アイデンティティ サービスのための ISE と FirePOWER 統合のトラブルシューティング

目次

概要

この資料に TrustSec わかっているポリシーを on Cisco 設定し解決する方法を次世代侵入防御システム（NGIPS）記述されています（NGIPS）。 NGIPS バージョン 6.0 は識別によって基づくわかっているポリシーを構築することを割り当てる Identity Services Engine （ISE）を搭載する統合をサポートします。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco 適応型セキュリティ アプライアンス（ASA）VPN の設定
- Cisco AnyConnect セキュア モビリティ クライアントの設定
- Cisco Firepower Management Center 基本設定
- Cisco ISE の設定
- Cisco TrustSec ソリューション

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Microsoft Windows 7
- Microsoft Windows 2012 認証局（CA）
- Cisco ASA バージョン 9.3
- Cisco ISE ソフトウェア バージョン 1.4
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.2
- Cisco Firepower Management Center （FMC）バージョン 6.0
- Cisco Firepower NGIPS バージョン 6.0

設定

Firepower Management Center （FMC）は Firepower のための管理プラットフォームです。 ISE 統合に関する機能性には 2 つの型があります:

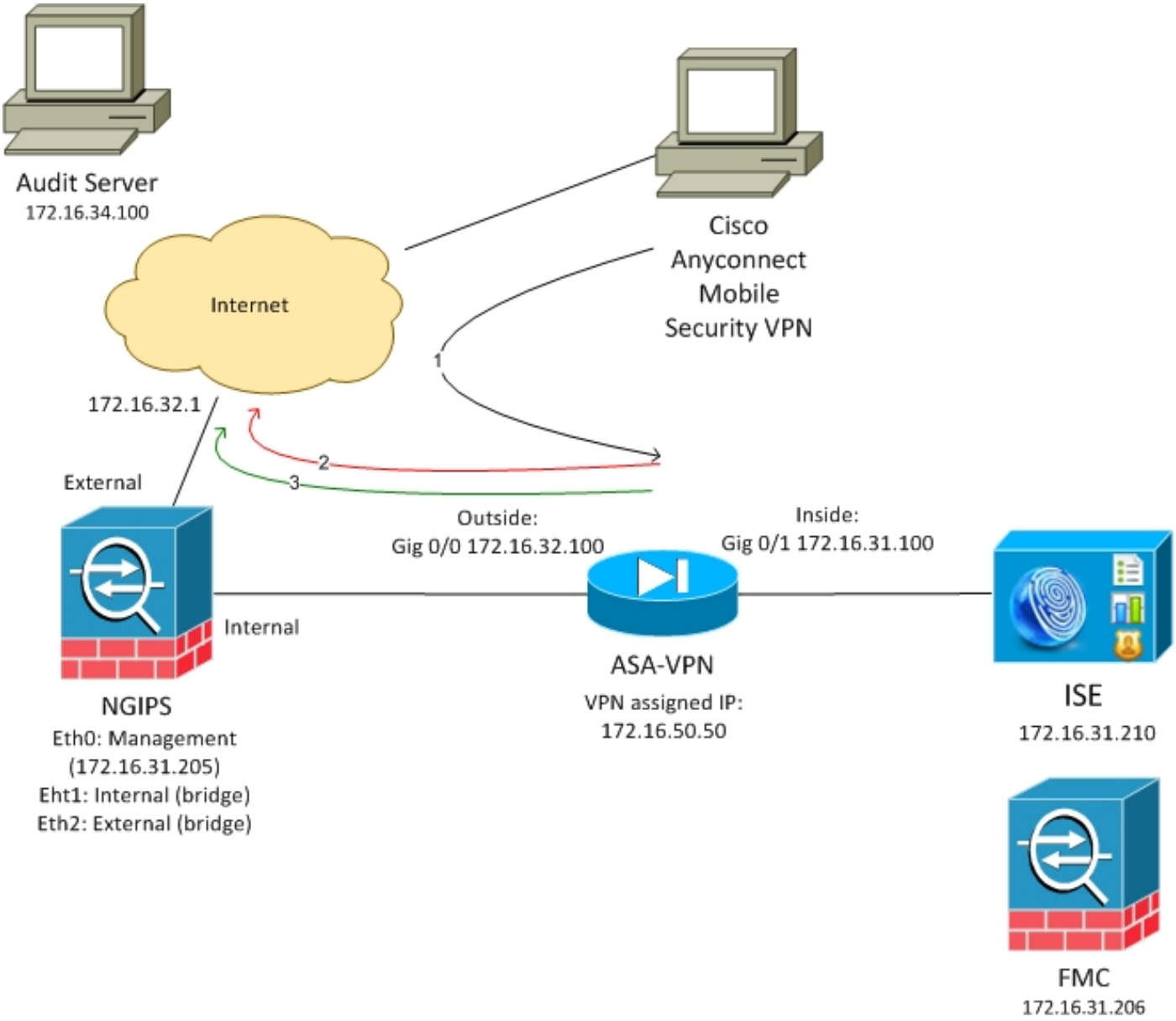
- 治療-限られたネットワーク アクセスを提供するアクセスデバイスの絶えず変化する認証ステータスである ISE によって攻撃者を検疫する割り当て FMC。 このソリューションの 2 つの生成があります:

  1. ISE へのエンド ポイント保護 サービス（EPS） API コールを使用するレガシー パールスクリプト。
  2. ISE への pxGrid プロトコル コールを使用するより新しいモジュール（このモジュールは 6.0 でサポートされないバージョン 5.4 でだけ- 6.1）計画されるネイティブサポート サポートされます。

- ポリシー- TrustSec セキュリティグループ タグ（SGT）に基づくポリシーを設定する割り当て FMC。

この技術情報は第 2 機能性に焦点を合わせます。 治療に関しては例は References セクションを読みました

ネットワーク図



FMC は 2 つのルールが含まれているアクセス制御ポリシーで設定されます:

- カスタム URL（不正侵入 URL）の HTTPトラフィックのための拒否
- カスタム URL（不正侵入 URL）の HTTPトラフィックを可能にしかしときだけ（9）SGT タグを監査するためにユーザが ISE によって割り当てられる

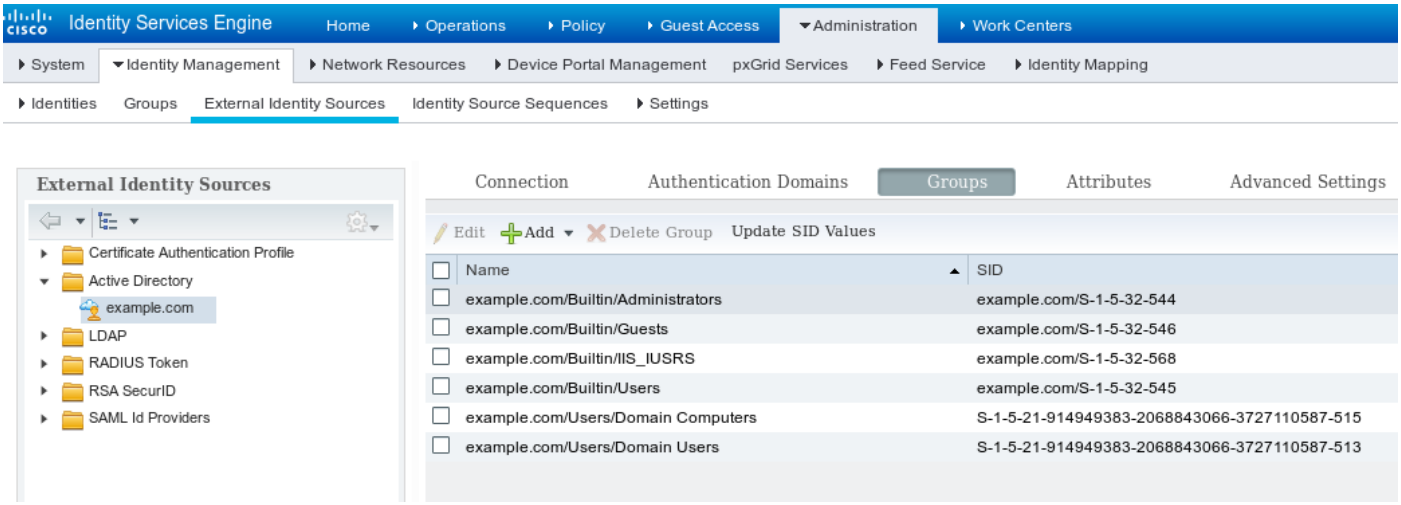
管理者グループに属し、ネットワーク アクセスのために ASA-VPN デバイスを使用する ISE はすべてのアクティブ ディレクトリ ユーザに監査タグを割り当てることにします。

ASA の VPN 接続によるユーザアクセス ネットワーク。 ユーザはそれから URL 不正侵入 URL を使用して監査されたサーバにアクセスすることを試みますが、- SGT グループを監査するために彼が割り当てられなかったので失敗します。 それが固定なら、接続は正常です。

ISE

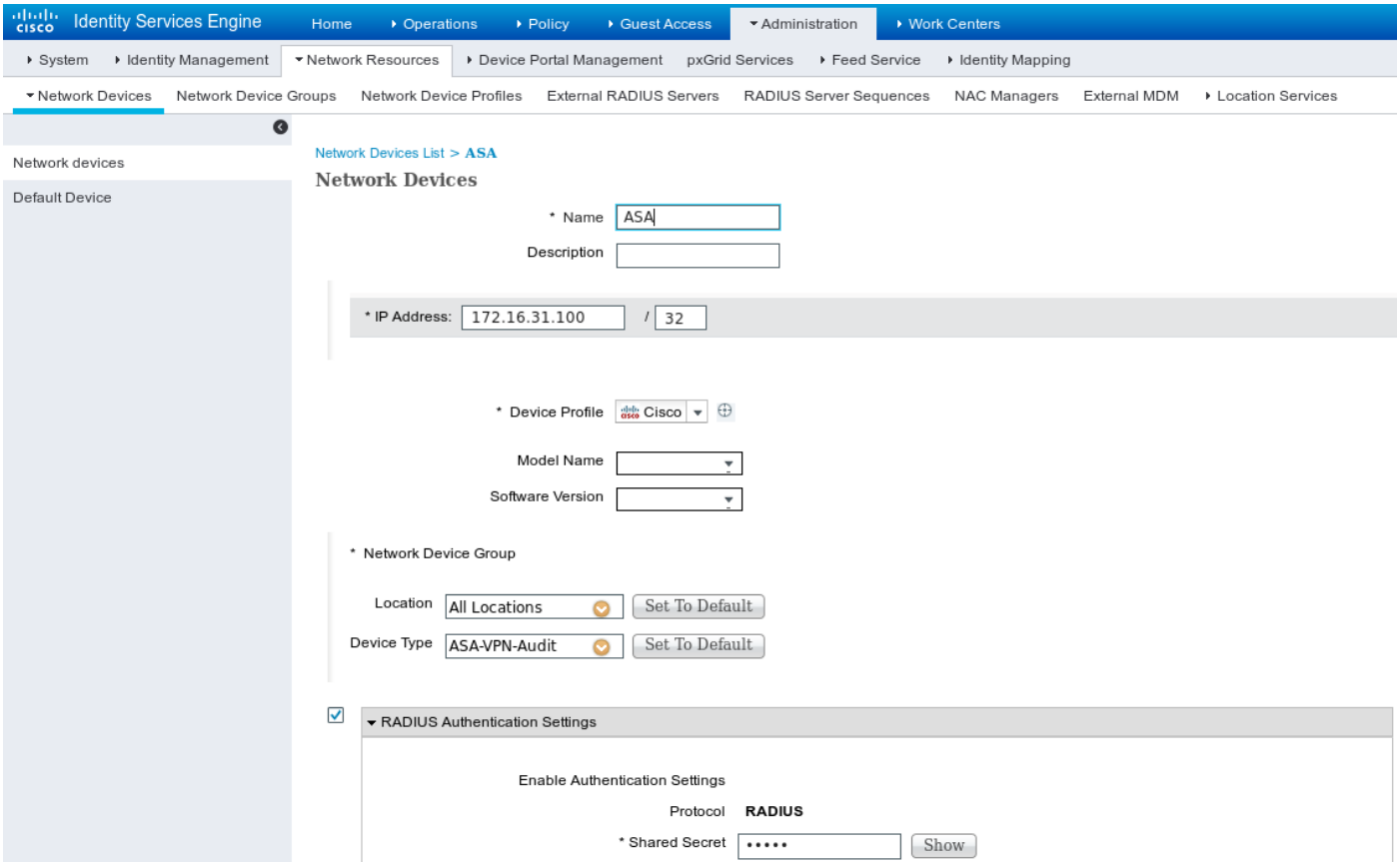
Active Directory

AD 統合は設定し、正しいグループは取出す必要があります（管理者グループは承認規則状態のために使用されます）:



