

# تام دځل FirePOWER چم دو ISE ءاطخأ فاشك تسأ اه حال صا و ةي وهلا

## تا يوت حمل

[ةمدقملا](#)

[ةيساس ال ا تابلطت ملا](#)

[تابلطت ملا](#)

[ةمدختس ملا تانوك ملا](#)

[نيوكتلا](#)

[ةكبش ل ل يطيطختلا مسرلا](#)

[\(ISE\) ةي وهلا فشك تامدخ كرحم](#)

[ةمدخ Active Directory](#)

[ةكبش ل ل ا لوصولا زاځ](#)

[MnT و pxGrid ل تاداهش](#)

[pxGrid ةمدخ](#)

[ل يوختللا ةسايس](#)

[FMC](#)

[Active Directory قاطن](#)

[Admin و pxGrid ل تاداهش](#)

[ISE لمكت](#)

[ةي وهلا ةسايس](#)

[لوصولا ي ف مكحتلا ةسايس](#)

[قحصلا نم ققحتلا](#)

[VPN ةسلج ءاشنا](#)

[MnT نم ةسلجلا تانايب ل صلح ي FMC](#)

[تازايتما و ا تازايتما ي ا نود ةكبش ل ل ا لوصولا](#)

[FMC ل ي ج ست ل ل ا لوصولا](#)

[اه حال صا و ءاطخأ ل فاشك تسأ](#)

[FMC ءاطخأ ح ي حصت](#)

[PXgrid رب ع SGT م العتسا](#)

[MnT ل ل REST API رب ع لمعلا ةسلج م العتسا](#)

[ISE ءاطخأ ح ي حصت](#)

[تارشح](#)

[عجارملا](#)

## ةمدقملا

اه ءاطخأ فاشك تسأ او TrustSec ل ةكردم تاسايس نيوكت ةي ف ي ك دن تس ملا اذه فص ي NGIPS معد ي Cisco. نم (NGIPS) ي ل ل ل ل ي ل ل نم ل ل ف ط ت ل ل نم ةي ام ح ل ل ما ظ ن ل ل ع اه حال صا و ةكردم تاسايس ءاشناب حم سي ي ذل ا Identity Services Engine (ISE) عم لمكت ل ل 6.0 رادصل ا ةي وهلا ل .

# ةيساسألا تابلطتملا

## تابلطتملا

ةيلالاتلا عيضاوملاب ةفرعم كيذل نوكت نأب Cisco ي صوت:

- Cisco نم VPN (ASA) فيكتلل لباقل نامأل زاا نيوكت
- Cisco AnyConnect Secure Mobility Client نيوكت
- Cisco نم FirePOWER ةراذل زكرم يساسألا نيوكتلا
- Cisco ISE نيوكت
- Cisco TrustSec لولح

## ةمدختسملا تانوكملا

ةيلالاتلا ةيداملا تانوكملا وجماربال تارااصلإل دنننسملا اذف ةدراولا تامولعمل دنننست:

- Microsoft Windows 7 ليغشتلا ماظن
- Microsoft Windows 2012 (CA) ليغشتلا ماظن ةداهشل قءصملا عجرملا
- Cisco نم 9.3 رادصلإلا ASA
- Cisco ISE، جم انرب 1.4 تارااصلإلا
- Cisco AnyConnect Secure Mobility Client، رادصلإلا 4.2
- Cisco، رادصلإلا 6.0 نم FirePOWER (FMC) ةراذل زكرم
- Cisco FirePOWER NGIPS، رادصلإلا 6.0

## نيوكتلا

نم ناعون كانه FirePOWER ةراذل يساسألا ماظنلا (FMC) ةراذل زكرم ءي قيوستلا ءو فيظوتلا تامءل لماءاب ءقل ءعمل ءيظوتلا:

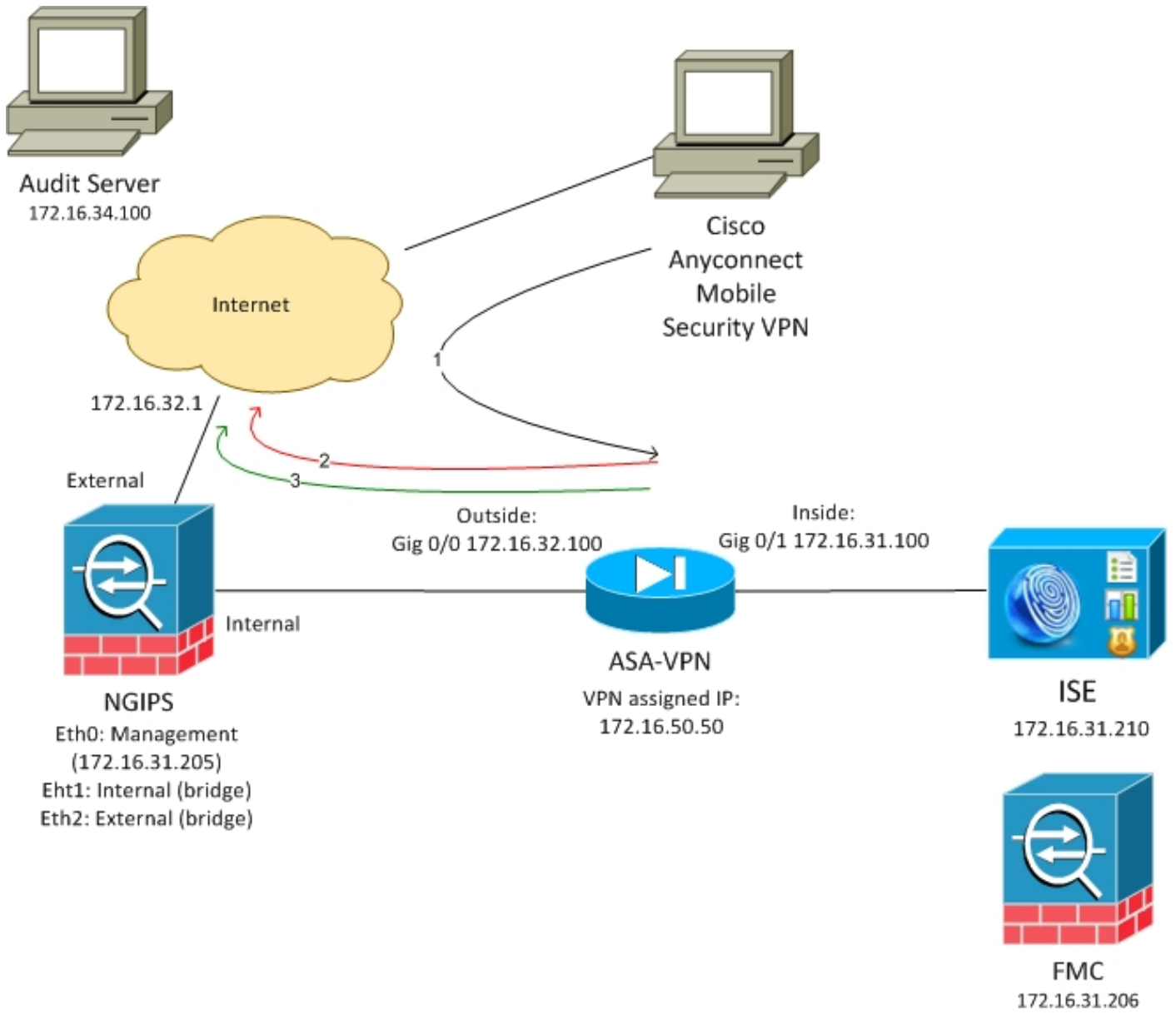
- ليظوتلا ءلاا ريغت لعل لمعت يالا، ISE ربع مءاهملا لزع FMC ل حمسي - ءالصإلا نالاچ كانه. ءكبشلا لءل اءءوم الوصو رفوي يذلا لوصولا زاا لعل يكيمائيء لكشب للءلا اذف نم:

