMC日誌記錄訪問

此活動可通過連線事件報告確認：



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

Jump to... ▾

	□	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

View | Delete
View All | Delete All

首先，使用者沒有分配SGT標籤，並且正在觸發DenyUnprivileged-HTTP規則。ISE分配了審計者標籤（並由FMC檢索）規則後，使用PermitPrivileged-HTTP並允許訪問。

另請注意，要顯示內容，多列已被刪除，因為通常訪問控制規則和安全組標籤顯示為最後一列之一（且需要使用水準捲軸）。 將來可以儲存和重用該自定義檢視。

疑難排解

FMC調試

要檢查負責身份服務的adi元件的日誌，請檢查/var/log/messages檔案：

```
[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
```

要獲得更詳細的調試，可以終止adi進程（從sudo後的根目錄）並使用debug引數運行該進程：

```
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
```

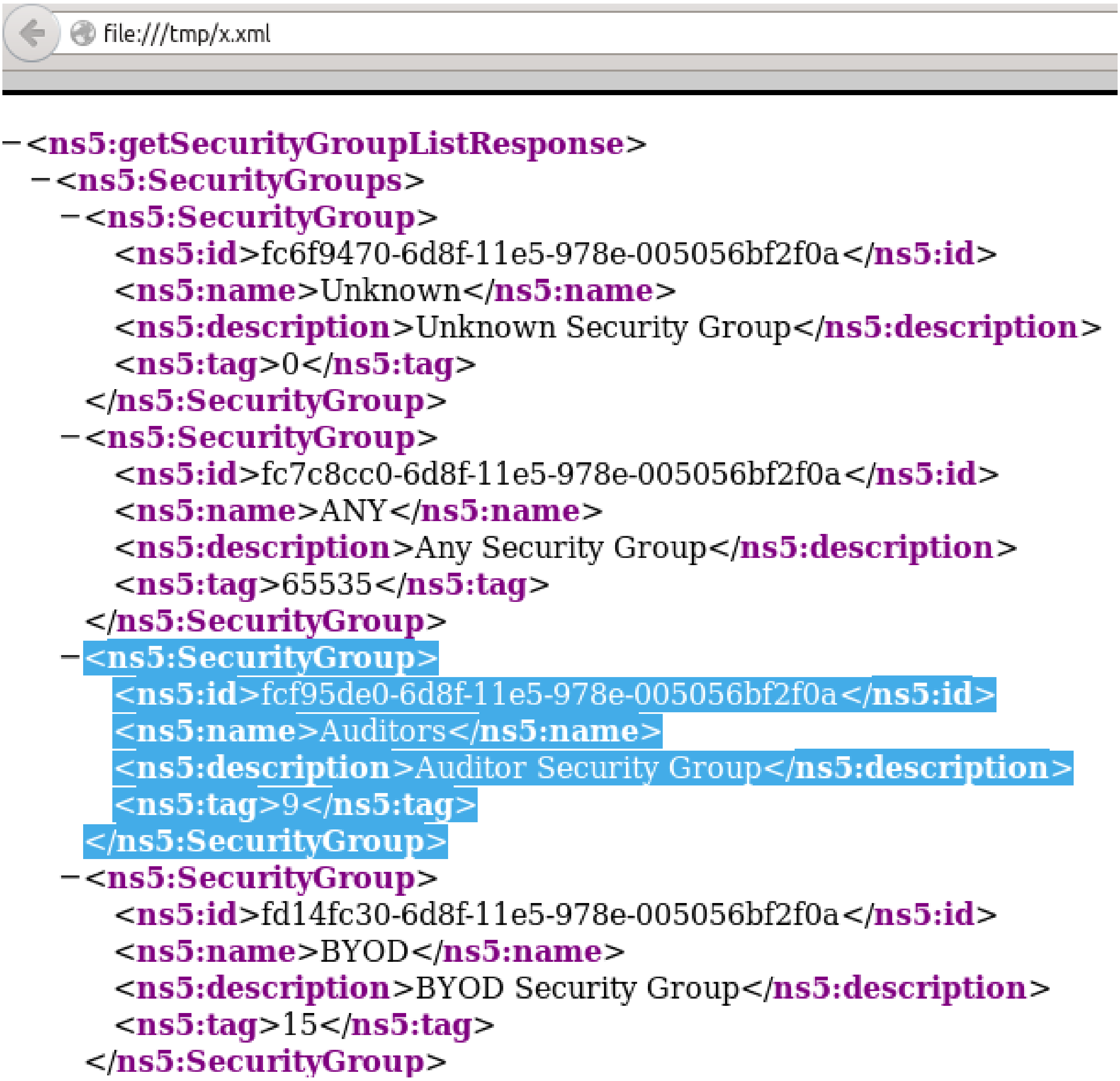
```
Dec 01 23:14:34 firepower SF-IMS[24106]: [24106] ADI:config [DEBUG]
config.cpp:289:ProcessConfigGlobalSettings(): Parsing global settings
<..........a lot of detailed output with data.......>
```

通過pxGrid進行SGT查詢

在**ISE整合**部分按一下**測試**按鈕或刷新SGT清單時，在訪問控制策略中新增規則時執行該操作。

```
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>]
```

為了更好地檢視xml內容，可將日誌中的xml內容複製到xml檔案，並通過web瀏覽器開啟。您可以確認是否收到特定的SGT（稽核）以及在ISE上定義的所有其他SGT:



file:///tmp/x.xml

```
- <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>
```

通過REST API到MnT的會話查詢

這也是測試操作的一部分（請注意MnT主機名和埠通過pxGrid）。 使用批次會話下載：

```
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>
```

和分析結果（已接收1個活動會話）：

```
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}
```

在此階段，NGIPS會嘗試將該使用者名稱（和域）與領域AD使用者名稱相關聯：

```
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用於查詢使用者和組成員身份：

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.LdapRealm [INFO] adi.cpp:322:
HandleLog(): search '(|(sAMAccountName=Administrator))' has the following
DN: 'CN=Administrator,CN=Users,DC=example,DC=com'.
Dec 01 23:14:39 firepower SF-IMS[24106]: [24142] ADI:adi.LdapRealm [DEBUG] adi.cpp:319:
HandleLog(): getUserIdentifier: searchfield sAMAccountName has display naming attr:
```

```
Administrator.
```

ISE調試

為pxGrid元件啟用TRACE級別調試後，可以檢查每個操作（但無負載/資料，如FMC）。

SGT標籤檢索示例：

```
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
```

錯誤

CSCuv32295 - ISE可能傳送使用者名稱欄位中的域資訊

CSCus53796 -無法獲取REST批次查詢的主機的FQDN

CSCuv43145 - PXGRID和身份對映服務重新啟動，信任儲存的匯入/刪除

參考資料

- **通過ISE和FirePower整合配置補救服務**
- **在分散式ISE環境中配置pxGrid**
- **如何使用Cisco pxGrid部署證書：配置CA簽名的ISE pxGrid節點和CA簽名的pxGrid客戶端**
- **ISE 1.3版pxGrid與IPS pxLog應用的整合**
- **思科身份服務引擎管理員指南2.0版**
- **思科身份服務引擎API參考指南，版本1.2 — 外部REST風格簡介......**
- **思科身份服務引擎API參考指南，版本1.2 — 監控RES簡介......**
- **思科身份服務引擎管理員指南，版本1.3**
- **技術支援與檔案 — Cisco Systems**