ネットワーク アクセス デバイス

ASA はネットワークデバイスとして追加されます。 カスタム グループ ASA VPN 監査はこのイメージに示すように、使用されます:



pxGrid および MnT のための証明書

FMC は ISE の両方のサービスを利用します:

- SGT およびプロファイリング データ クエリのための pxGrid
- バルク セッション ダウンロードのためのモニタリングおよびレポート（MnT）

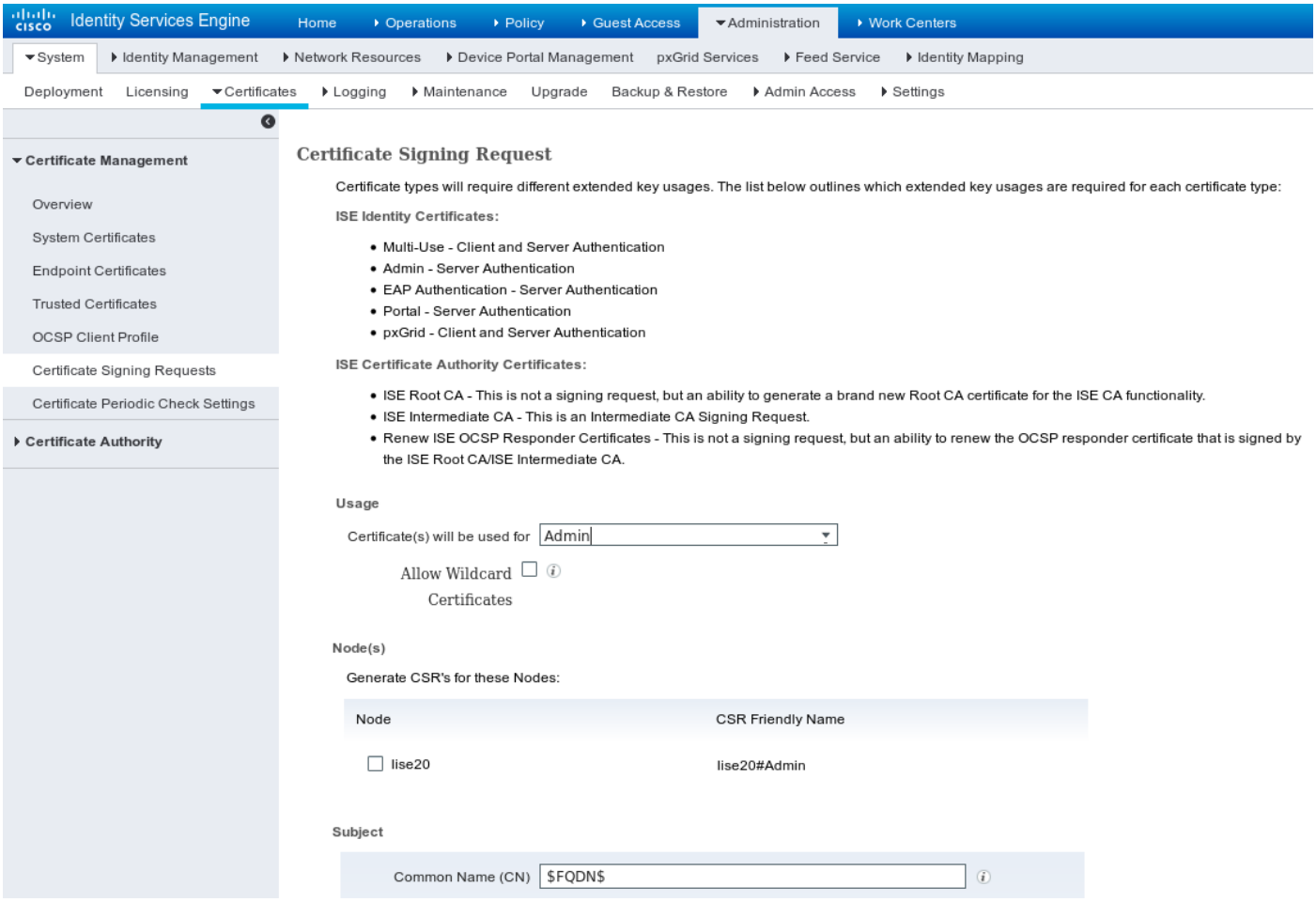
MnT アベイラビリティは認証 された セッションの IP アドレスは、またユーザ名および SGT タグである何こうすれば FMC が知識のあっているので非常に重要です。 それに基づいて、正しいポリシーは適用します。 NGIPS が ASA のような SGT タグ（インライン タギング）を元々サポ

ートしないことを注意して下さい。 しかし ASA への反対で、それは数だけの代りに SGT 名前をサポートします。

それらの要件が理由で ISE および FMC は両方サービス（証明書）互いを信頼する必要があります。 MnT はちょうどサーバ側証明書を使用します、pxGrid はクライアントおよびサーバ側証明書を両方使用します。

Microsoft CA がすべての証明書に署名するのに使用されています。

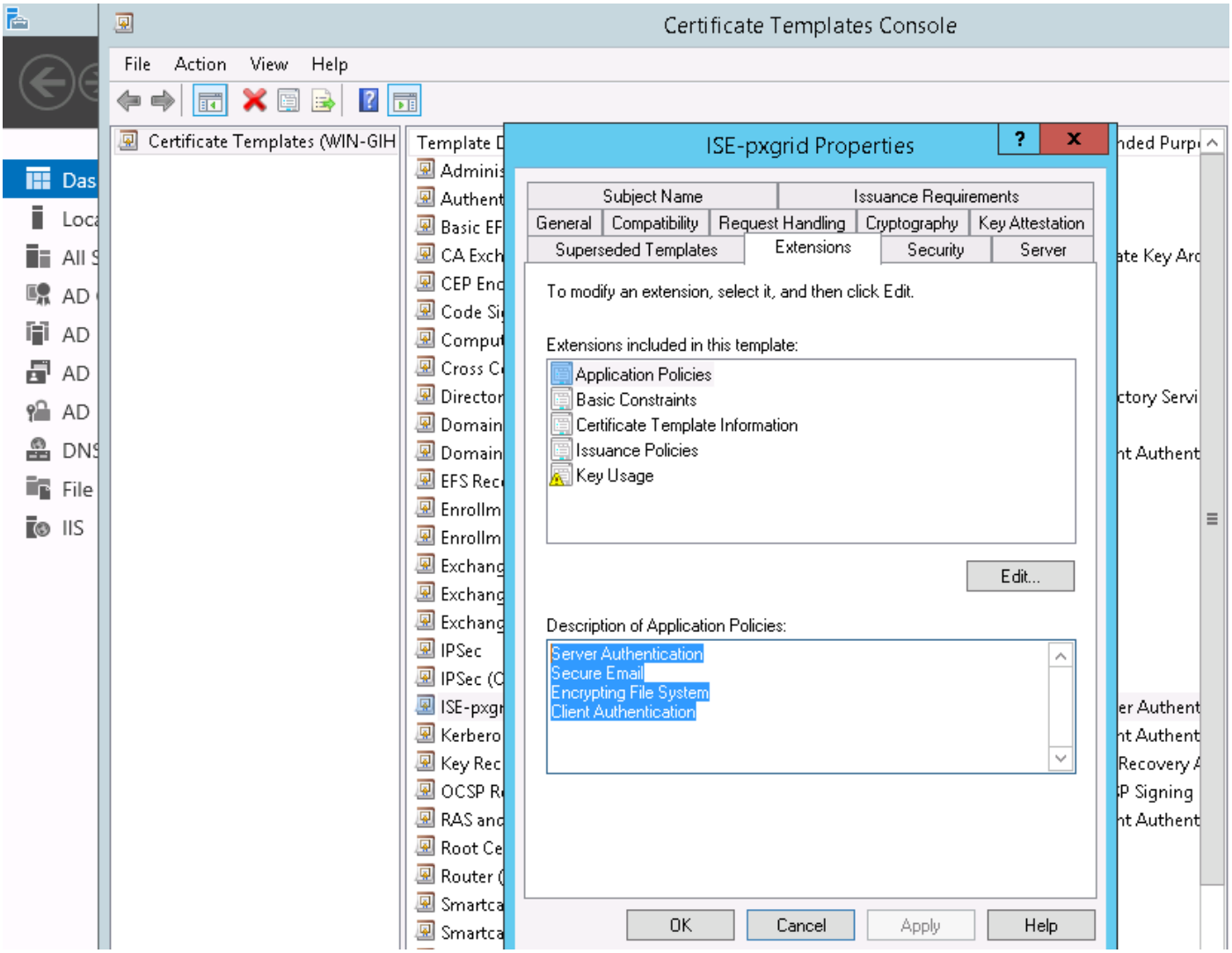
MnT （Admin 役割）に関しては ISE はこのイメージに示すように証明書署名要求（CSR）を、生成する必要があります:



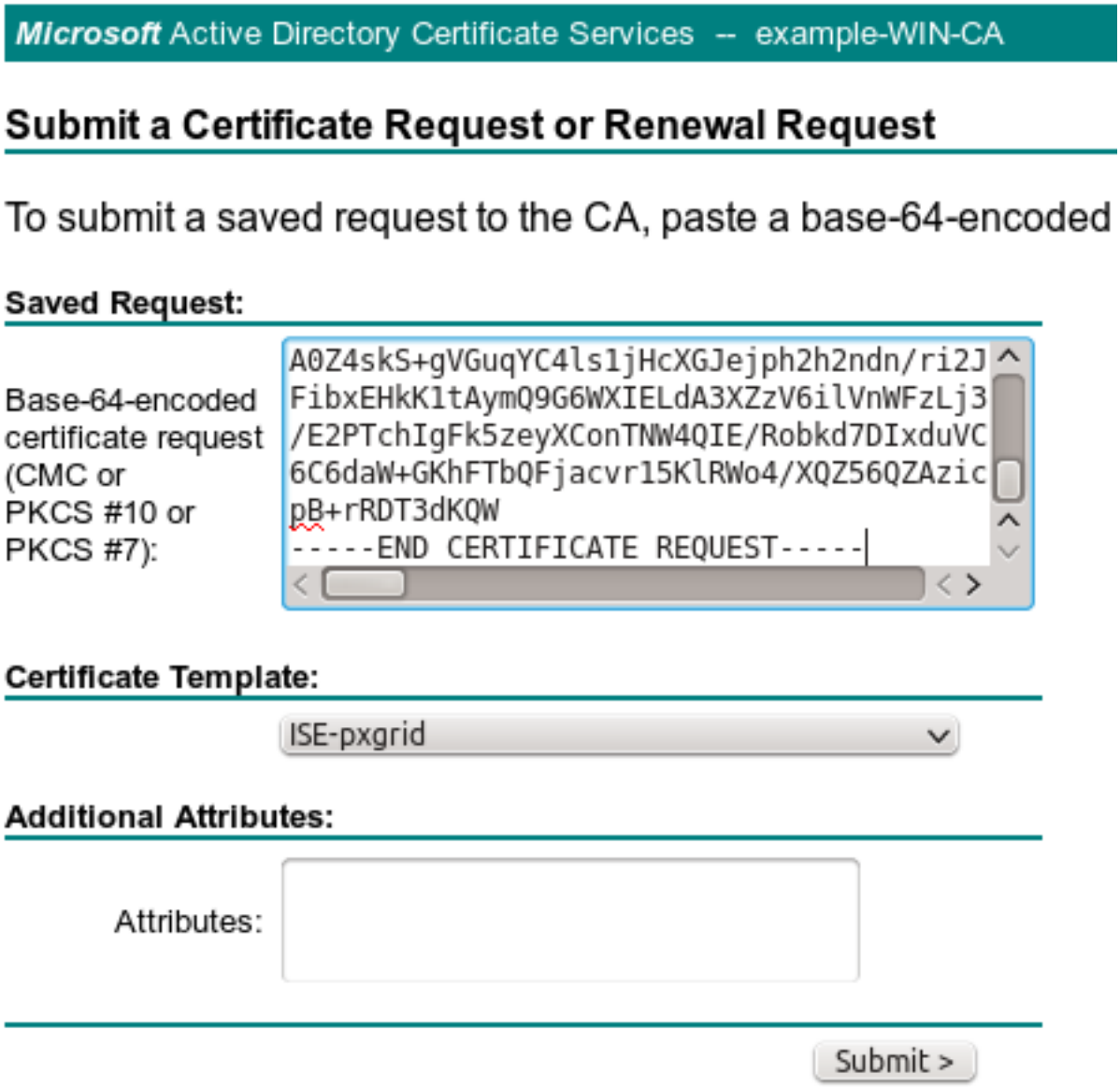
Microsoft CA によって署名の後でそれは **バインド証明書**オプションによってインポートする必要があります。
同じようなプロセスは pxGrid サービスのために従う必要があります。 **証明書は**オプション **のために** pxGrid を選択してもらわなければなりません **使用されます**。
同一のサブジェクト名を用いる 2 つの証明書がある場合もないので OU または O セクション（たとえば pxGrid）の別を追加することは十分に受諾可能評価しますです。