1. ءمدءل (API) تاقيبطتلا ءجمرب ءءا وءاءءءسا مءءءءسا ب مءءقلا Perl ل يصن جم انرب ISE. ءي ءرطا ءءقنلا ءي ءماء (EPS).
2. ءيظمنلا ءءوللا (هءه) ل ISE ل pxGrid لوكوئورب مءءءءسا ب ءءءا ءيظمن ءءو وءاءءءسا ل. (6.1) ي ءءءملا يءصألا مءءلا، 6.0 ي ءم وءءم ريغ - 5.4 رادصلإلا ي ءءق ءءمءم.

- TrustSec نام ءمومءم تامالء لءل اءانءسا تااسا يساسألا نيوكتب FMC ل حمسي - ءهنلا (SGT).

ءءارملا مسق ءءارق ءاچرلا، ءالصإلا لاءم لءا نم. ءينائل ءفيظوتلا لعل ءلاقملا هءه زكراء

## ءكبشلا لءيظمءءلا مسرلا



نيتدعاق ىلع يوتحي يذلا لوصولو ي ف مكحتلا جهن مادختساب FMC نيوكت متي

- صصخم URL مادختساب HTTP رورم ةكرح صفر (attack-url)
  - ةلاح ي ف طقف نكلو (attack-url) صصخم URL مادختساب HTTP رورم ةكرح ب حامسلا ISE ةطساوب (9) قيقدتلا بيقر ةمالعل مدختسملا نييعت
- ىلإ نومتنني نيزال Active Directory مدختسم عي مج ىلإ قيقدت ةمالع نييعت ISE ررقي ةكبشلا ىلإ لوصولل ASA-VPN زاهج مدختسيو نيولوؤسملا ةومجم

ىلإ لوصولو مدختسملا لواحي مث. ASA ىلإ VPN لاصتا ربع ةكبشلا ىلإ مدختسملا لوصولو ننييعت متي مل هنال لشفي هنكلو - موجهلل URL ناو نع مادختساب هقيقدت مت يذلا مداخل لاصتالاجني، كلذ حالصا درجمبو. قيقدتلا بيقر ةومجم ىلإ

## ISE) ةيوهلا فشك تامدخ كرحم

### مدخ Active Directory

Administrators ةومجم مادختسا متي) ةحيحصلا تاومجملا راضحا بجي و AD لمات نيوكت بجي (ليوختلا ةدعاق طرشل

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

## تكوين الواجهة للوصول إلى إيدنتي

وهو أمر مهم، خاصة في حالة إعداد ASA-VPN-Audit. تكوين الواجهة هو جزء من إعداد ASA. هذه هي الخطوات:

Network Devices List > ASA

**Network Devices**

\* Name: ASA

Description: [Empty]

\* IP Address: 172.16.31.100 / 32

\* Device Profile: Cisco

Model Name: [Empty]

Software Version: [Empty]

\* Network Device Group

Location: All Locations [Set To Default]

Device Type: ASA-VPN-Audit [Set To Default]

RADIUS Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

\* Shared Secret: [Masked] [Show]

## إعداد MNT و pxGrid

إعداد ISE للتحقق من الوصول (FMC) إلى الواجهة:

- إعداد SGT و PROFILE
- إعداد MNT (MnT) للتحقق من الوصول

وهو أمر مهم، خاصة في حالة إعداد FMC. الخطوات هي:

1. إعداد الواجهة للتحقق من الوصول (MNT) للتحقق من الوصول.

2. إعداد الواجهة للتحقق من الوصول (MNT) للتحقق من الوصول.

3. إعداد الواجهة للتحقق من الوصول (MNT) للتحقق من الوصول.

طوق ماقرالال نم الدب بيقرال عامسا معدت اهناف عامسالال هرادا س كع ىلع .ASA لثم (فورال

ةداهش) ىرخالال مةدخالل يفة قثلال ىلإ FMC و ISE نم لك جاتحي ،تابللطتملا هذه ببسبو نم لك ةداهشلل PxGrid مةدختستو ،طوق مةدخالل ةداهشلل MnT مةدختسي مةدخالل اولي مةل.

تاداهشلال ةفاك عي قوتل Microsoft CA مةدختسي

(CSR) ةداهشلال عي قوت بلط عاشناب ISE موقوي نأ بجي ،(لوؤس ملال رود) MnT ىلإ ةبسنلاب ةروصلال هذه يفضوم وه امك

**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

Allow Wildcard  Certificates

**Node(s)**

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input type="checkbox"/> ise20	ise20#Admin

**Subject**

Common Name (CN)

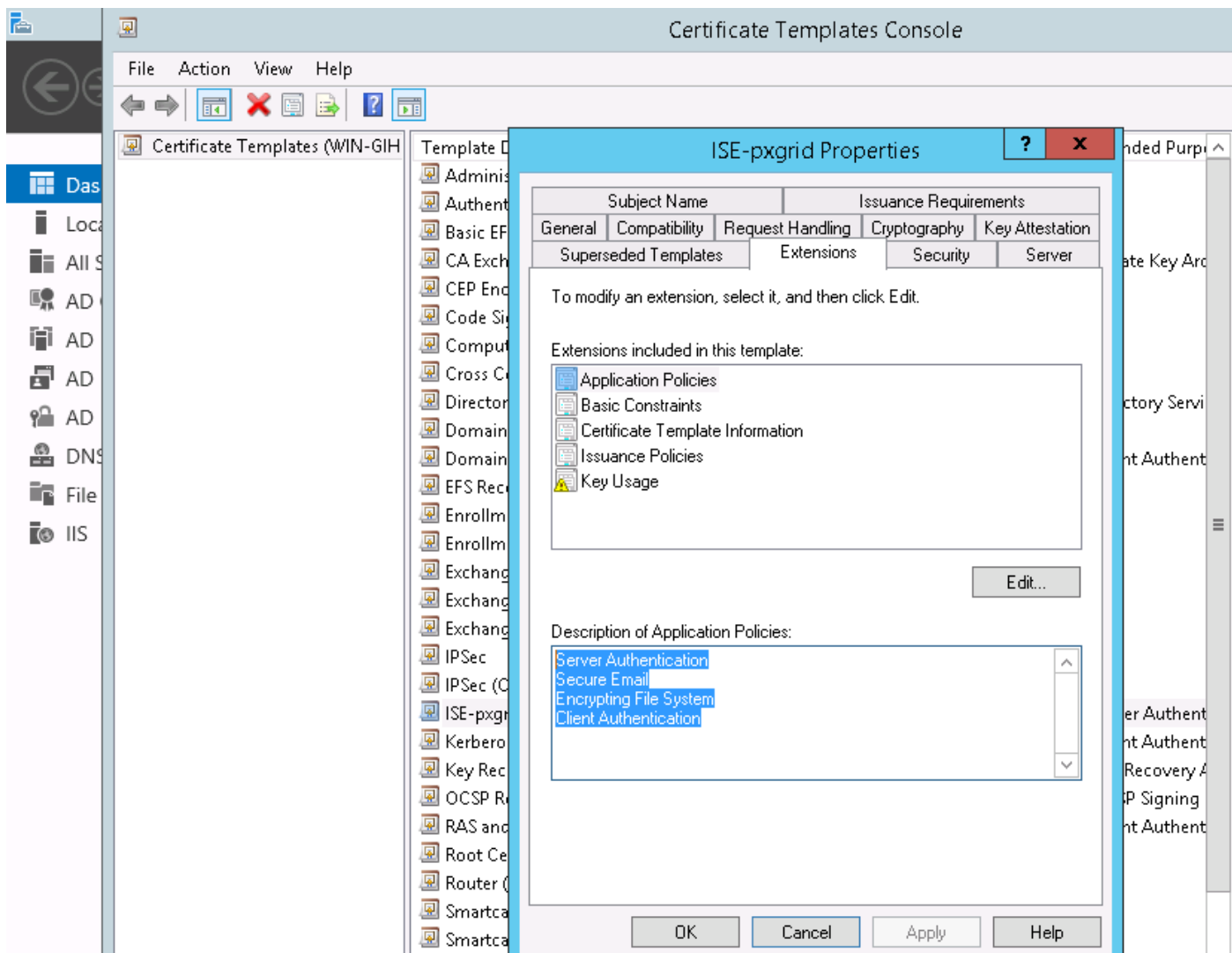
ةداهشلال طبر راخي ربع هداريتسإ بجي Microsoft CA ةطساوب عي قوتل دعب

بجي راخلل (تاداهشلال) ةداهشلال مةدختسإ متيس .PxGrid مةدخالل ةلثام مةل معةاب تا بجي PxGrid ديدحت

امامت لوبقملا نم ف ،قباطتم عوضوم مسا مهل نيصيخرت كانه نوكت نأ نكمي ال هنأ امب (PxGrid لاثملا لبس ىلع) "o" وأ "نأ" مسقل ةفلتخم ةميق ةفاضإ

لهؤم لاجم مسا لكل DNS مةدخالل ىلع حيحصلال DNS لچس نيوكت نم دكأتلال اءارللا :ةظالم  
FMC و ISE نم لكل (FQDN) لمكالب

تاداهش نأ امب .عي قوتل ةل معة يفة وه PxGrid ةداهش و Admin ةداهش نيبة ديجولال قرفلال ةقداصل صصخمل بلالال نم لكل عسوم حاتم مةدختسإ تاراخي نمضتت نأ بجي PxGrid لكذل مةدختسإ نكمي Microsoft CA ىلع مةدخالل اولي مةل



ةروصلإا هذة يف CSR pxGrid عي قوتل Microsoft نم بي وةمدخ مادختسإ ةيفيك رهطت:

## 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:

Submit >

قد صمما عجرملا نم ةعقوم pxGrid و Admin تاداهش ىلع يوتحي نأ يغبني ISE ةياهنلا يف ةروصلا هذه يف حضورم وه امك (Microsoft) ةقثلا

Friendly Name	Used By	Portal group tag	Issued To	Issued By
Admin	Admin, Portal	Default Portal Certificate Group (i)	ise20.example.com	example-WIN-CA
EAP	EAP Authentication		ise20.example.com	example-WIN-CA
pxgrid	pxGrid		ise20.example.com	example-WIN-CA

### pxGrid ةمدخ

ةروصلا هذه يف حضورم وه امك، ةني عم ةدقعل حيحصلا pxGrid تاداهشلا رود نيكم ت بجي

**Deployment**

Deployment Nodes List > **lise20**

**Edit Node**

General Settings Profiling Configuration

Hostname **lise20**  
 FQDN **lise20.example.com**  
 IP Address **172.16.31.210**  
 Node Type **Identity Services Engine (ISE)**

**Personas**

Administration Role **STANDALONE** [Make Primary](#)

Monitoring Role PRIMARY [Other Monitoring Node](#)

Policy Service

Enable Session Services [i](#)  
 Include Node in Node Group **None** [i](#)

Enable Profiling Service

Enable SXP Service  
 Use Interface **GigabitEthernet 0** [i](#)

Enable Device Admin Service [i](#)

Enable Identity Mapping [i](#)

**pxGrid** [i](#)

نيكمت ىل عة ئاق ل لتل ة ق ف او مل ل ني ع ت ب ج و :

Clients Live Log

Enable Auto-Registration Disable Auto-Registration View By Capabilities

Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
ise-admin-lise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	<a href="#">View</a>
ise-mnt-lise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	<a href="#">View</a>
iseagent-frepower.example.co...		Capabilities(0 Pub, 3 Sub)	Online	Session	<a href="#">View</a>
fresightsest-frepower.examp...		Capabilities(0 Pub, 0 Sub)	Offline	Session	<a href="#">View</a>

## لي وخت ل ة سايس

ىل ع روث ع ل ا مد ع ل ا ح ي ف AD ش ح ب ا ر ج ا م ت ي ) ي ض ا ر ت ف ا ل ا ة ق د ا ص م ل ا ج ه ن م ا د خ ت س ا م ت ي ( ي ل ح م ل ا م د خ ت س م ل ا ) .