> **注:** ISE および FMC 両方の各完全修飾ドメイン名 （FQDN）のために、正しい DNS レコードが DNSサーバで設定されることを確かめて下さい。

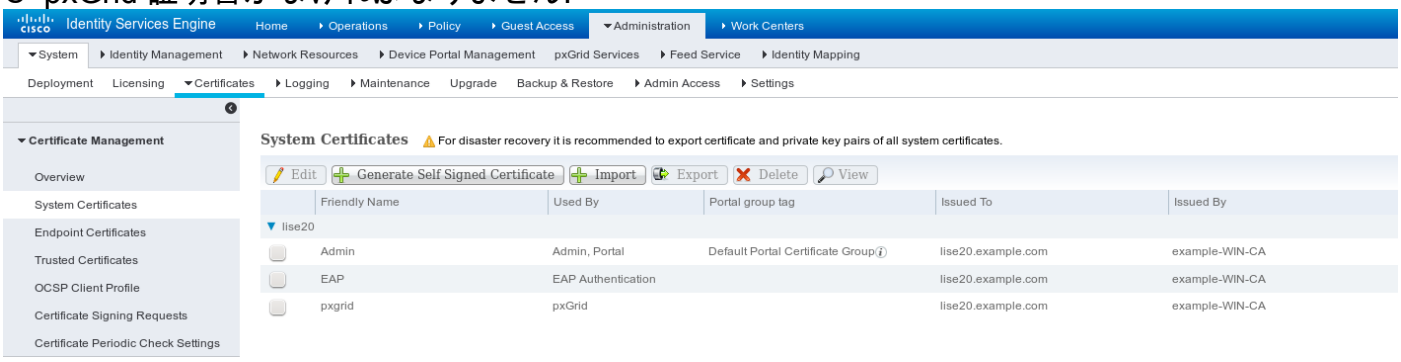
Admin と pxGrid 証明書の唯一の違いは署名プロセスとあります。 pxGrid 証明書が伸びたにちがいないので両方でキー使用法オプションはそれに Microsoft CA のクライアント および サーバ認証カスタム テンプレート使用することができます:



方法マイクロソフトのWeb サービスを pxGrid CSR に署名するのに利用するこのイメージで示されています:

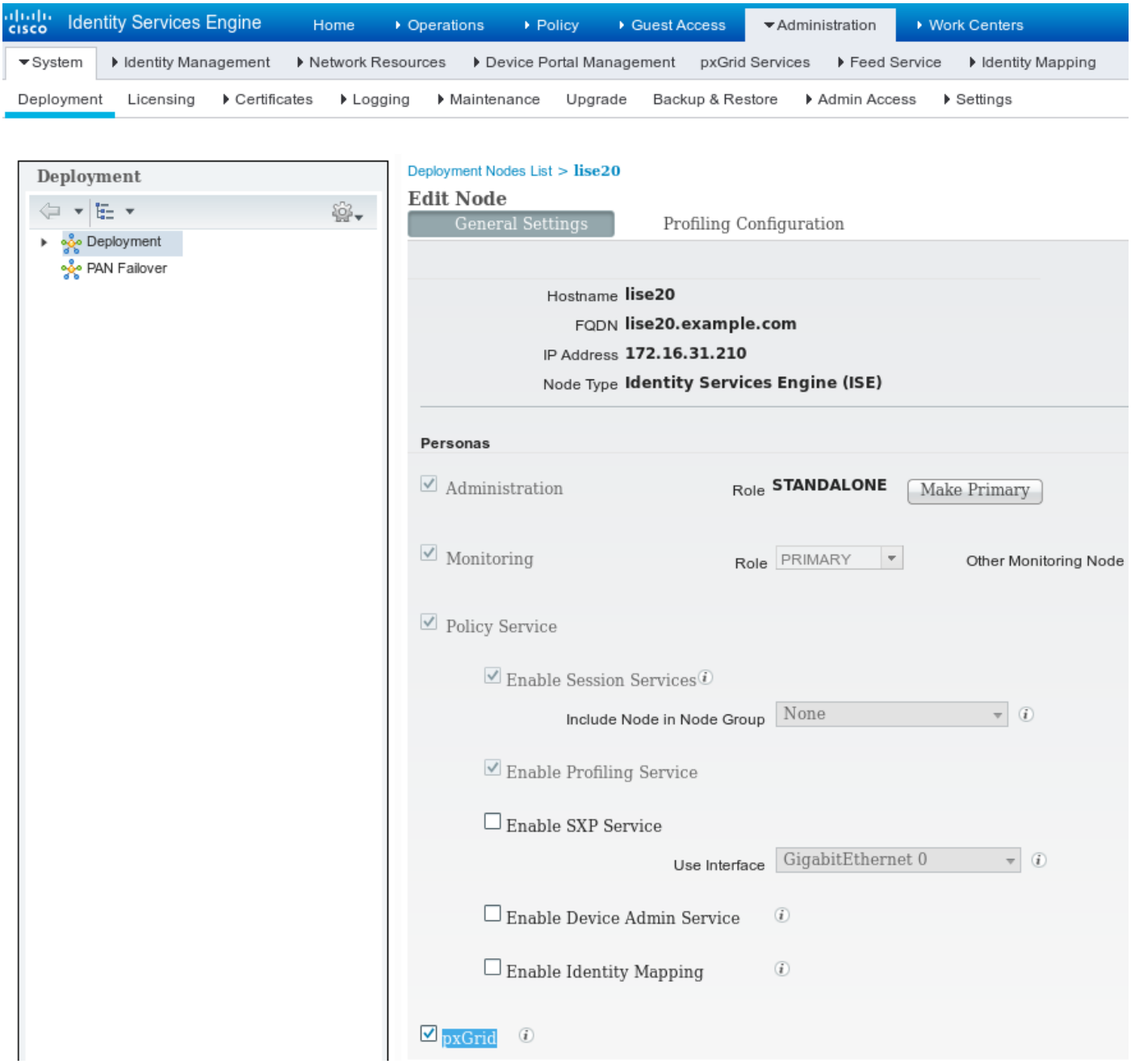


端に ISE はこのイメージに示すように信頼された CA （ Microsoft ）によって署名する Admin および pxGrid 証明書がなければなりません:

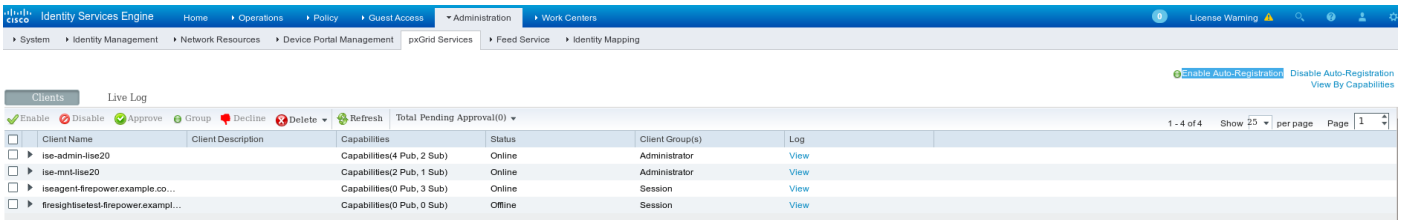


pxGrid サービス

正しい証明書によって特定のノードのための pxGrid 役割はこのイメージに示すようにイネーブルになる、必要があります:



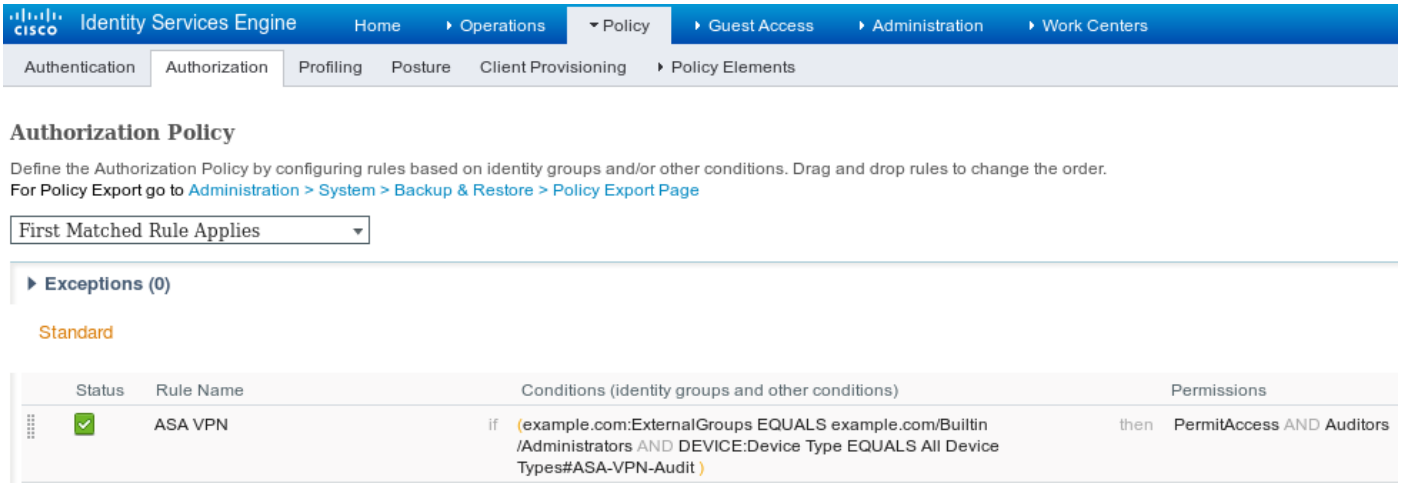
そして自動承認はイネーブルになったに設定する必要があります:



認可ポリシー

デフォルトの認証 ポリシーはローカルユーザがない場合）使用されます（AD ルックアップは実行された。

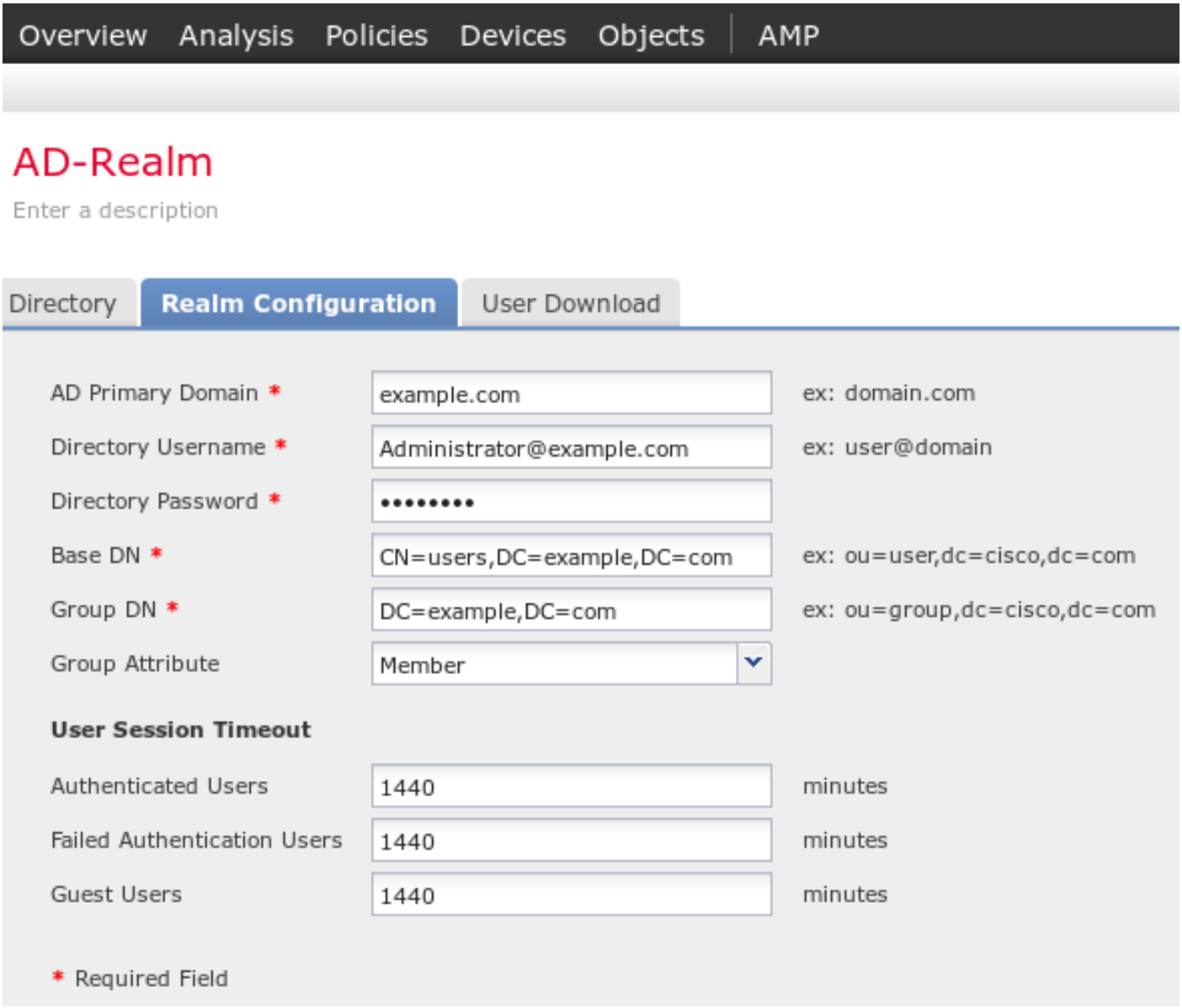
承認ポリシーは完全なネットワーク アクセス（権限を提供するために設定されました: ASA-VPN によって認証し、アクティブ ディレクトリ グループ管理者に属しているユーザ向けの PermitAccess）-それらのユーザ SGT タグ オーディタのために...戻されます:



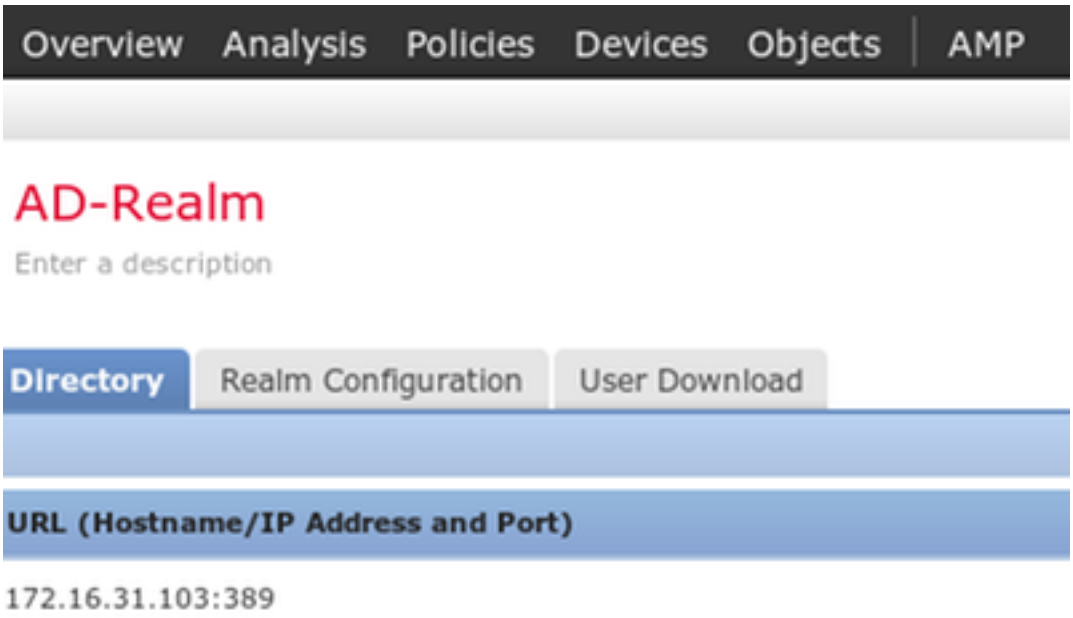
FMC

アクティブ ディレクトリ レルム

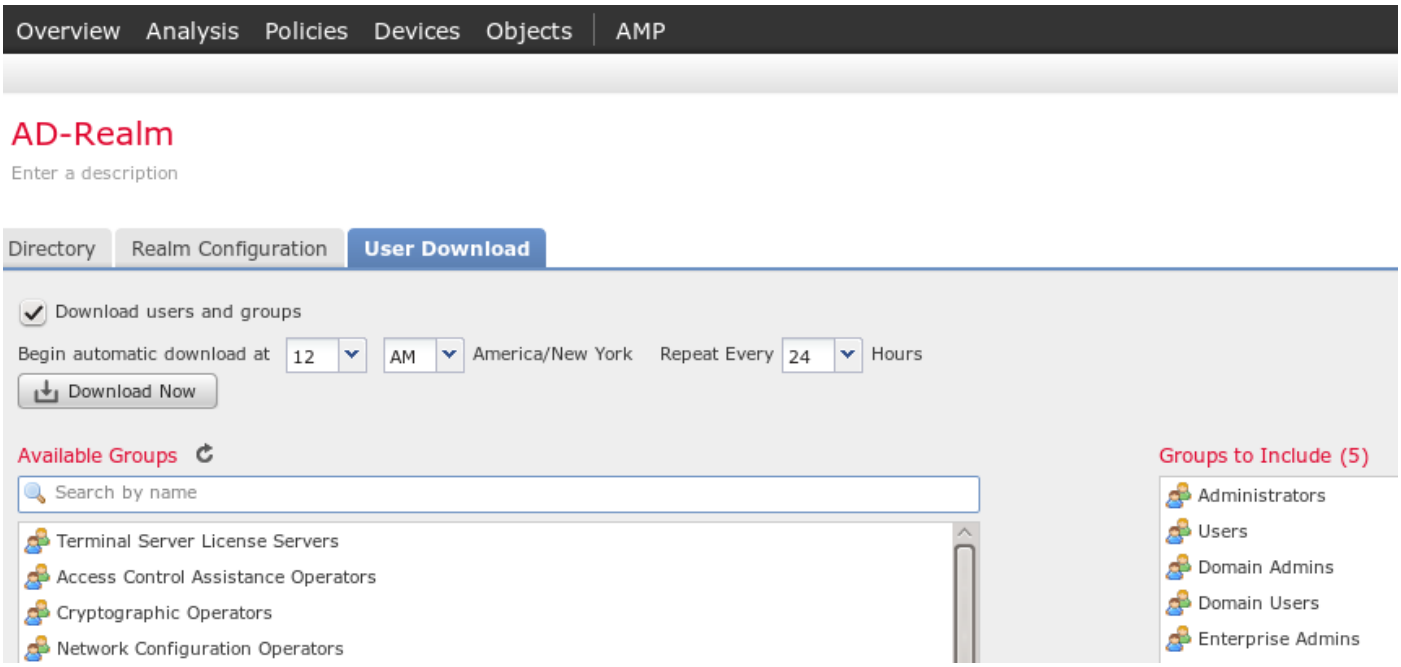
ISE 統合と機能するためにレルム設定が必要となります（識別ポリシーを使用し、団体会員を向けに受動的に取得するため認証済みユーザ）。 レルムはアクティブ ディレクトリか Lightweight Directory Access Protocol（LDAP）のために設定することができます。 この例で AD は使用されています。 **システム > 統合 > レルム**から:



標準ディレクトリ設定は使用されます:

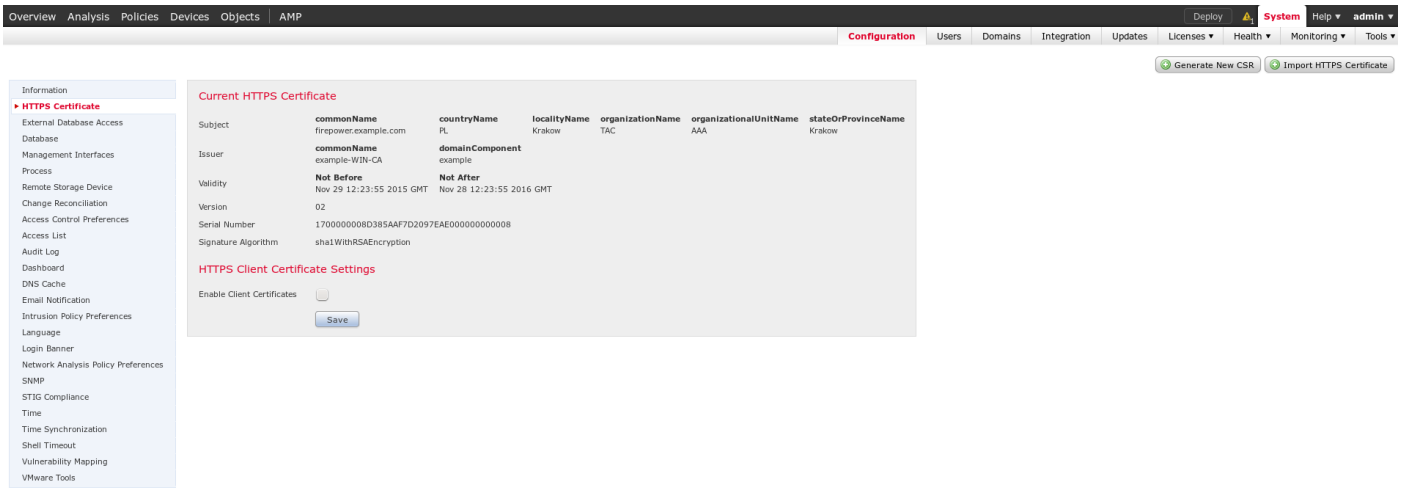


そしてアクセス制御の追加状態が支配するように）いくつかの AD グループは取得されます（使用されるため:



Admin および pxGrid のための証明書

必要とされない、admin アクセスのための CSR を生成する好ましい習慣が。 このイメージに示すように信頼された AD を使用してその CSR に、インポート署名入り認証、署名して下さい:



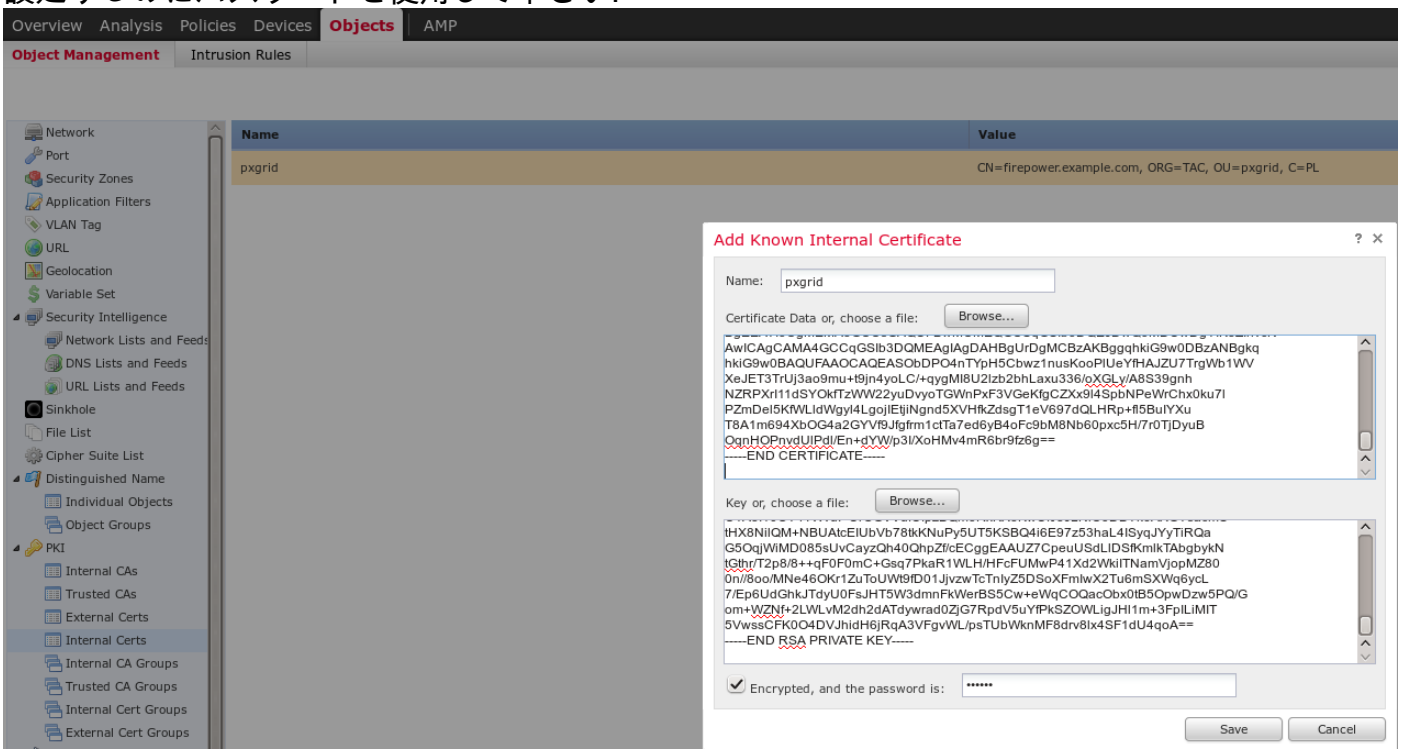
CA 認証は信頼された記憶装置に追加される必要があります:

最後のステップは ISE pxGrid サービスに承認するのに FMC によって使用される pxGrid 証明書

を生成することです。 CSR CLI を生成することは使用される必要があります（または openssl ツールが付いている他のどの外部マシンも）。

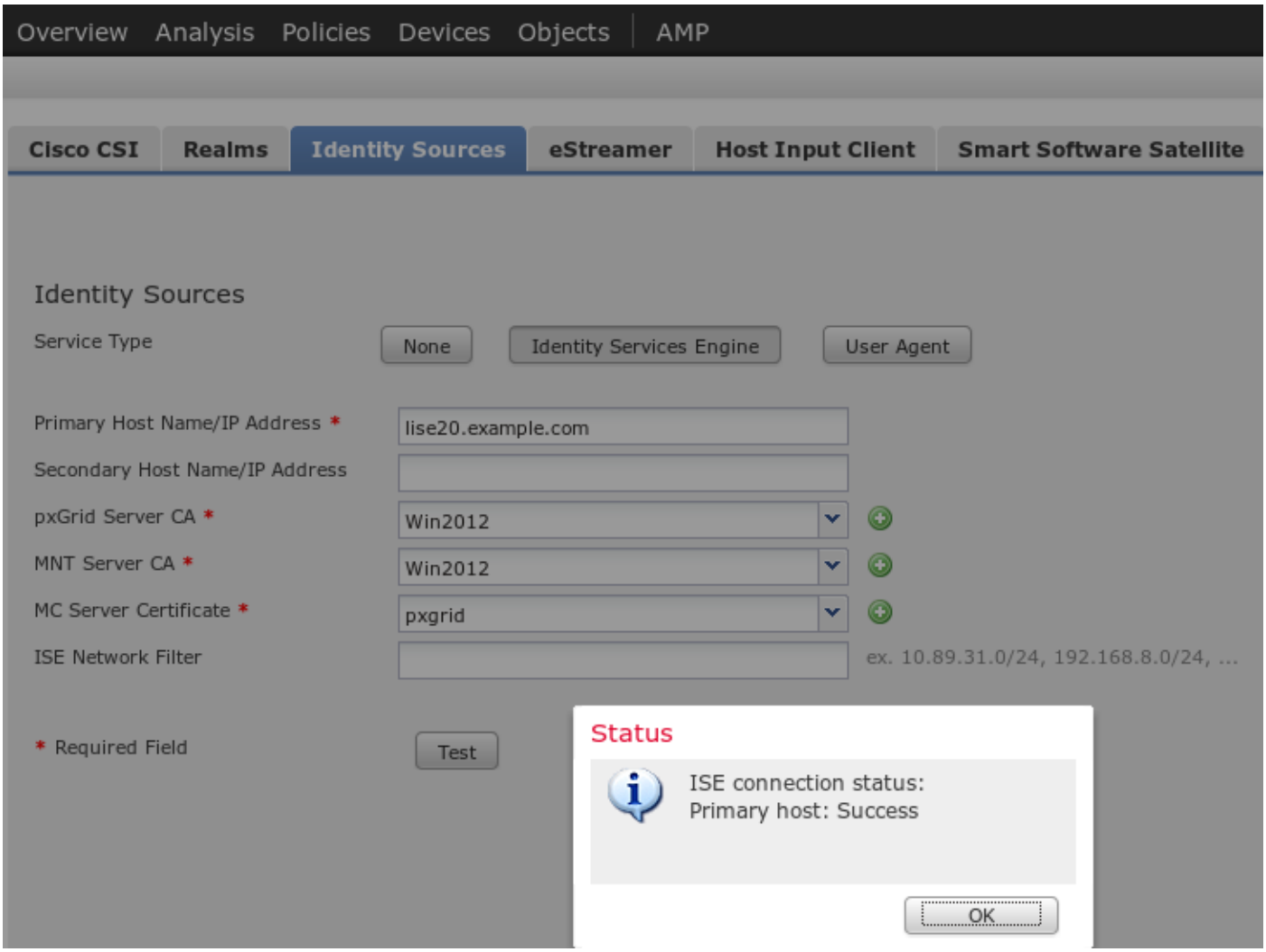
```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
root@firepower:~# openssl genrsa -des3 -out fire.key 4096
Generating RSA private key, 4096 bit long modulus
.........
..............
e is 65537 (0x10001)
Enter pass phrase for fire.key:
Verifying - Enter pass phrase for fire.key:
root@firepower:~#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

生成されて fire.csr は Microsoft CA（pxGrid テンプレート）を使用して、それに署名します。 FMC 内部証明書記憶装置にプライベートキー（fire.key）および署名入り認証（fire.pem）をインポートして下さい。 プライベートキーに関してはキー（openssl **genrsa コマンド**）の生成の間に設定するのにパスワードを使用して下さい:



ISE 統合

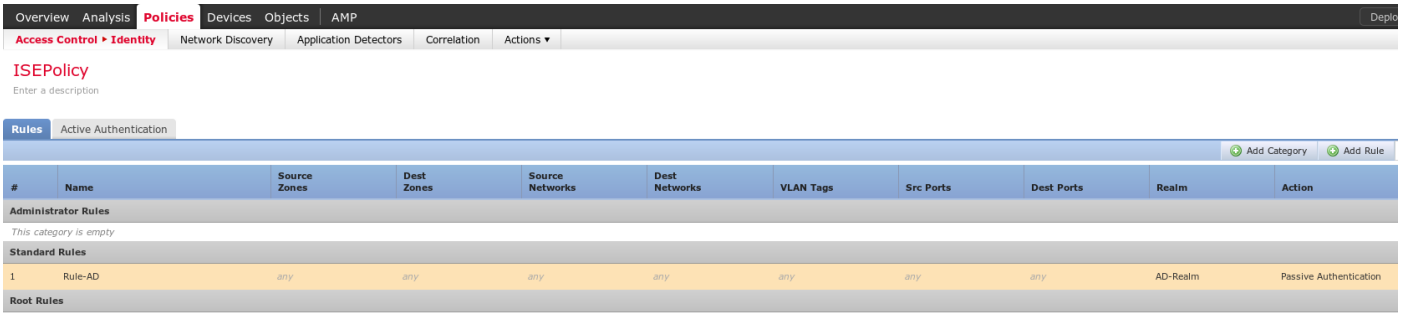
すべての証明書がインストールされていたら**システム > 統合**からの ISE 統合を設定して下さい:



pxGrid および MnT サービス両方証明書 検証のためにインポートされた CA を使用して下さい。マネジメントコンソール（MC）に関しては生成される pxGrid のために内部証明書を使用して下さい。

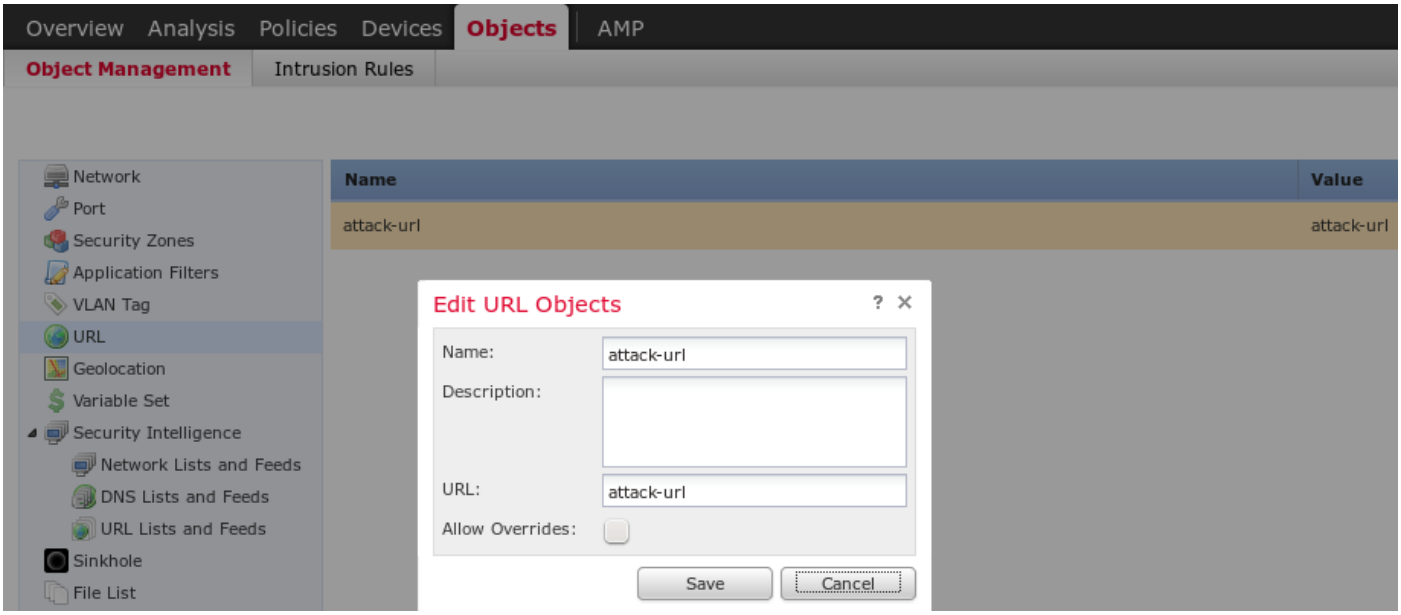
識別ポリシー

識別ポリシーを設定して下さい受動認証のために前もって設定された AD レルムを利用している:

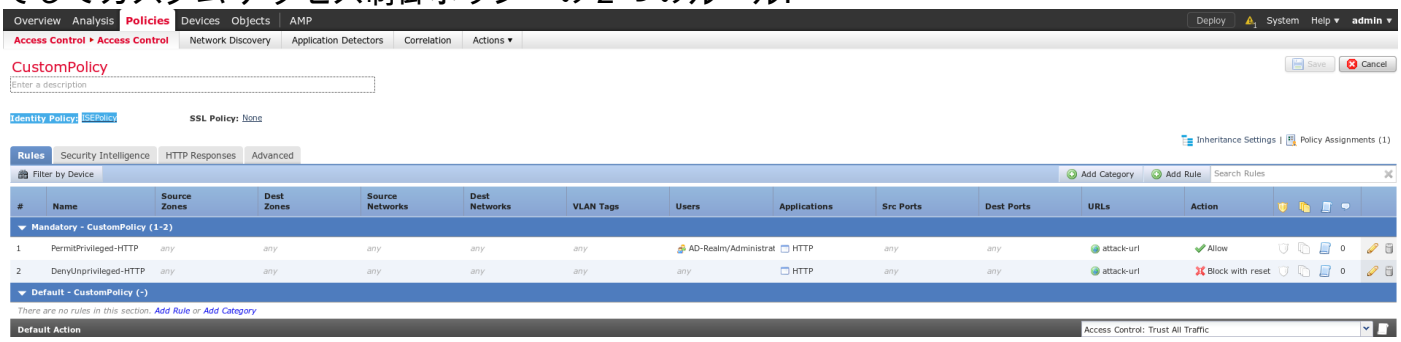


アクセス制御ポリシー

この例に関してはカスタムは URL 作成されました:



そしてカスタム アクセス制御ポリシーの 2 つのルール:

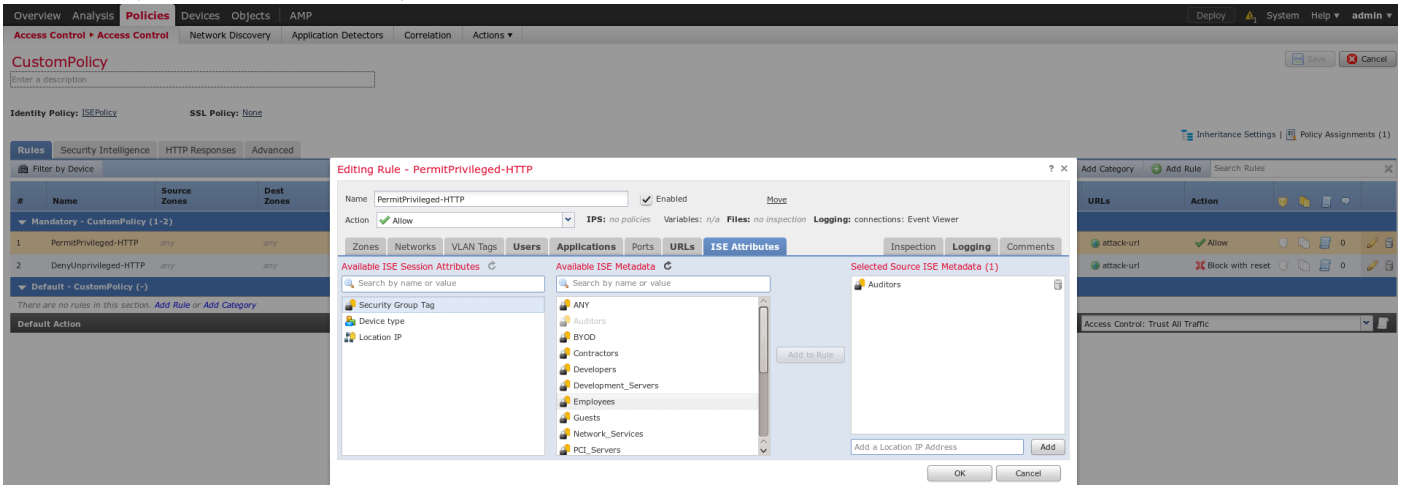


PermitPrivileged HTTP ルールは AD 管理者グループに属している SGT タグを割り当てられたすべてのユーザを割り当てます。 すべてのターゲットの HTTP 不正侵入を実行するオーディタ。

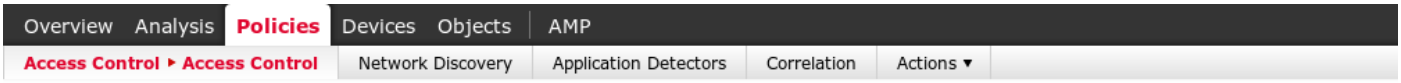
DenyUnprivileged HTTP は他のすべてのユーザにその操作を否定します。

また以前に作成された識別ポリシーがこのアクセス制御ポリシーに割り当てられたことに注意して下さい。

このタブ SGT タグを見ること可能性のあるはしかしそれらで目に見えま特定のルールを作成しているか、または編集します:

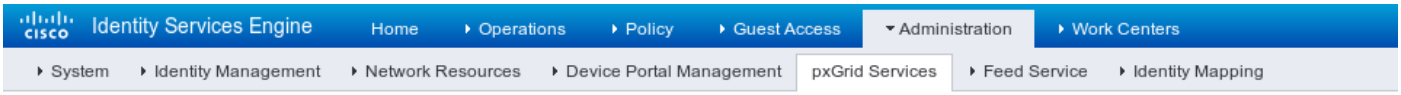


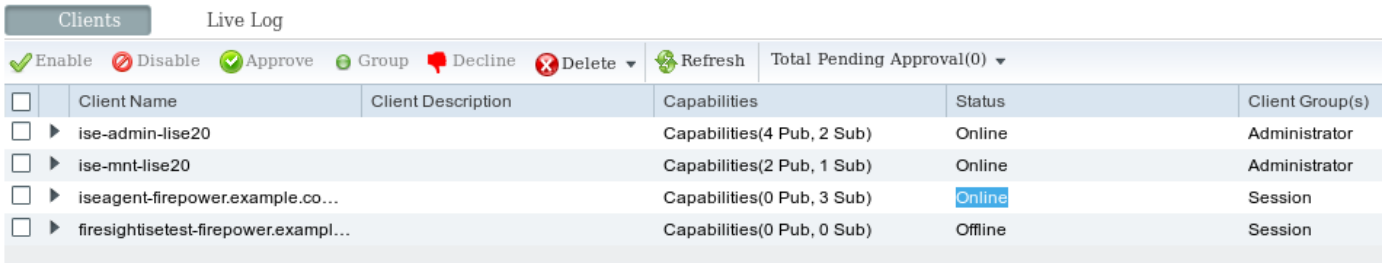
ポリシーが NGIPS に割り当てられ、すべての変更が展開されるようにして下さい:



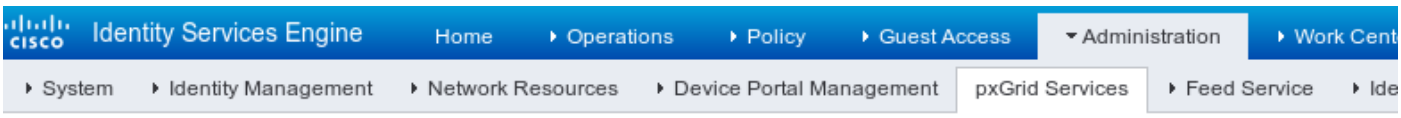
確認

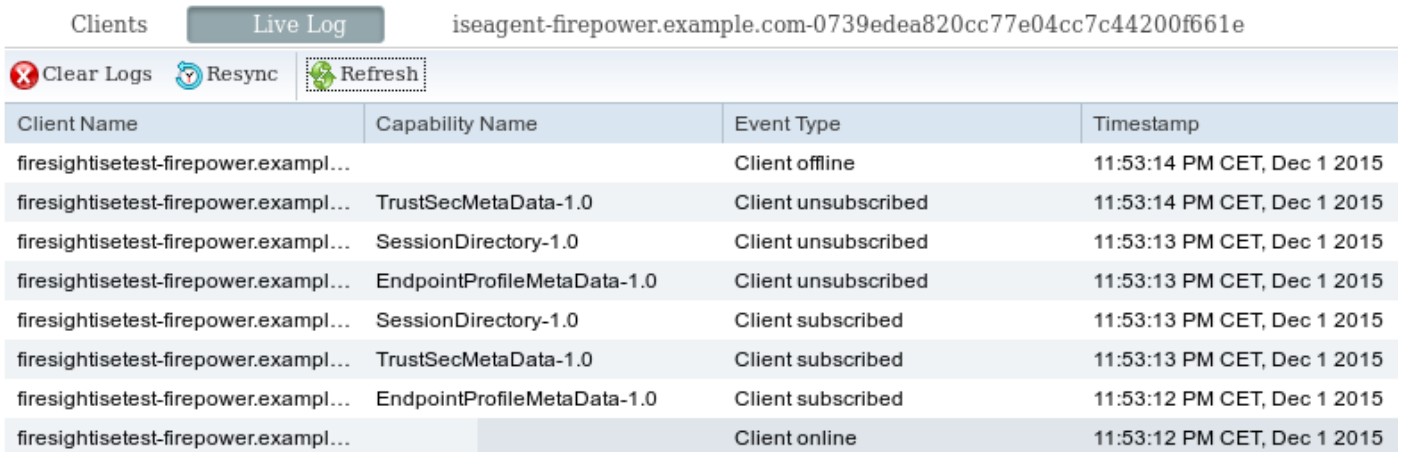
すべてが正しく設定された後 ISE はセッションサービス（オンラインでステータス）については pxGrid クライアントが定期講読することを見るはずです。





ログからまた FMC が TrustSecMetaData（SGT タグ）サービスのために定期講読したことを確認できます-すべてのタグを得、定期講読を解除しました。

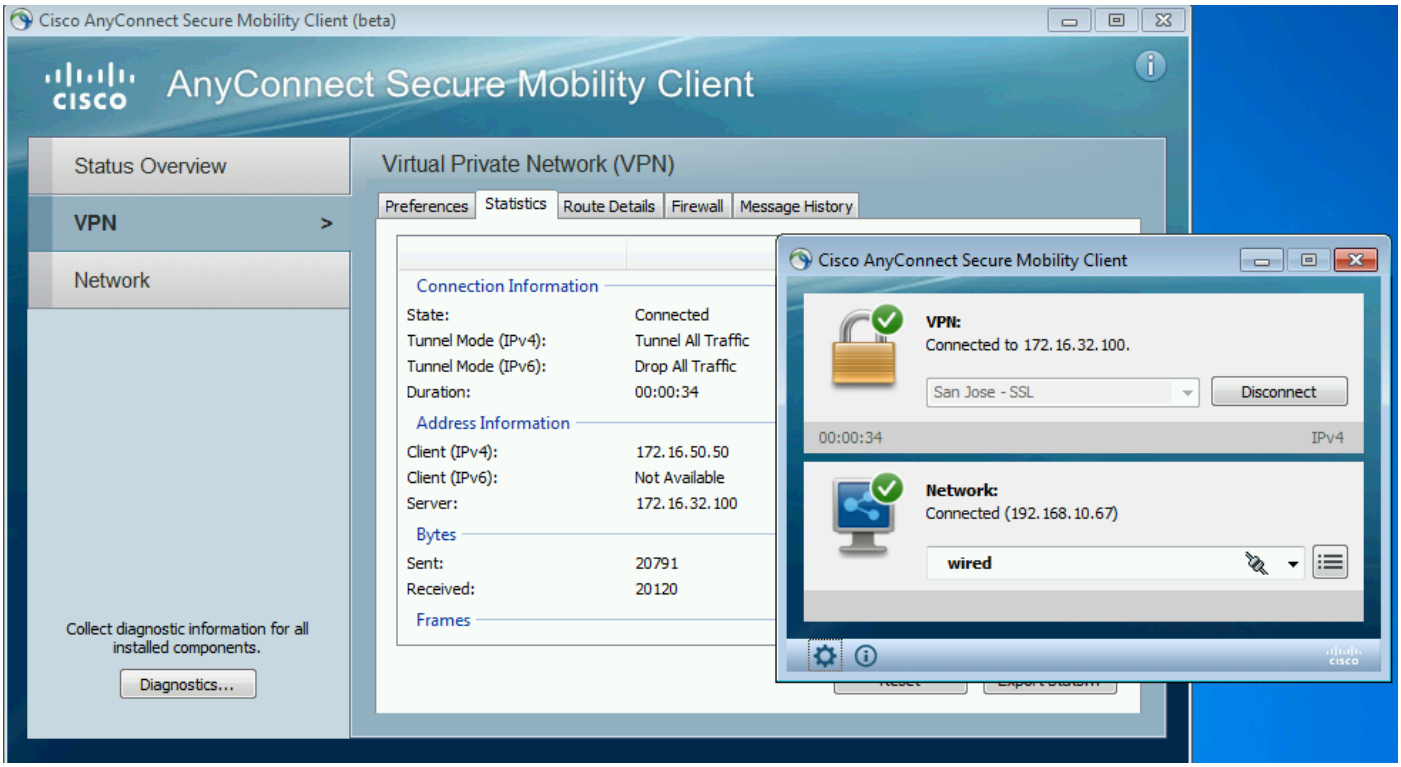




VPN セッション確立

最初のテストはシナリオのために ISE の許可が正しい SGT タグを戻さないとき実行された（NGIPS は監査テストを可能にしません）。

VPN セッションが AnyConnect ユーザインターフェイス（UI）の上により多くの詳細を提供できればあれば:



ASA は確立されますセッションを確認できます:

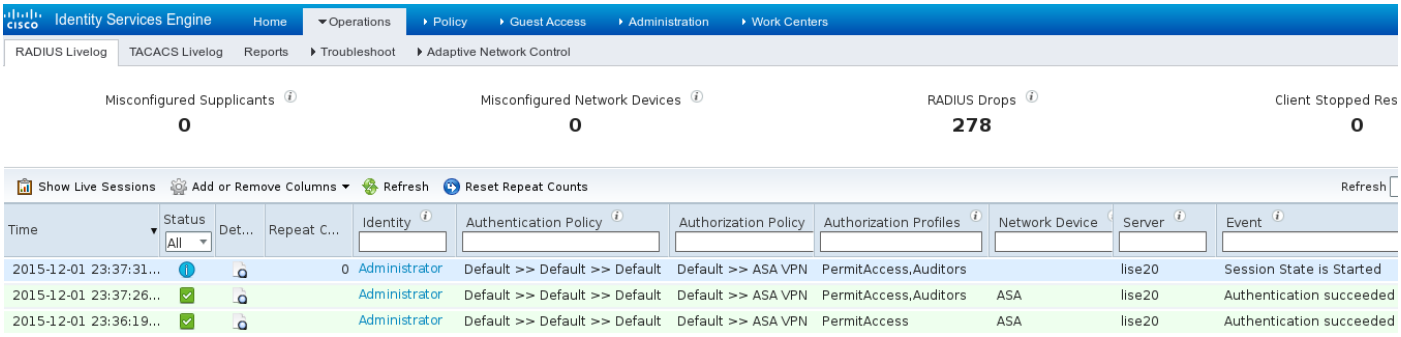
```
asav# show vpn-sessiondb anyconnect

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

ASA がこの認証については戻る SGT タグを見ることに注意して下さい。 ASA は TrustSec のために-情報がとにかくスキップされるように設定されません。

ISE はありまた認証の成功（23:36:19 のログ）-戻る SGT タグ報告します:



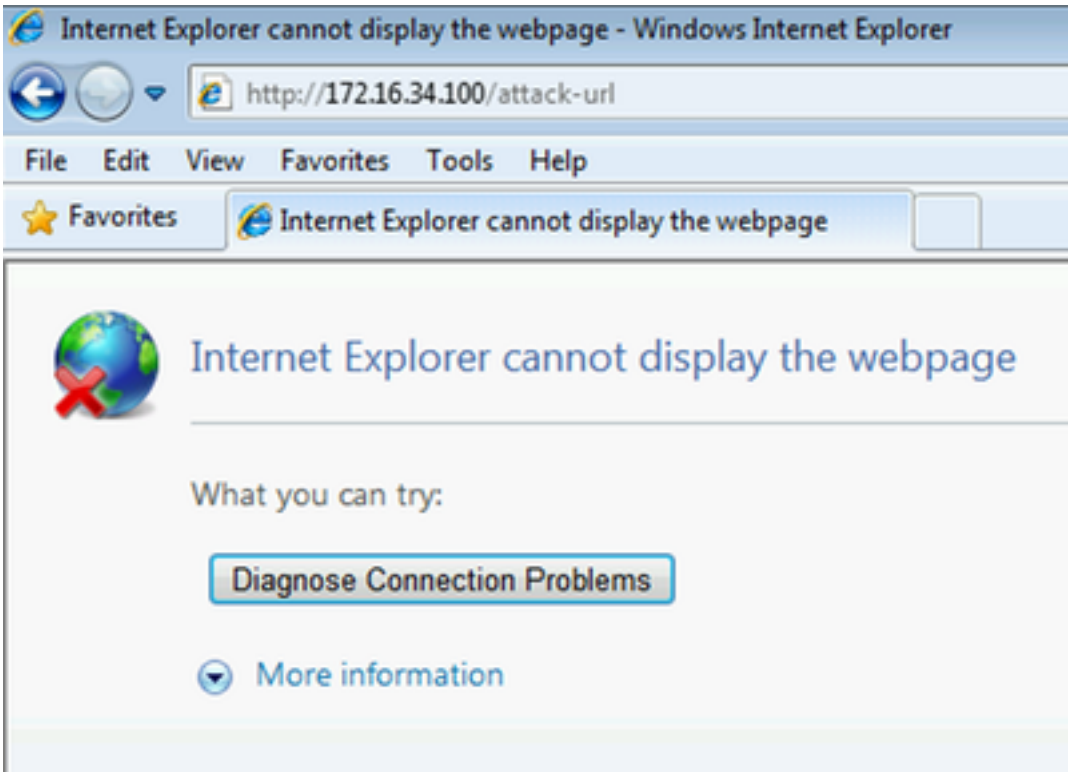
MnT からセッションデータを入手する FMC

そのステージで /var/log/messages の FMC は団体会員の管理者のユーザ名および peform AD ルックアップのための新しいセッションを（pxGrid サービスのためのサブスクライバとして受け取った）報告します:

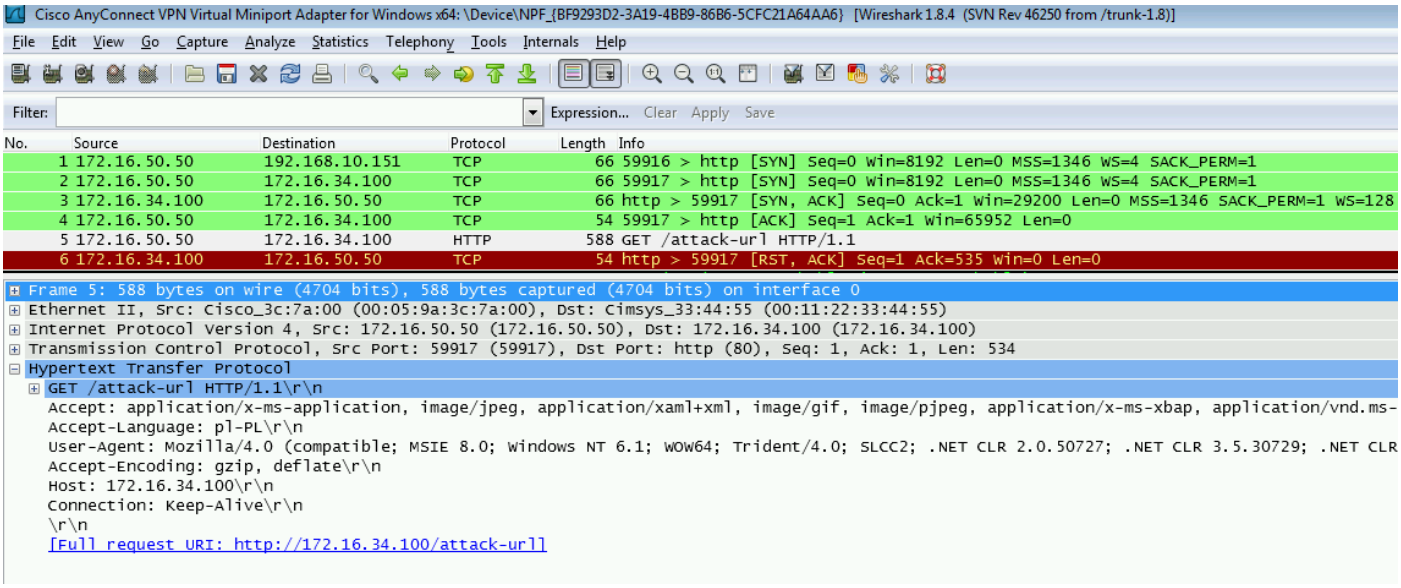
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search
'(|(sAMAccountName=Administrator))' has the following DN:
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

権限のなく、特権ネットワーク アクセス

そのステージでユーザは Webブラウザを開くことを試み、場合監査されたサーバにアクセスするために、接続は終わります:



それはクライアント（FMC 設定による TCP RST 送信）から奪取 される パケットキャプチャによって確認することができます:

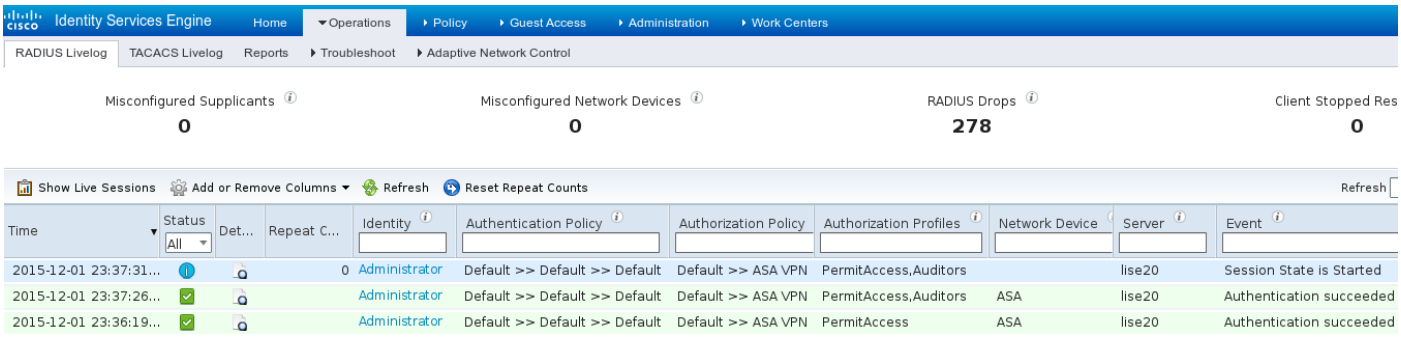


ISE が戻るために設定されれば監査タグ ASA セッションは報告します:

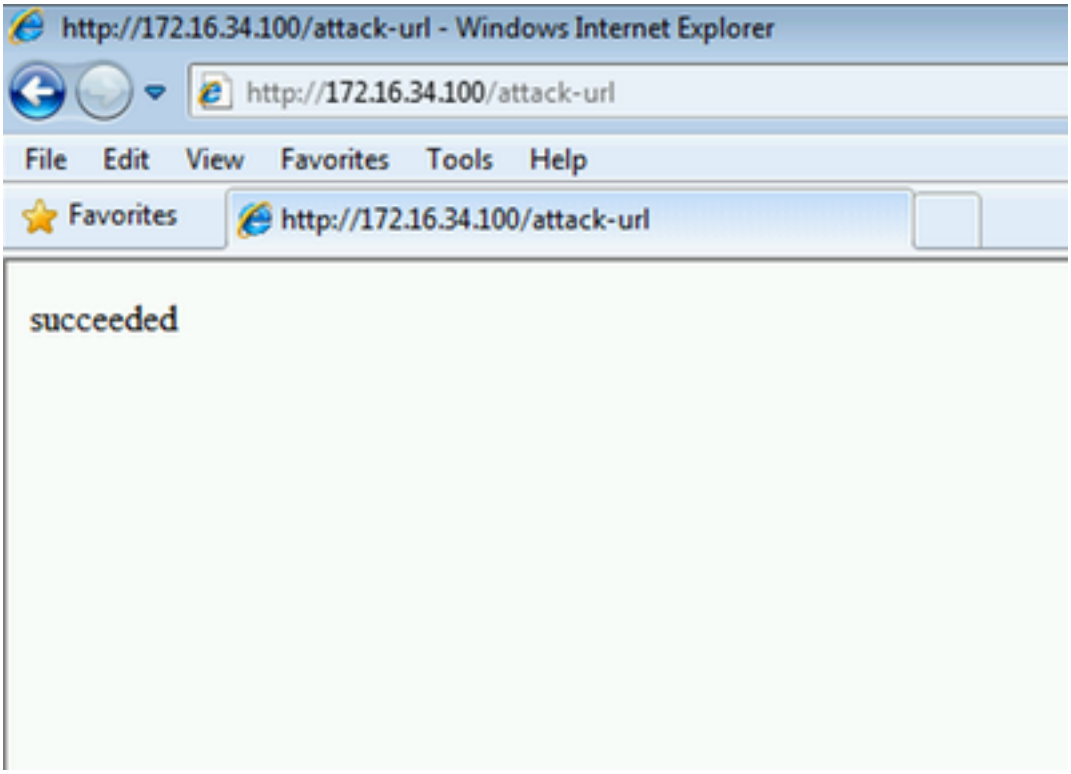
```
asav# show vpn-sessiondb anyconnect

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 はまた報告します認証の成功（23:37:26 の口グ）- SGT タグ オーディタを戻りますあります

:

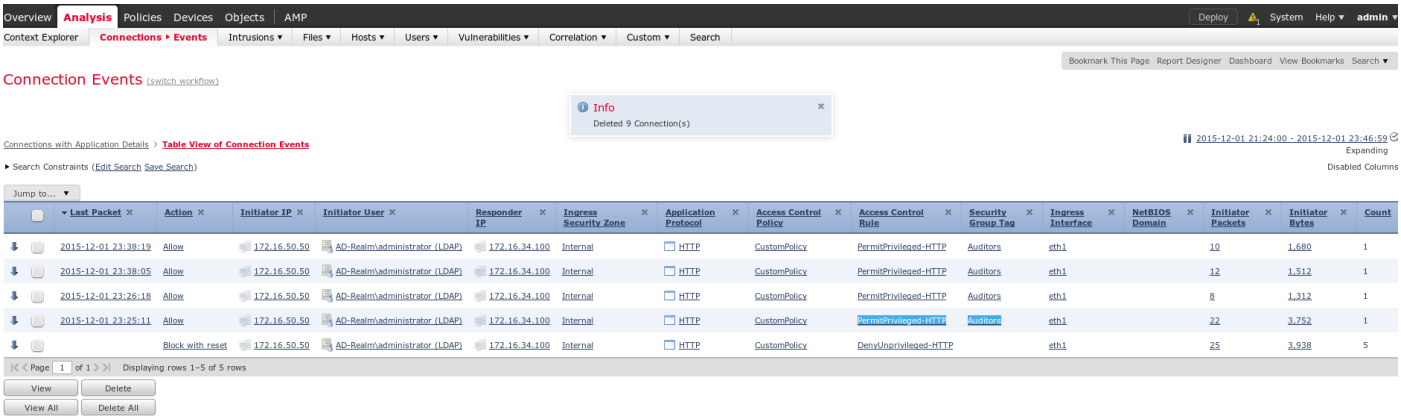


そしてユーザは述べられたサービスにアクセスできます:



FMC ロギング アクセス

このアクティビティは接続イベント レポートによって確認することができます:



最初に、ユーザは SGT タグを割り当ててもらわなかったし、DenyUnprivileged HTTP ルールを見つけていました。 オーディタのタグが ISE（割り当てられ、FMC によって取得されました）ルールによって、PermitPrivileged HTTP は使用され、アクセスは許可されます。

またディスプレイを持つためにそれに注意して下さい普通アクセス制御ルールおよびセキュリティグループ タグが最後のカラム表示されるので複数の列は取除かれました (および水平スクロール バーの 1 として使用される必要があります)。 カスタマイズされたビューは将来保存され、再使用することができること。

トラブルシューティング

FMC デバッグ

識別 サービスに責任がある adi コンポーネントのログをチェックするために /var/log/messages ファイルをチェックして下さい:

```
[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
```

より詳しくなるためにそれをです adi プロセスを (sudo の後のルートから) 強制終了し、デバッグ引数とそれを実行すること可能性のあるデバッグします:

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

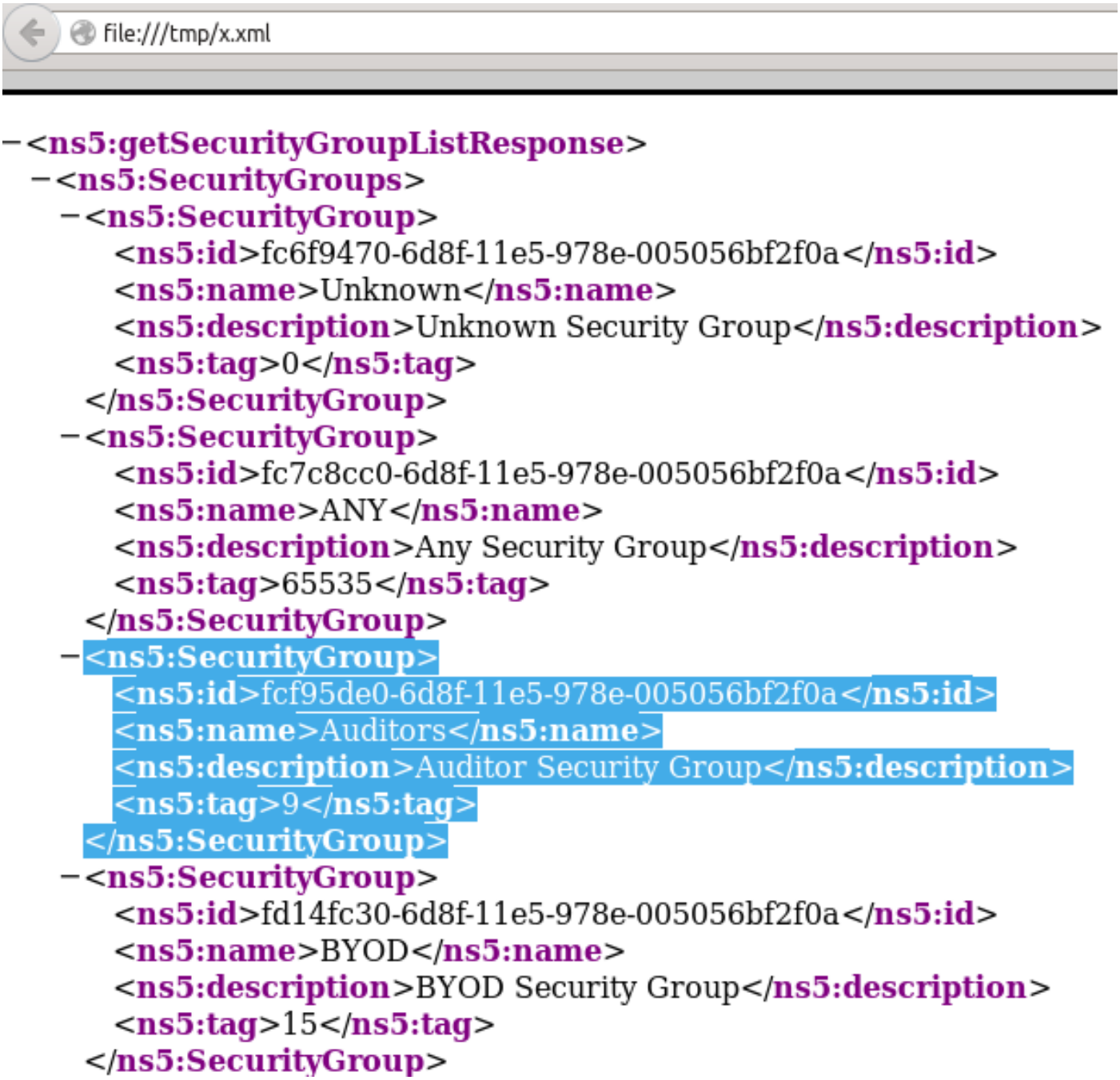
pxGrid による SGT クエリ

オペレーションはアクセス制御ポリシーのルールを追加している間 **Test ボタンが ISE 統合セクション**でクリックされるか、または SGT リストがリフレッシュされるとき実行されます。

```
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>]

よりよいビュー XML の場合その口グから内容は XML ファイルにコピーされ、Webブラウザによって開くことができます。 仕様 SGT （監査）が受け取られている、また他の SGT がすべて ISE で定義されていることを確認できます:



他 API への MnT によるセッション クエリ

それはまた MnT ホスト名およびポートが pxGrid によって渡されることに) テストオペレーションの一部です (注意して下さい。 バルク セッション ダウンロードは使用されます:

```
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>]

そして解析された結果 (受け取った 1 人のアクティブセッション) :

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}
```

そのステージで NGIPS はレルム AD ユーザ名にそのユーザ名（およびドメインを）関連させることを試みますあります:

```
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 がユーザおよび団体会員を見つけるのに使用されています:

```
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 デバッグ

pxGrid コンポーネントのためのトレース レベル デバッグをイネーブルにした後各オペレーションをチェックすること可能性のある（しかしペイロード/データなしで FMC で好んで下さい）。

SGT タグ検索を用いる例:

```
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
```

バグ

CSCuv32295 - ISE はユーザ名フィールドのドメイン情報を送信 するかもしれません

CSCus53796 -他バルク クエリのためのホストの FQDN を得ることが不可能

CSCuv43145 - PXGRID 及び識別マッピング サービス再起動、信頼ストアのインポート/削除

参考資料

- ISE と Firepower の統合での修復サービスの設定
- 分散 ISE 環境の pxGrid の設定

- Cisco pxGrid が付いている証明書を展開するハウツー: CA 署名付き ISE pxGrid ノードおよび CA 署名付き pxGrid クライアントの設定
- IPS pxLog アプリケーションとの ISE バージョン 1.3pxGrid 統合
- Cisco Identity Services Engine 管理者ガイド リリース 2.0
- Cisco Identity Services Engine リファレンス ガイド、リリース 1.2 –外部 RESTful S への紹介…
- Cisco Identity Services Engine リファレンス ガイド、リリース 1.2 –監察 RES への紹介…
- Cisco Identity Services Engine 管理者ガイド リリース 1.3
- テクニカル サポートとドキュメント – Cisco Systems