م ت ( PermitAccess : ن ذ ا ل ا ) ة ك ب ش ل ا ل ل ا ل م ا ك ل ل ا ل و ص و ل ا ر ي ف و ت ل ل ي و خ ت ل ا ج ه ن ن ي و ك ت م ت Active Directory ل ل ا ن و ب س ت ن ي و ASA-VPN ر ب ع م ه ي ل ع ة ق د ا ص م ل ا م ت ي ن ي ذ ل ا ن ي م د خ ت س م ل ل ا Sgt Tag ي ق ق د م ا ج ا ر ا م ت ي ن ي م د خ ت س م ل ا ا ل و ه ل ة ب س ن ل ا ب - Group Administrators



### 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

### ق اطن Active Directory

ةيوضع دادرتساو ةيوهال تاسايس مادختسال) ISE لم اكات عم لم علل ق اطنللا نيوك ت مزلي ل ق اطنللا نيوك ت نكمي. (ي بلس لك ش ب مهت ق داصم تمت نذيلا ني مدختس ملل ة ومجمل Active Directory ل اذ ه في ف (LDAP) ل ل دلل ل وصلل في ف خ ل ل و ك و ت و ر ب ل ل و ا Active Directory ق اطنللا > لم اكاتللا > ماظنللا نم AD. مادختس ا

## AD-Realm

Enter a description

Directory **Realm Configuration** User Download

AD Primary Domain *	<input type="text" value="example.com"/>	ex: domain.com
Directory Username *	<input type="text" value="Administrator@example.com"/>	ex: user@domain
Directory Password *	<input type="password" value="••••••••"/>	
Base DN *	<input type="text" value="CN=users,DC=example,DC=com"/>	ex: ou=user,dc=cisco,dc=com
Group DN *	<input type="text" value="DC=example,DC=com"/>	ex: ou=group,dc=cisco,dc=com
Group Attribute	<input type="text" value="Member"/>	

### User Session Timeout

Authenticated Users	<input type="text" value="1440"/>	minutes
Failed Authentication Users	<input type="text" value="1440"/>	minutes
Guest Users	<input type="text" value="1440"/>	minutes

\* Required Field

ةيساي قولا ليلدلا تادادع امدختسا متي

## AD-Realm

Enter a description

**Directory** Realm Configuration User Download

**URL (Hostname/IP Address and Port)**

172.16.31.103:389

(لوصولك حالي دعاوق يف يفاضل طرشك اهم ادختس ال) AD تاعومجم ضعب دادر تس ا متيو

Overview Analysis Policies Devices Objects | AMP

## AD-Realm

Enter a description

Directory Realm Configuration **User Download**

Download users and groups

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

[Download Now](#)

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

### Admin و pxGrid ل تاداهش

مق لوؤس مل لوصول CSR عاشن ال ةديج ةسرامم اهنا ال ةبولطم ريغ اهنا نم مغرلا يلع امك ةرم ةعقو مل ةداهش ال داريتساب مق ةب قوئوم AD مادختساب CSR يلع عي قوئولاب ةروصل اهذه يف حضوم وه

Overview Analysis Policies Devices Objects | AMP

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

[Generate New CSR](#) [Import HTTPS Certificate](#)

Information

- External Database Access
- Database
- Management Interfaces
- Process
- Remote Storage Device
- Change Reconciliation
- Access Control Preferences
- Access List
- Audit Log
- Dashboard
- DNS Cache
- Email Notification
- Intrusion Policy Preferences
- Language
- Login Banner
- Network Analysis Policy Preferences
- SNMP
- STIG Compliance
- Time
- Time Synchronization
- Shell Timeout
- Vulnerability Mapping
- VMware Tools

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	17000000080385AAF7D2097EAE000000000008					
Signature Algorithm	sha1WithRSAEncryption					

HTTPS Client Certificate Settings

Enable Client Certificates

[Save](#)

### ةب قوئوم نزخم يل قدصل مل ةجرمل ةداهش ةفاضل مزلي

Overview Analysis Policies Devices | **Objects** | AMP

Object Management Intrusion Rules

Name	Value
VeriSign Class 3 Public Primary Certification Authority - G5	CN=VeriSign Class 3 Public Primary Certification Authority - G5, 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, 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 Certification Authority	CN=Wells Fargo Root Certification 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

AMP for Network Status

firepower.example.com - Cannot connect to cloud

ةرادل يف مكحتل ةدحو اهم دختست يتل PXgrid ةداهش عاشن يف ةريال ةوطخل لثمت

أهم ادخاتسإ بـجـي CSR (CLI) رم اوأ رطس ةهـجـاو ءاشنإل ISE pxGrid ةمدخ لـيـوختل (FMC) تاراطإل (وأ OpenSSL ةادأ مدخاتسإب رخآ يـجـراخ زاهـجـيـأ).

```
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:~#
```

مق (pxGrid بلاق) Microsoft CA مدخاتسإب هئاشنإ درجم بـ Fire.csr لـعـيـقـوتـلـابـ مق لـيـلـخـادـلـا تاداهشـلـا نـزـمـيـلـا (fire.pem) ةـعـقـومـلـا ةـداهـشـلـاو (fire.key) صـاخـلـا حـاتـفـمـلـا دـارـيـتـسـاب حـاتـفـمـلـا ءاشنـا ءاداعـا مـتـيـتـلـا رورمـلـا ةـمـلـكـ مـدخـتـسـا صـاخـلـا حـاتـفـمـلـلـ ةـبـسـنـلـابـ FMC. حـاتـفـمـلـا (رمـا openssl genrsa):

The screenshot shows the Cisco ISE GUI with the 'Add Known Internal Certificate' dialog box open. The 'Name' field is set to 'pxgrid'. The 'Certificate Data' field contains a long base64-encoded string. The 'Key' field contains another long base64-encoded string. There are 'Browse...' buttons for both fields. At the bottom, there is a checkbox for 'Encrypted, and the password is:' followed by a password field. 'Save' and 'Cancel' buttons are at the bottom right.

لماكتال > ماظنلا نم ISE لماكت نيوكتب مق ، تاداهشلا عيمج تيبتت درجمب

Overview Analysis Policies Devices Objects AMP

Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite

### 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**  
i ISE connection status:  
Primary host: Success  
OK

مادخ تاداهش ةحص نم ققحتلا نم لك دروتسملا قدصملا عجرملا مدختسا و MNT و PXgrid. pxGrid ل اهؤاشنإ مت ةيلخاد ةداهش مادختسا (MC) ةيرادلإ مكحتلا ةدحول.

## ةيوهلا ةسايس

ةلماخلا ةقداصملا ل اقبسم نوكملا AD قاطن مدختسي يذلا ةيوهلا جهن نيوكت:

Overview Analysis Policies Devices Objects AMP

Access Control > Identity Network Discovery Application Detectors Correlation Actions

### ISEPolicy

Enter a description

Rules Active Authentication + Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Src Ports	Dest Ports	Realm	Action
1	Rule-AD	any	any	any	any	any	any	any	AD-Realm	Passive Authentication

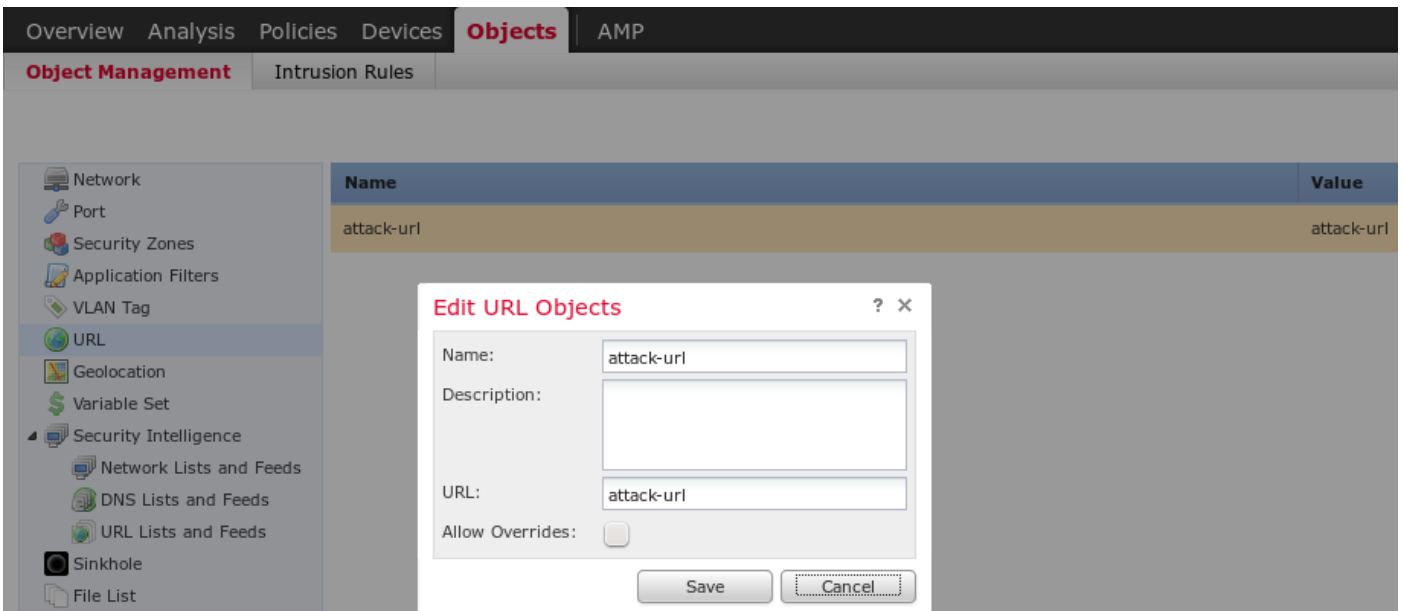
Administrator Rules  
This category is empty

Standard Rules

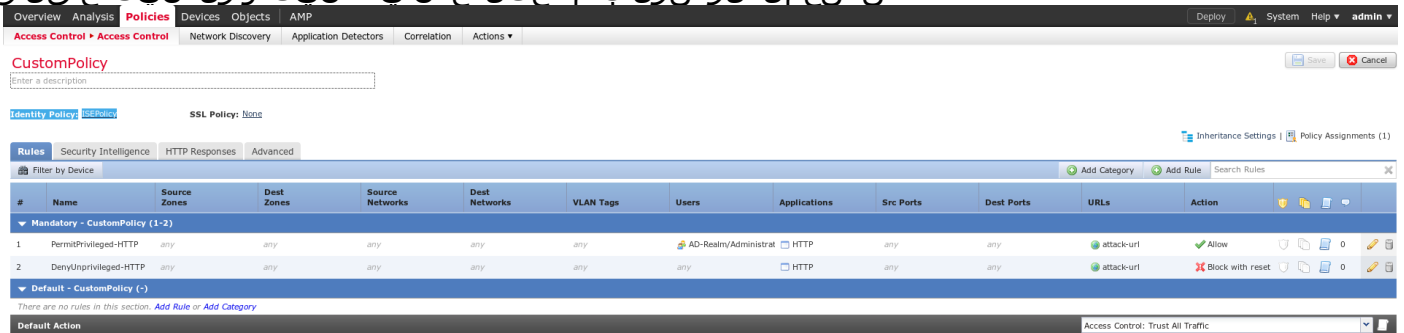
Root Rules  
This category is empty

## لوصول ي ف مكحتلا ةسايس

صصخملا URL ناونع ءاشنإ مت ، لاثملا اذهل:



### صخصم لوصول اب مكحتال جهن في ني تدرالو ني تدعاق لالو:

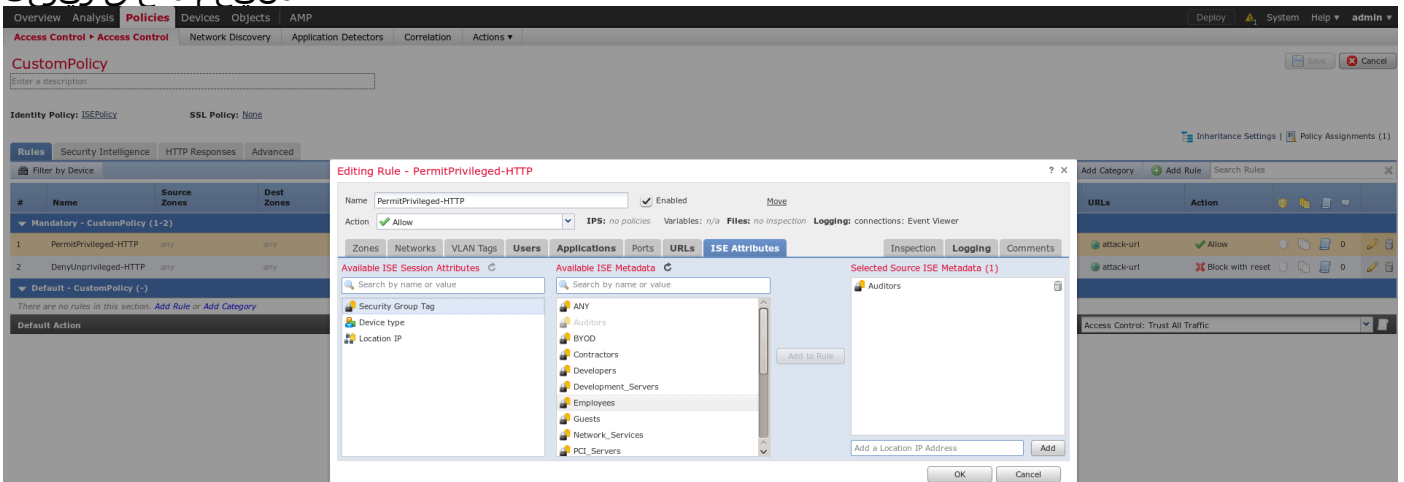


ةومجم لى نومتن ني نى ذل ني مدختسم ل عي مجل PermitPrivileged-HTTP ةدعاق حمست ةفاك لى HTTP موجه ذيفنتل نوقق دم ل. مهل SGT ةمالع ني يعت مت ني ذل AD لى وووسم فادهال.

نرخ آل ني مدختسم ل ةفاكل عارج ال اذ DenyUnprivileged-HTTP ضفر.

لوصول اب مكحتال جهن ل اقبسم هؤاشن ل مت ي ذل ةي وهال جهن ني يعت مت دق هن اضى اظحال اذ.

وا عاشن ل انثا ةي ئرم انكلو، بيقرل تامالع ةيؤر نكمم ل ريغ نم، هذ بيوبت ل ةمالع يف ةنعم ةدعاق ريرحت:



تاريغ التا عي مج رشن مت و NGIPS لى ةسايس ل ني يعت نم دكأت:

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

## ةحصلال نم ققحتال

ةسلج ةمدخ ي ف pxGrid ليمع كارتشا ISE يري نأ بجي ،ححيحص لكشرب ءيش لك نيوكت دعب (تنرتنإل ربع ةلحال) لمعال.

Identity Services Engine Home ▶ Operations ▶ Policy ▶ Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Clients Live Log

Enable 
  Disable 
  Approve 
  Group 
  Decline 
  Delete 
 Refresh 
 Total Pending Approval(0)

Client Name	Client Description	Capabilities	Status	Client Group(s)
ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator
ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator
iseagent-firepower.example.co...		Capabilities(0 Pub, 3 Sub)	Online	Session
firesightisetest-firepower.exempl...		Capabilities(0 Pub, 0 Sub)	Offline	Session

تامالع) TrustSecMetaData ةمدخ ي ف كرتشا دق FMC نأ ديكأت اضيأ ك نكمي تالجال نم كارتشال ءاغأل متوزييمتال تامالع ءيمج يلع تلصح - SGT).

Identity Services Engine Home ▶ Operations ▶ Policy ▶ Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Ide

Clients Live Log iseagent-firepower.example.com-0739edea820cc77e04cc7c44200f661e

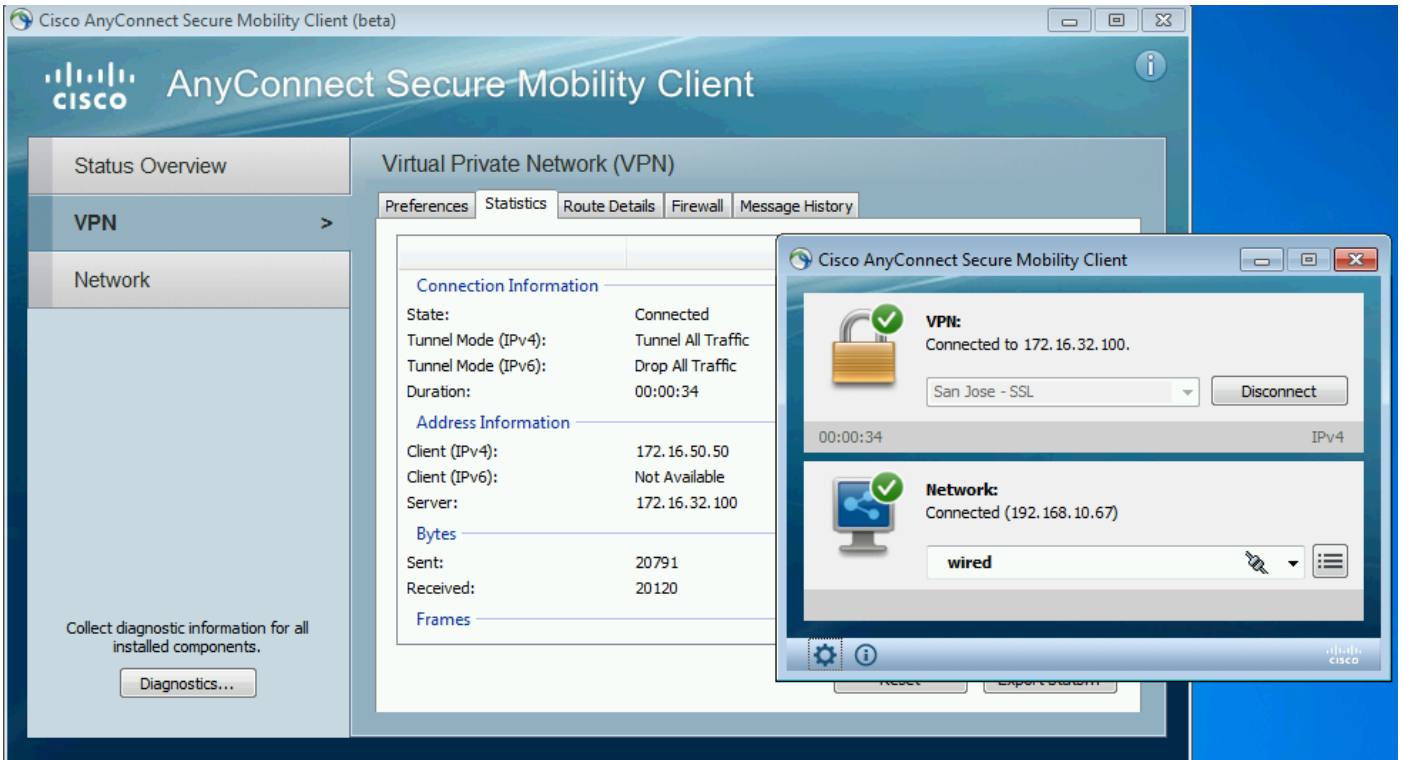
Clear Logs 
  Resync 
 Refresh

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

## VPN ةسلج ءاشنإ

SGT ةمالع ءاچارب ISE يلع ضيوفتال موقوي ال امدنع وييرانيسل لوالأ رابتخال ءارجإ متي (قويقتال تارابتخاب NGIPS تاقاطب حمست ال) ءححيحصال.

ليصفات ريثك تدوز عي طتسي (UI) نراق لمعتسم AnyConnect up ةس لج VPN نإ ام



ةس لجل سيسي سأت دي كأت ASA ل نكمي

```
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 نيوكت متي مل .ةقداصملا هذهل هعاجرا مت بيقر مقر ي اري ال ASA نأ ةظحالم يجرى ل.اح ي اىل ع تامولعمل ي طخت متي تح - TrustSec

متي مل - (23:36:19 ةعاسلا مامت ي ف لچسلا) حج انلا ضيوفتلا نغ غالب اب اضي ا ISE موقى بيقر ةمالع ةي اعاجرا:

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

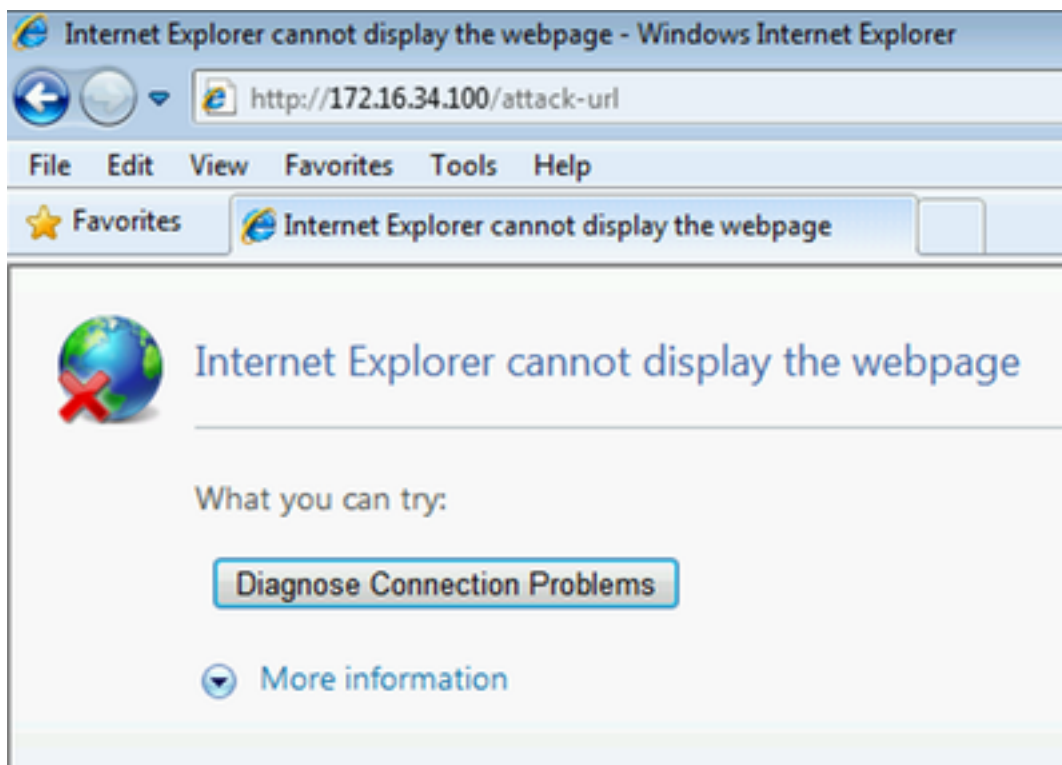
## MnT نم ةسلجلا تانايب لىل لصحي FMC

مت) ةديج لمع ةسلج نغ اري رقت /var/log/messages ي ف FMC لسري ،ةلحرملا كلت ي ف يساسا ل ا ج ذوم نلل ل AD تحبو لوؤسملا مدختسم مسال (pxGrid ةمدخل كرتشمك اه يقلت ةوعومجملا ةيوضع:

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

## تازايتما وا تازايتما ي نود ةكبشلا لىل لوصول

مت ي ذل ا مدخال لىل لوصول او بي و ضرعتسم حتف ةلحرملا هذه ي ف مدختسملا لواحي امدنع ل:اصتالا اءان متيس ،هقيقت



اقف و TCP RST لاسرا) ليمعلا نم اهذخأ مت يتلا طاقن طاقن اة طساوب اهديكأت نكمي  
 نيوكتل FMC):

Cisco AnyConnect VPN Virtual Miniport Adapter for Windows x64: \\Device\NPF\_{BF9293D2-3A19-48B9-86B6-5CFC21A64AA6} [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 W=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 W=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 W=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]

ريراقت ةسلج ASA ةقاطب قيقدتلا، عجري نأ نوكي ISE تلكش نإم

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

عاجرا متي - (23:37:26 ةعاسلا مامت يف لجسلا) ضيوفتلا حاجن نع مالعإ اب اضيأ ISE موقى

## SGT: عمال ال ق ق دم

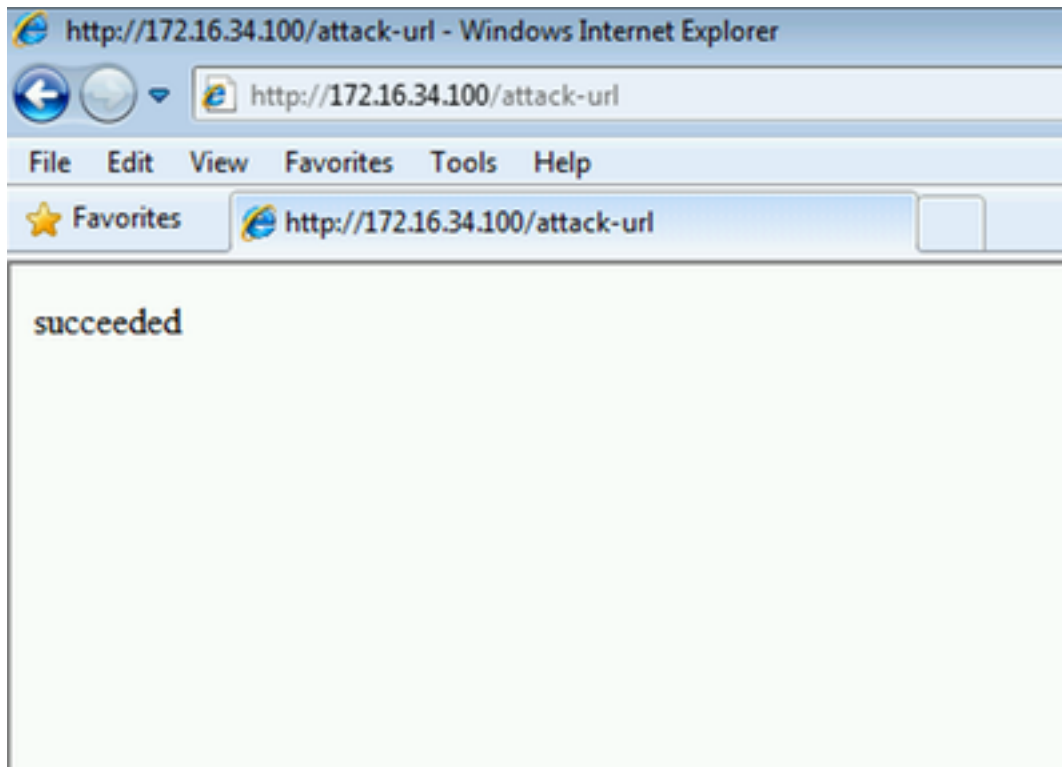
The screenshot shows the Cisco ISE dashboard with the following metrics:

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

Below the metrics is a table of live sessions:

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

## ة روك ذملا ة مدخل ال ال لوصول م دخت س مل ل ن ك مي و



## ل ف M C ل ج س ت ال ل لوصول

## ل: اصت ال ا ث د ح ر ي ر ق ت ة ط س ا و ب ط ا ش ن ل ا ذ ه د ي ك أ ت ن ك م ي

The screenshot shows the Cisco FMC 'Connection Events' table. The table lists connection events with the following columns:

Time	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	DenyUnprivileged-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	Auditors	eth1		25	3,928	5

الوا م ادخت س ا م ت ي ، ( F M C ة د ع ا ق ة ط س ا و ب ا ه ت د ا ع ا ت س ا و ) I S E ة ط س ا و ب ق ق د م ل ا ة م ا ل ع ن ي ي ع ت د ر ج م ب ل . و ل و ص ل ا ب ح ا م س ل ا م ت ي و P e r m i t P r i v i l e g e d - H T T P

ةدعاق ضرع متي ام ةداع هنأل ةددعتم ةدمعأ ةلازا تمت، ضرعلا لىلع لوصحلل هنأ اضيأ طحال  
ريرمتلا طيرش مادختسا بجي و) ةريخأل ةدمعأل دحأك نامأل ةومجم ةمالعو لوصولاب مكحتلا  
لبقتسمل ي اهمادختسا ةداعإ و هذه ةصصخملا ضرعلا ةقيرط ظفح نكمي. (يقفألا

## اهحالصإ وءاطخأل فاشكتسا

### FMC ءاطخأ حيحصت

/var/log/messages file: ةيوهلا تامدخ نم ققحتلا نع لوؤسمل ADI نوكم تالچس نم ققحتلل

```
[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 .....
```

دع رذجال نم) ةيمويلا ةيلمعلا لتق نكمملا نم ،اليصفت رثكأ حيحصت يلعل لوصحلل  
ءاطخالأ حيحصت ةطيسو ماخذتساب اهليغشتو (ودسلل

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

## مراجعة SGT PXgrid

معلومات شديحة دنع وإ ISE لمات مسق يف رابتخال رز قوف رقنل دنع ةي لمعلا ذي فنت متي لوصولاب مكحتل اجهن يف ةدعاق ةفاضل اناثأ، بيقرللا

```
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>fe2d22f0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Production_Servers</ns5:name><ns5:description>Production Servers Security
Group</ns5:description><ns5:tag>11</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe487320-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Production_Users</ns5:name><ns5:description>Production User Security
Group</ns5:description><ns5:tag>7</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe62d8f0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Quarantined_Systems</ns5:name><ns5:description>Quarantine Security
Group</ns5:description><ns5:tag>255</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe7d3ec0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Test_Servers</ns5:name><ns5:description>Test Servers Security
Group</ns5:description><ns5:tag>13</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe99c770-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>TrustSec_Devices</ns5:name><ns5:description>TrustSec Devices Security
Group</ns5:description><ns5:tag>2</ns5:tag></ns5:SecurityGroup></ns5:SecurityGroups></ns5:getSecurityGroupListResponse>]
```

نم هحتف و xml فلم ىل هخسن نكم ىل جسلا ك لذ نم xml ىوت حمل لصف اضرع ىل لوصحلل همالتسا مت دق (ققدملا) ددحمل بىقرلا نا نم دكأت نا عىطتست كن ا بىو حفتصتم لالخ (ISE) جمدملا بىقرلاب فرعمل رخال بىقرلا لك هاقلت ىذلا ردقلا س فنب

```
-<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>
```

## MnT إلى REST API ربع لمعالج ةس لجالع ساء

(pxGrid ربع MnT ذفنم و ففضم مسا ريرمت ةظحالما عاجرلا) رابخالال ةفلمع نم عئاضف اذهو  
ةةمجالع لعال ةس لجالع لزنن ماذخسائ مئ:

```
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>UGVybw10QWNjZXRzLEF1ZG10b3Jz</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</ADUserDNSDomain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfile>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>UGVybw10QWNjZXNzLEF1ZG10b3Jz</attribute></extraAttributes><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:E6: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</ADUserDNSDomain><ADUserNetBIOSName>EXAMPLE</ADUserNetBIOSName></user><assessedPostureEvent/><endpointProfile>Windows7-Workstation</endpointProfile><securityGroup>Auditors</securityGroup></session>
```

(دحاو ةطشن لم ةس ل ج مالتسا مت) اهل لي لحت مت يتي ل ةجيت نل او

```
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}
```

Realm-AD: مدختسم مساب (ل ا ج م ل او) مدختسم ل مساب طبر NGIPS ل و احي، ةل ح ر م ل كلت ي ف

```
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
```

ة و م ج م ل او مدختسم ل ة ي و ض ع ي ل ع ر و ث ع ل ل LDAP مادختسا مت ي

```
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 اءاطخ احي حصت

لك نم ققحت ل نك م م ل نم، pxGrid تانوك م ل ع بتت ل يوتسم اءاطخ احي حصت ني ك مت دعب  
FMC) لثم تاناي ب/ ةلومح نودب نكلو) ةي ل م ع

ب: بي قرة م ال ع ة داعتسا عم ل اثم

```
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
```

## تارشح

[CSCuv32295](#) - مدختسمل مسال لوقح ي ف لاجمل تامول عم ISE لسري نأ زوجي -

[CSCus53796](#) - عمجم ال REST مالع تسال فيضمل اب صاخ ال FQDN لى لوصح ال رذعتي -

[CSCuv43145](#) - قوثل نزم فذح/داري تسال، ةي وهال طي طخت و PXGRID ةمدخ لي غشت ةداع | -

## عجارم ال

- [FirePOWER و ISE لمالك ت مادختساب حالصل ال تامدخ ني وكت](#)
- [قعووم ال ISE ةئيب ي ف pxGrid ني وكت](#)
- [CA نم ةعقووم ال PXgrid ISE ةدوع ني وكت: Cisco PXgrid مادختساب تاداهش ال رشن ةي فيك  
CA-Signed PXgrid لي معو](#)
- [IPS PXlog قي بطت عم PXgrid 1.3 رادصل ال ISE لمالك](#)
- [2.0 رادصل، Cisco، نم ةي وهال تامدخ كرحم لوؤسم لي لد](#)
- [1.2 - رادصل ال، Cisco، نم ةي وهال تامدخ كرحم ال \(API\) تاق ي بطت ال ةجمر ب ةه او عجرم لي لد  
...ي جراخ ال RESTful S لى ةمدقم](#)
- [رادصل ال، Cisco، نم ةي وهال تامدخ كرحم ال \(API\) تاق ي بطت ال ةجمر ب ةه او عجرم ال لي لد  
Monitoring RES... لى ةمدقم - 1.2](#)
- [1.3 رادصل ال، Cisco، نم ةي وهال تامدخ كرحم لوؤسم لي لد](#)
- [زمتس يس وكس يس - قي ثوت & معد](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت م م م دقت ل ة يرش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا