

Fehlerbehebung bei ISE- und FirePOWER-Integration für Identity Services

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[ISE](#)

[Active Directory](#)

[Netzwerkzugriffsgerät](#)

[Zertifikate für pxGrid und MnT](#)

[pxGrid-Service](#)

[Autorisierungsrichtlinie](#)

[FMC](#)

[Active Directory-Bereich](#)

[Zertifikate für Admin und pxGrid](#)

[ISE-Integration](#)

[Identitätsrichtlinie](#)

[Zugriffskontrollrichtlinie](#)

[Überprüfen](#)

[Einrichtung von VPN-Sitzungen](#)

[FMC empfängt Sitzungsdaten von MnT](#)

[Unprivilegierter und privilegierter Netzwerkzugriff](#)

[Zugriff auf FMC-Protokollierung](#)

[Fehlerbehebung](#)

[FMC-Debugger](#)

[SGT-Abfrage über pxGrid](#)

[Sitzungsabfrage über REST-API zu MnT](#)

[ISE-Debugging](#)

[Bug](#)

[Referenzen](#)

Einführung

Dieses Dokument beschreibt die Konfiguration und Fehlerbehebung von TrustSec-Richtlinien auf dem Cisco Next Generation Intrusion Prevention System (NGIPS) (NGIPS). NGIPS 6.0 unterstützt die Integration mit Identity Services Engine (ISE), sodass identitätsbasierte Richtlinien erstellt werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- VPN-Konfiguration der Cisco Adaptive Security Appliance (ASA)
- Konfiguration des Cisco AnyConnect Secure Mobility Client
- Grundkonfiguration des Cisco FirePower Management Center
- Cisco ISE-Konfiguration
- Cisco TrustSec-Lösungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Microsoft Windows 2012 Certificate Authority (CA)
- Cisco ASA Version 9.3
- Cisco ISE Software Version 1.4
- Cisco AnyConnect Secure Mobility Client Version 4.2
- Cisco FirePower Management Center (FMC) Version 6.0
- Cisco FirePOWER NGIPS 6.0

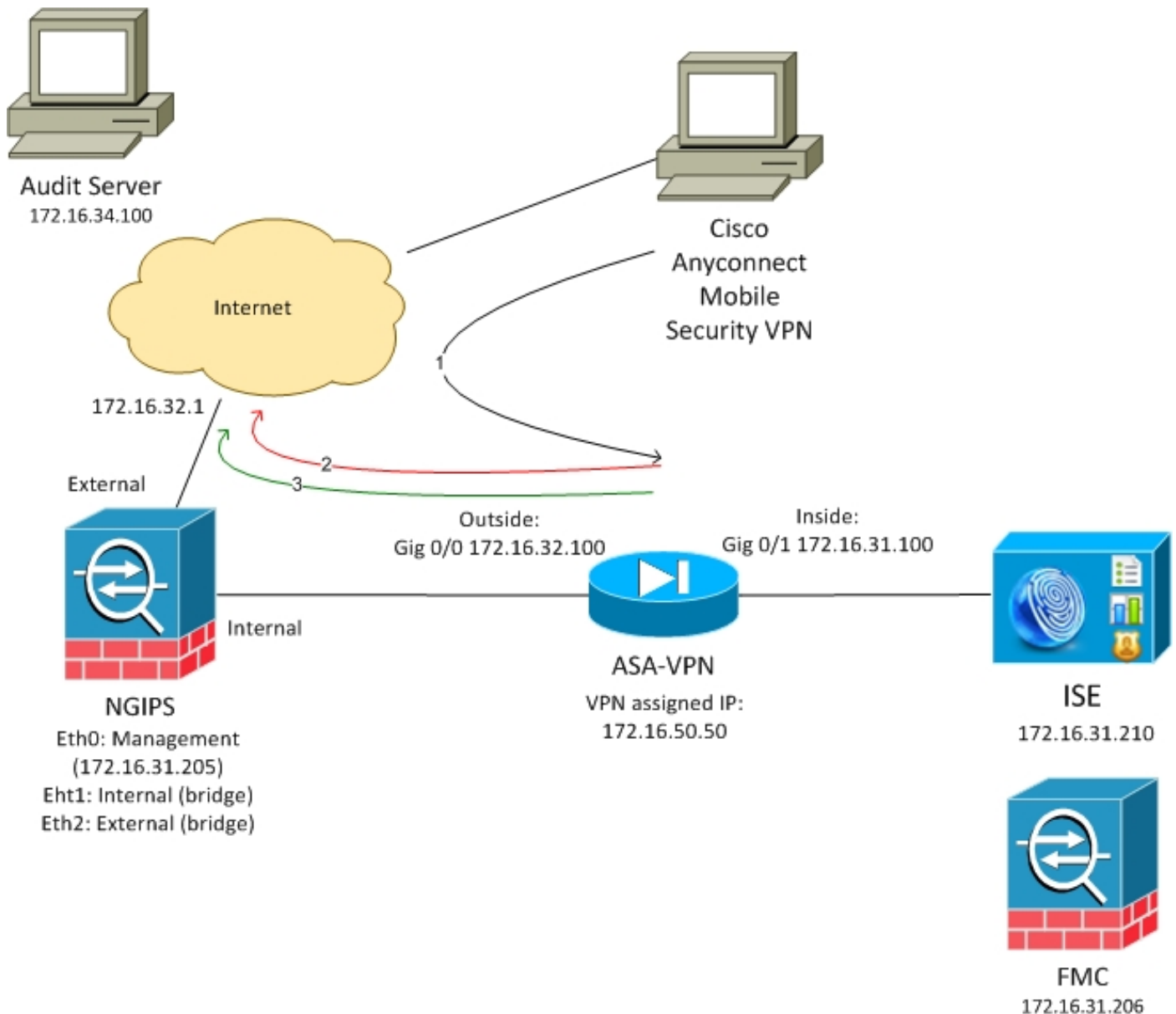
Konfigurieren

FirePower Management Center (FMC) ist die Managementplattform für FirePower. Es gibt zwei Arten von Funktionen für die ISE-Integration:

- **Problembehebung** - Ermöglicht FMC die Quarantäne des Angreifers über die ISE, die den Autorisierungsstatus auf dem Zugriffsgerät dynamisch ändert und einen begrenzten Netzwerkzugriff ermöglicht. Es gibt zwei Generationen dieser Lösung:
 1. Legacy-Perl-Skript mit EPS-API-Aufruf (Endpoint Protection Service) für ISE.
 2. Neueres Modul, das pxGrid-Protokoll-Aufruf für ISE (dieses Modul wird nur in Version 5.4 unterstützt - nicht in 6.0, native Unterstützung in 6.1 geplant).
- **Richtlinie** - Ermöglicht der FMC die Konfiguration von Richtlinien auf der Grundlage von TrustSec Security Group Tags (SGT).

Dieser Artikel konzentriert sich auf die zweite Funktionalität. Ein Beispiel zur Problembehebung finden Sie im Abschnitt zu Referenzen.

Netzwerkdiagramm



Das FMC wird mit einer Zugriffskontrollrichtlinie konfiguriert, die zwei Regeln enthält:

- Für HTTP-Datenverkehr mit benutzerdefinierter URL verweigern (Attack-URL)
- Zulassen von HTTP-Datenverkehr mit benutzerdefinierter URL (attack-url), jedoch nur, wenn der Benutzer dem Audit (9) SGT-Tag von der ISE zugewiesen wird

Die ISE beschließt, allen Active Directory-Benutzern, die der Administratorgruppe angehören, Audit-Tag zuzuweisen und verwendet das ASA-VPN-Gerät für den Netzwerkzugriff.

Der Benutzer greift über eine VPN-Verbindung auf das Netzwerk auf der ASA zu. Der Benutzer versucht dann, mithilfe von URL attack-url auf den überwachten Server zuzugreifen, schlägt aber fehl, weil er nicht der Audit SGT-Gruppe zugewiesen wurde. Sobald diese behoben ist, ist die Verbindung erfolgreich.

ISE

Active Directory

Die AD-Integration muss konfiguriert und die richtigen Gruppen abgerufen werden (für die Autorisierungsregel wird die Administratorgruppe verwendet):

The screenshot shows the Cisco Identity Services Engine Administration console. The navigation menu includes Home, Operations, Policy, Guest Access, Administration, and Work Centers. Under Administration, the 'Groups' tab is selected. The left sidebar shows 'External Identity Sources' with a tree view containing Certificate Authentication Profile, Active Directory (example.com), LDAP, RADIUS Token, RSA SecurID, and SAML Id Providers. The main content area shows a table of groups under the 'Groups' tab.

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

Netzwerkzugriffsgert

ASA wird als Netzwerkgerat hinzugefugt. Die benutzerdefinierte Gruppe ASA-VPN-Audit wird verwendet, wie in diesem Bild gezeigt:

The screenshot shows the Cisco Identity Services Engine Administration console for configuring a Network Device. The 'Network Devices' tab is selected. The configuration form includes the following fields:

- Name: ASA
- Description: (empty)
- IP Address: 172.16.31.100 / 32
- Device Profile: Cisco
- Model Name: (dropdown)
- Software Version: (dropdown)
- Network Device Group:
 - Location: All Locations (dropdown) [Set To Default]
 - Device Type: ASA-VPN-Audit (dropdown) [Set To Default]
- RADIUS Authentication Settings:
 - Enable Authentication Settings: (checked)
 - Protocol: RADIUS
 - Shared Secret: (masked) [Show]

Zertifikate für pxGrid und MnT

FMC nutzt beide Services auf der ISE:

- pxGrid für SGT und Profiling-Datenabfrage
- Überwachung und Reporting (MnT) für den Download von Massensitzungen

Die MnT-Verfügbarkeit ist sehr wichtig, da FMC auf diese Weise über die IP-Adresse der authentifizierten Sitzung informiert wird, auch über den Benutzernamen und das SGT-Tag. Auf dieser Grundlage können die richtigen Richtlinien angewendet werden. Bitte beachten Sie, dass

NGIPS keine nativen SGT-Tags (Inline-Tagging) wie die ASA unterstützt. Im Gegensatz zur ASA unterstützt sie jedoch nur SGT-Namen statt Zahlen.

Aufgrund dieser Anforderungen müssen sowohl ISE als auch FMC einander vertrauen (Zertifikat). MnT verwendet nur serverseitiges Zertifikat, pxGrid verwendet sowohl das clientseitige als auch das serverseitige Zertifikat.

Microsoft CA wird zum Signieren aller Zertifikate verwendet.

Für MnT (Admin-Rolle) muss die ISE, wie in diesem Bild gezeigt, eine Zertifikatssignierungsanfrage (CSR) generieren:

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"/> lise20	lise20#Admin

Subject

Common Name (CN) [?](#)

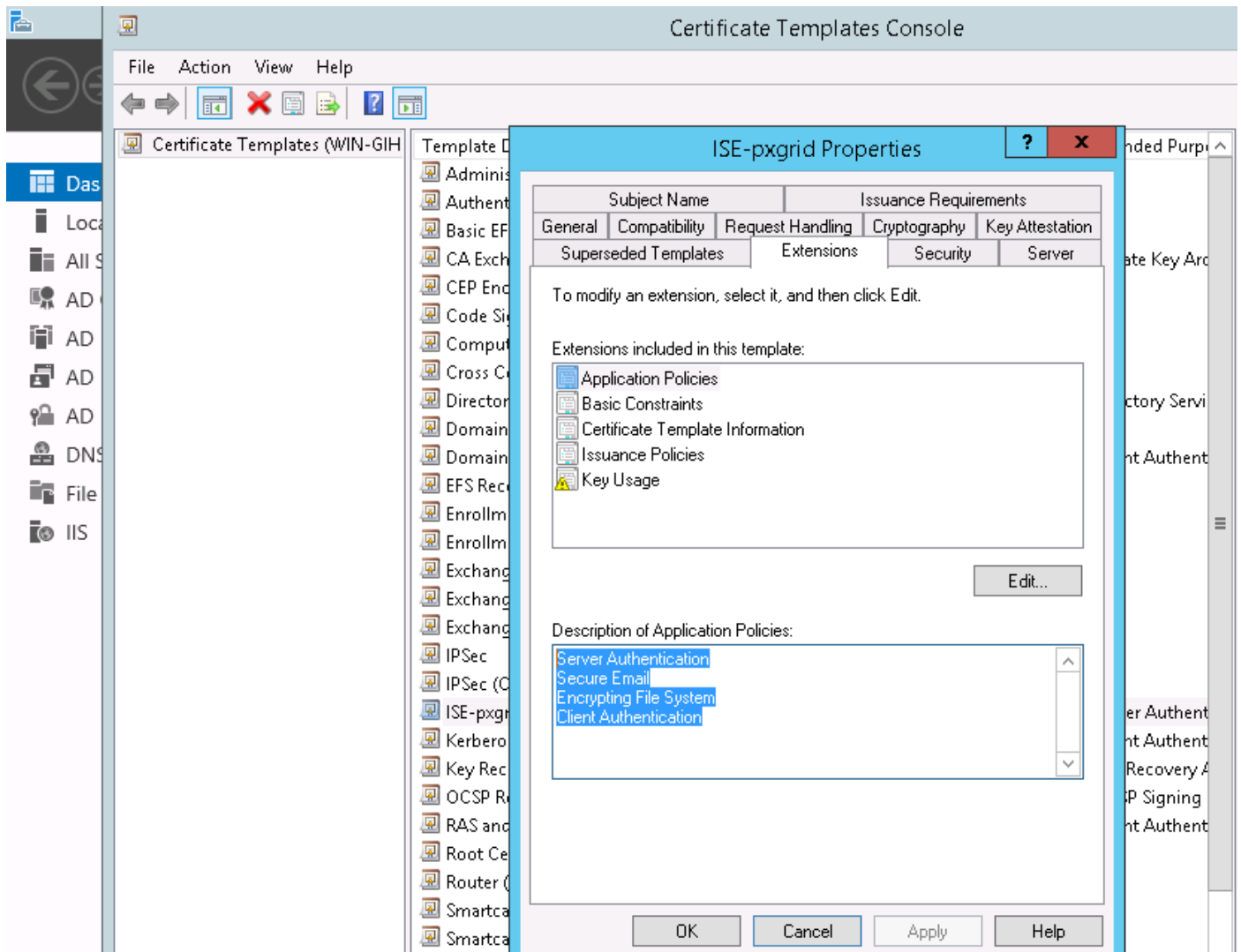
Nach der Signierung durch Microsoft CA muss der Import über die Option **Bind Certificate** erfolgen.

Ein ähnlicher Prozess muss für den pxGrid-Dienst befolgt werden. **Für die Option werden Zertifikate verwendet**, muss pxGrid ausgewählt sein.

Da es nicht zwei Zertifikate mit identischem Betreffnamen geben kann, kann für den OU- oder O-Abschnitt (z. B. pxGrid) ein anderer Wert hinzugefügt werden.

Hinweis: Stellen Sie sicher, dass für jeden vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) für ISE und FMC der richtige DNS-Datensatz auf dem DNS-Server konfiguriert wird.

Der einzige Unterschied zwischen dem Admin- und dem pxGrid-Zertifikat besteht im Signierungsprozess. Da pxGrid-Zertifikate über Extended Key Usage-Optionen für die benutzerdefinierte Client- und Serverauthentifizierung in Microsoft CA verfügen müssen, können folgende Aufgaben durchgeführt werden:



In diesem Bild wird gezeigt, wie der Microsoft-Webdienst zum Signieren von pxGrid CSR verwendet wird:

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:

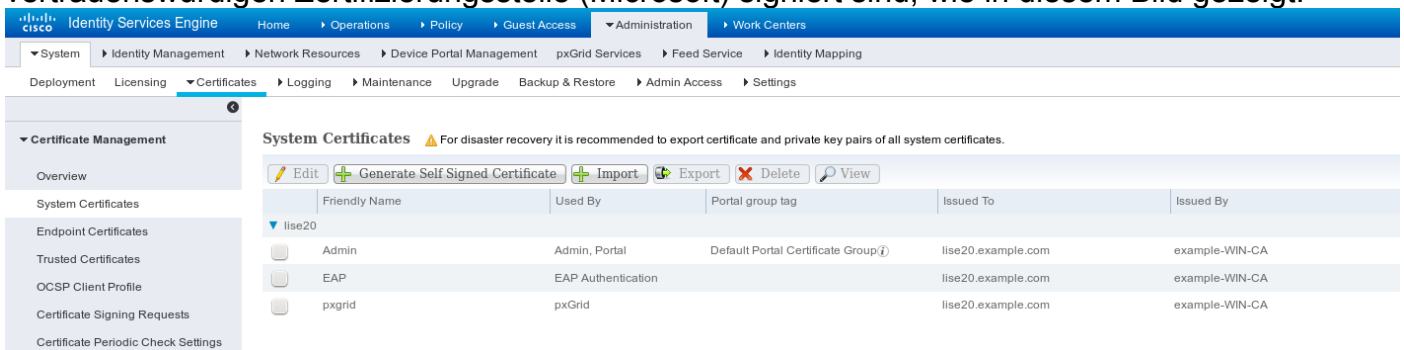
ISE-pxgrid

Additional Attributes:

Attributes:

Submit >

Am Ende muss die ISE über Admin- und pxGrid-Zertifikate verfügen, die von der vertrauenswürdigen Zertifizierungsstelle (Microsoft) signiert sind, wie in diesem Bild gezeigt:



pxGrid-Service

Mit den richtigen Zertifikaten muss die pxGrid-Rolle für einen bestimmten Knoten aktiviert werden, wie in diesem Bild gezeigt:

Deployment

Deployment

PAN Failover

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 ⓘ
 Include Node in Node Group None ⓘ

Enable Profiling Service

Enable SXP Service Use Interface GigabitEthernet 0 ⓘ

Enable Device Admin Service ⓘ

Enable Identity Mapping ⓘ

pxGrid ⓘ

Die automatische Genehmigung muss aktiviert sein:

[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	View
ise-mnt-lise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
iseagent-frepower.example.co...		Capabilities(0 Pub, 3 Sub)	Online	Session	View
fresightsest-frepower.examp...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

Autorisierungsrichtlinie

Die Standardauthentifizierungsrichtlinie wird verwendet (AD-Suche wird durchgeführt, wenn kein lokaler Benutzer gefunden wird).

Die Autorisierungsrichtlinie wurde so konfiguriert, dass sie vollständigen Netzwerkzugriff bereitstellt (Berechtigung: PermitAccess) für Benutzer, die sich über ASA-VPN authentifizieren und zu Active Directory-Gruppenadministratoren gehören - für diese Benutzer werden SGT-Tag-Auditoren zurückgegeben:

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-Bereich

Für die ISE-Integration ist eine Bereichskonfiguration erforderlich (um Identitätsrichtlinien zu verwenden und die Gruppenmitgliedschaft für passiv authentifizierte Benutzer abzurufen). Der Bereich kann für Active Directory oder Lightweight Directory Access Protocol (LDAP) konfiguriert werden. In diesem Beispiel wird AD verwendet. Von **System > Integration > Bereich**:

AD-Realm

Enter a description

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

Es werden folgende Standardverzeichniseinstellungen verwendet:

AD-Realm

Enter a description

URL (Hostname/IP Address and Port)

172.16.31.103:389

Der letzte Schritt besteht in der Generierung des pxGrid-Zertifikats, das vom FMC zur Autorisierung für den ISE pxGrid-Service verwendet wird. Zur Generierung von CSR CLI muss verwendet werden (oder ein anderes externes System mit openssl-Tool).

```
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:~#
```

Nachdem fire.csr erstellt wurde, signieren Sie es mit Microsoft CA (pxGrid-Vorlage). Importieren Sie privaten Schlüssel (fire.key) und signiertes Zertifikat (fire.pem) in den internen Zertifikatsspeicher von FMC. Verwenden Sie für private Schlüssel das Kennwort, das während der Generierung des Schlüssels eingerichtet wurde (**openssl genrsa** Befehl):

The screenshot shows the Cisco FMC GUI with the 'Objects' tab selected. A table lists the 'pxgrid' object with the value 'CN=firepower.example.com, ORG=TAC, OU=pxgrid, C=PL'. A dialog box titled 'Add Known Internal Certificate' is open, showing the following fields:

- Name: pxgrid
- Certificate Data or, choose a file: [Browse...]
- Key or, choose a file: [Browse...]
- Encrypted, and the password is: [Password field]

The Certificate Data field contains the following base64-encoded string:

```
AwiCAgCAMA4GCCqGSIb3DQMEAgIAGDAHBgUrdgMCBzAKBggqkiG9w0DBzANBgkqhkiG9w0BAQUFAAOCAQEASObDPO4nTYpH5Cbwz1nusKooPIUeYIHAJZU77TrgWb1WWXeaJET3TrUj3ao9mu+9jn4yoLC/+qygMl8U2lzb2bhLaxu336oXGLy/A8S39gnhNZRPXr1f1dSYokTzWW22yuDvyoTGVWnPxF3VGeKfgCZXx9I4SbNPeWrChx0ku7I PZmDeI5KNVldWgy4LgojIEjIjNgnd5XVHkZdsgT1eV697dQLHRp+I5BulYXuT8A1m694XbOG4a2GYV9Jlglfm1cTa7ed6yB4oFc9bM8Nb60pxc5H7rTjDyuBQxnhOCrYvdUjPdJEH+dYwWp3IXoHMv4mR6br9z6g==-----END CERTIFICATE-----
```

The Key field contains the following base64-encoded string:

```
IHX8NiiQM+NBuAtcEiUvB78tkNUPy5UT5KSBQ4i6E97z53haL4ISyqJyYtIRQaG5OqjWIMD085sUvCayzQh40QhpZf/cEggEAAUZ7CpeuUSdLDSkmlkTabgykNtGthrT2p8/B++qF0F0mC+Gsq7PkaR1WLH/HFcFUMwP41Xd2WkiITNamVjopMZ800n/8oo/MNe46OKr1ZuToUW9ID01JjvzwTcTnlyZ5DSoXFmlwX2Tu6mSXWq6yCL7/EpUdGhkJTdyU0fsJHT5W3dmnFkWerBS5Cw+eWqCOqacObx0IB5OpwDzw5PQ/Gom+WZNF+2LWlvM2dh2dATdywrad0ZjG7RpdV5uYfPkSZOWLigJH1m+3FpILIMIT5VwssCFK0O4DVJhidH6jRqA3VfgvWLpsTUvWknMF8drv8lx4SF1dU4qoA==-----END RSA PRIVATE KEY-----
```

ISE-Integration

Nachdem alle Zertifikate installiert wurden, konfigurieren Sie die ISE-Integration von **System > Integration**:

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 *

Secondary Host Name/IP Address

pxGrid Server CA * +

MNT Server CA * +

MC Server Certificate * +

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

* Required Field

Status
 ISE connection status:
Primary host: Success

Verwenden Sie die importierte CA für die Validierung von pxGrid- und Mnt-Dienstzertifikaten. Für die Management Console (MC) wird das interne Zertifikat verwendet, das für pxGrid generiert wurde.

Identitätsrichtlinie

Konfigurieren Sie die Identitätsrichtlinie, die den zuvor konfigurierten AD-Bereich für die passive Authentifizierung verwendet:

Overview Analysis **Policies** Devices Objects AMP

Access Control > Identity Network Discovery Application Detectors Correlation Actions

ISEPolicy

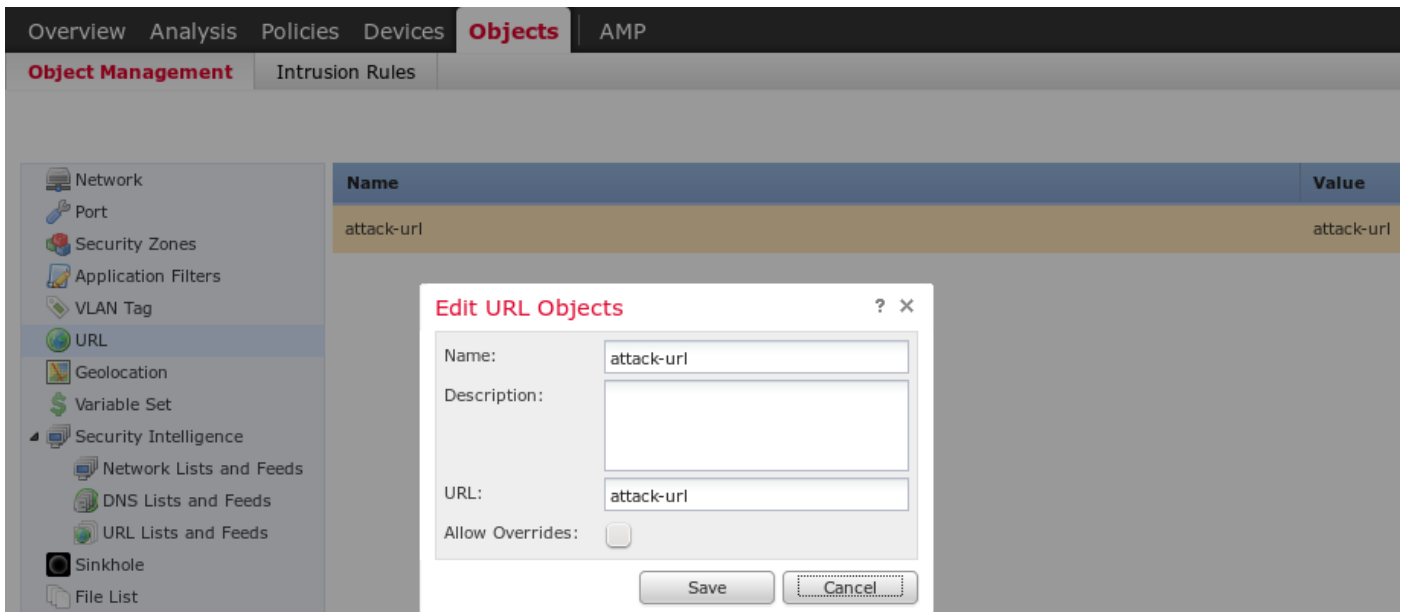
Enter a description

Rules Active Authentication

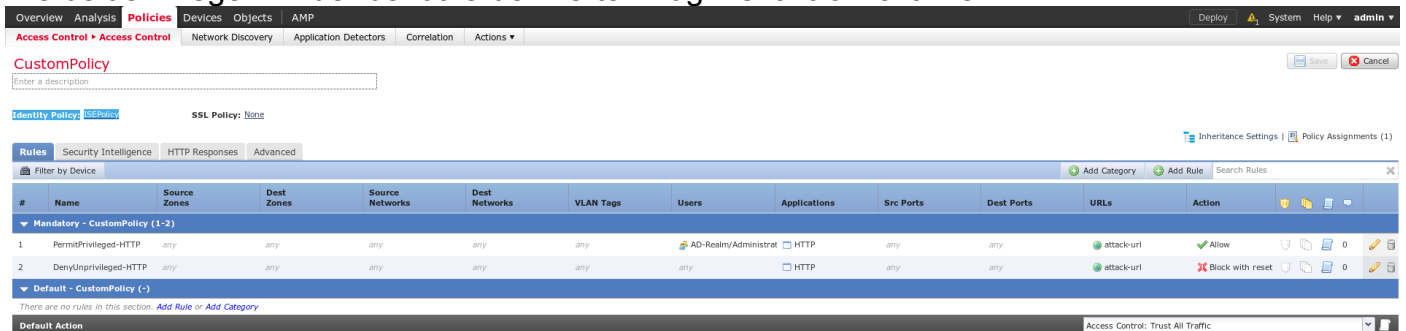
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Src Ports	Dest Ports	Realm	Action
Administrator Rules										
This category is empty										
Standard Rules										
1	Rule-AD	any	any	any	any	any	any	any	AD-Realm	Passive Authentication
Root Rules										
This category is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

Zugriffskontrollrichtlinie

Für dieses Beispiel wurde die benutzerdefinierte URL erstellt:



Die beiden Regeln in der benutzerdefinierten Zugriffskontrollrichtlinie:

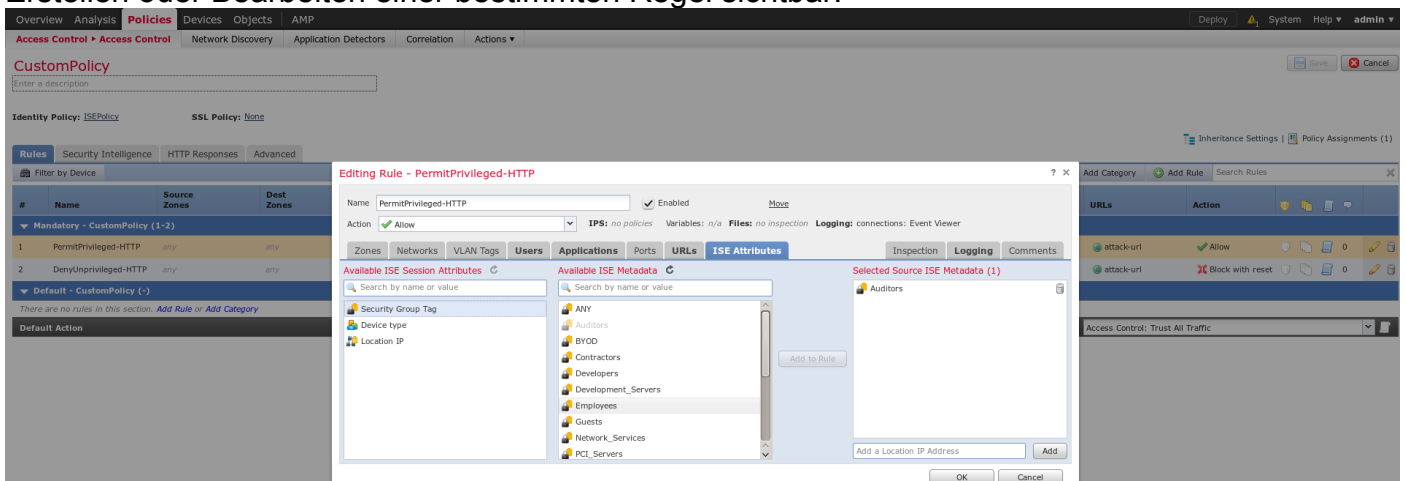


PermitPrivileged-HTTP-Regel ermöglicht allen Benutzern der Gruppe AD-Administratoren, denen das SGT-Tag zugewiesen wurde. Auditoren führen HTTP-Angriffe auf alle Ziele aus.

DenyUnprivileged-HTTP verweigert diese Aktion allen anderen Benutzern.

Beachten Sie außerdem, dass zuvor erstellte Identitätsrichtlinien dieser Zugriffskontrollrichtlinie zugewiesen wurden.

Auf dieser Registerkarte können keine SGT-Tags angezeigt werden, diese sind jedoch beim Erstellen oder Bearbeiten einer bestimmten Regel sichtbar:



Stellen Sie sicher, dass die Richtlinie dem NGIPS zugewiesen und alle Änderungen bereitgestellt werden:

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

Überprüfen

Nachdem alles korrekt konfiguriert wurde, sollte die ISE pxGrid-Client-Abonnement für einen Session-Service (Status Online) sehen.

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

Aus den Protokollen können Sie auch bestätigen, dass FMC den TrustSecMetaData-Dienst (SGT-Tags) abonniert hat - alle Tags erhalten und abbestellt hat.

Identity Services Engine Home ▶ Operations ▶ Policy ▶ Guest Access Administration ▶ Work Cent
 ▶ System ▶ Identity Management ▶ Network Resources ▶ Device Portal Management pxGrid Services ▶ Feed Service ▶ Ide

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

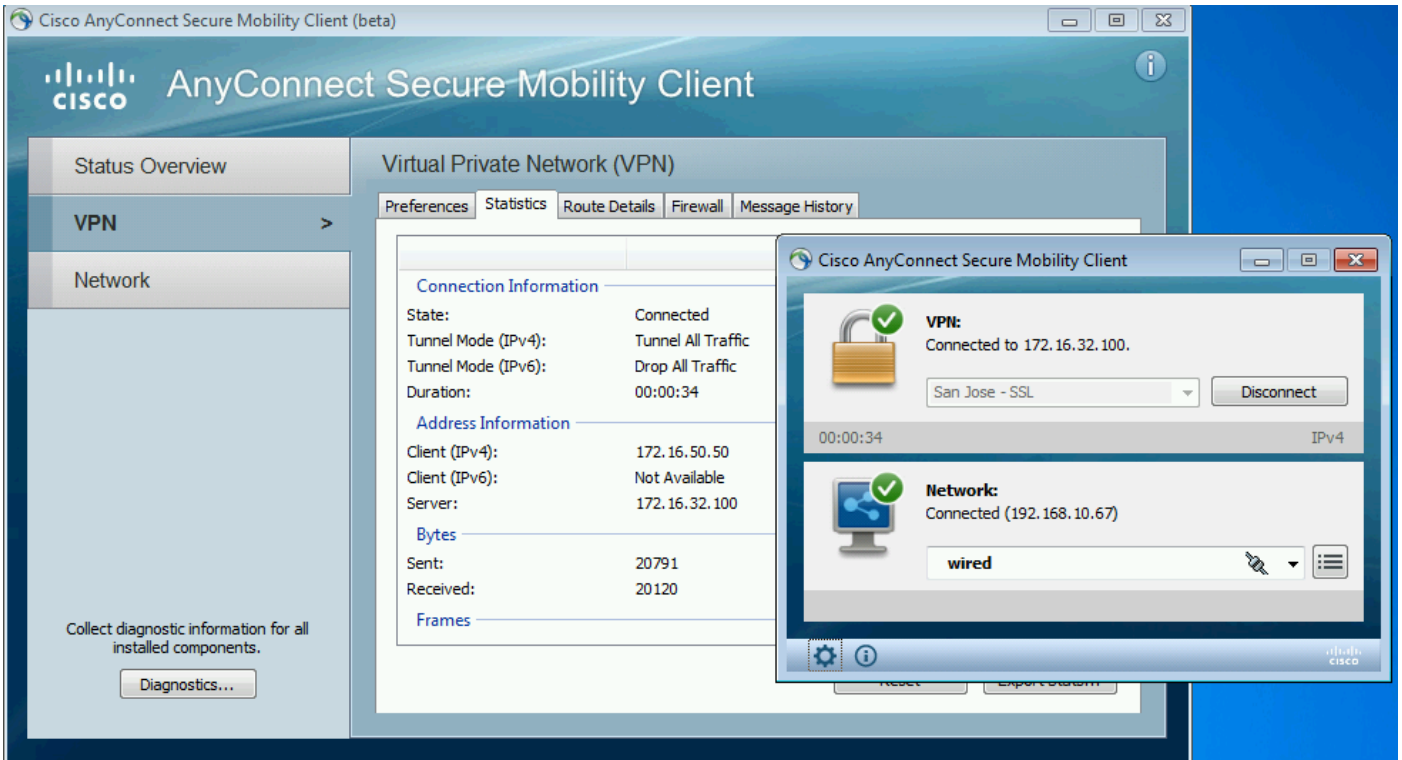
Clear Logs
 Resync
 Refresh

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

Einrichtung von VPN-Sitzungen

Der erste Test wird für ein Szenario durchgeführt, in dem die Autorisierung für die ISE nicht das richtige SGT-Tag zurückgibt (NGIPS lässt keine Audit-Tests zu).

Sobald die VPN-Sitzung die UP AnyConnect-Benutzeroberfläche (UI) ist, können weitere Details bereitgestellt werden:



ASA kann bestätigen, dass die Sitzung eingerichtet wurde:

```
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

Beachten Sie, dass ASA kein SGT-Tag für diese Authentifizierung zurückgibt. ASA ist nicht für TrustSec konfiguriert, sodass Informationen sowieso übersprungen werden.

Die ISE meldet ebenfalls eine erfolgreiche Autorisierung (Protokoll um 23:36:19) - kein SGT-Tag wurde zurückgegeben:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, Administration, and Work Centers. Below this, there are sub-tabs: RADIUS Livelog, TACACS Livelog, Reports, Troubleshoot, and Adaptive Network Control. The main dashboard displays four key metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (278), and Client Stopped Res (0). Below the metrics is a table of live sessions. The table has columns for Time, Status, Det..., Repeat C..., Identity, Authentication Policy, Authorization Policy, Authorization Profiles, Network Device, Server, and Event. Three sessions are listed, all for the user 'Administrator'.

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

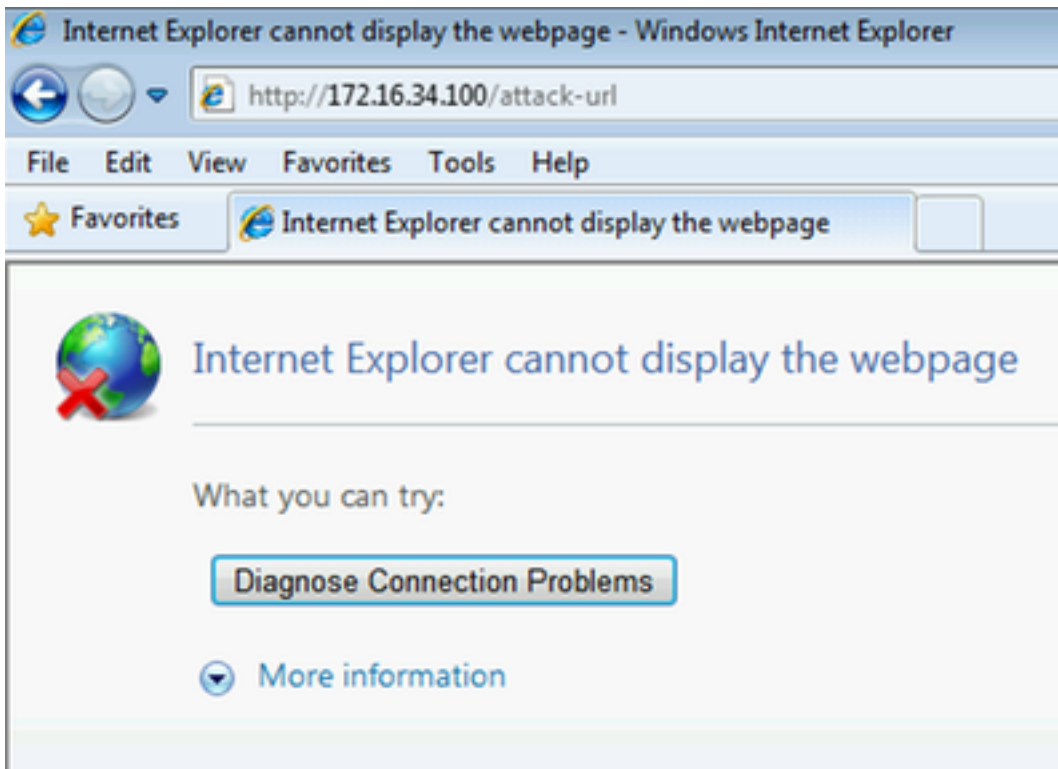
FMC empfängt Sitzungsdaten von MnT

In dieser Phase meldet das FMC in /var/log/messages eine neue Sitzung (die als Teilnehmer für den pxGrid-Dienst empfangen wurde) für den Administratorbenutzernamen und führt eine AD-Suche für die Gruppenmitgliedschaft durch:

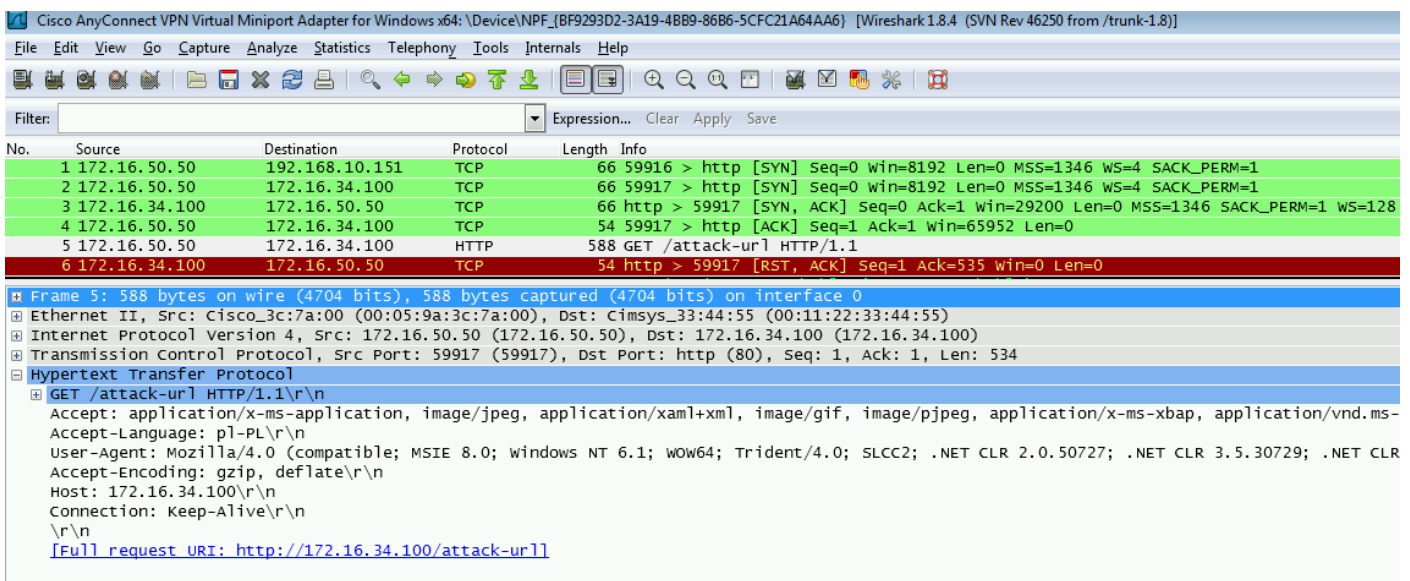
```
firepower SF-IMS[3554]: [17768] ADI:adi.LdapRealm [INFO] search  
'(|(sAMAccountName=Administrator))' has the following DN:  
'CN=Administrator,CN=Users,DC=example,DC=com'.
```

Unprivilegierter und privilegierter Netzwerkzugriff

Wenn der Benutzer zu diesem Zeitpunkt versucht, einen Webbrowser zu öffnen und auf einen überwachten Server zuzugreifen, wird die Verbindung beendet:



Dies kann durch die Paketerfassungen vom Client bestätigt werden (TCP RST-Senden gemäß FMC-Konfiguration):



Sobald die ISE für die Rückgabe konfiguriert ist, werden folgende Berichte über die Audit-Tag-ASA-Sitzung angezeigt:

```
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

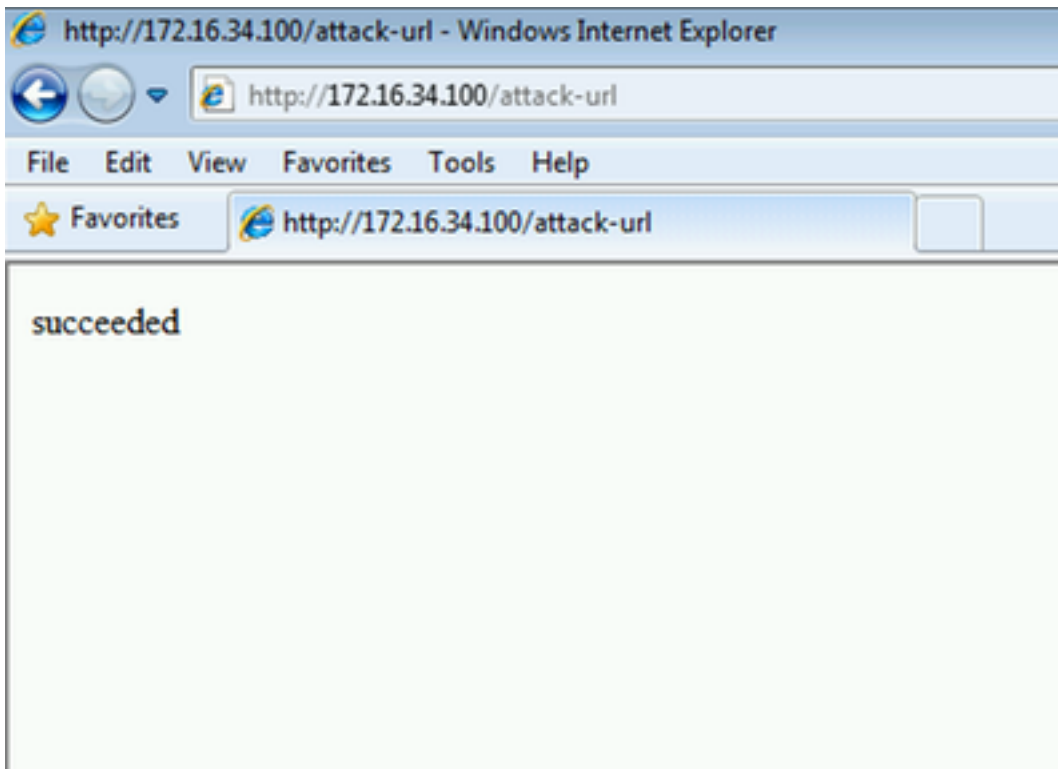
Security Grp : 9

Die ISE meldet auch eine erfolgreiche Autorisierung (das Protokoll wird um 23:37:26 Uhr gesendet) - der SGT-Tag-Auditor wird zurückgegeben:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there is a navigation bar with 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below this, there are tabs for 'RADIUS Live Log', 'TACACS Live Log', 'Reports', 'Troubleshoot', and 'Adaptive Network Control'. The main content area displays four summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (278), and 'Client Stopped Res' (0). Below these cards is a table titled 'Show Live Sessions' with columns for Time, Status, Det..., Repeat C..., Identity, Authentication Policy, Authorization Policy, Authorization Profiles, Network Device, Server, and Event. The table contains three rows of data, all with a status of 'Success' and an event of 'Authentication succeeded'.

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

Der Benutzer kann auf den genannten Service zugreifen:



Zugriff auf FMC-Protokollierung

Diese Aktivität kann im Connection Event-Bericht bestätigt werden:

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	3,252	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

Zuerst hatte der Benutzer kein SGT-Tag zugewiesen und hatte die DenyUnprivileged-HTTP-Regel erreicht. Nachdem der Prüfer-Tag der ISE-Regel zugewiesen (und von der FMC-Regel abgerufen) wurde, wird PermitPrivileged-HTTP verwendet, und der Zugriff ist zulässig.

Beachten Sie außerdem, dass mehrere Spalten entfernt wurden, um die Anzeige zu erhalten, da normalerweise die Zugriffskontrollregel und die Sicherheitsgruppen-Tag-Nummer als eine der letzten Spalten angezeigt werden (und eine horizontale Bildlaufleiste verwendet werden muss). Diese benutzerdefinierte Ansicht kann gespeichert und später wiederverwendet werden.

Fehlerbehebung

FMC-Debugger

So überprüfen Sie die Protokolle der adi-Komponente, die für Identitätsdienste zuständig ist:
 /var/log/messages file:

```
[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_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
```

Um detailliertere Debuggen zu erhalten, ist es möglich, adi-Prozess (von root nach sudo) zu beenden und mit debug argument auszuführen:

```

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.....>
```

SGT-Abfrage über pxGrid

Der Vorgang wird ausgeführt, wenn auf die **Test-Schaltfläche** im Abschnitt **ISE-Integration** geklickt

wird oder wenn die SGT-Liste aktualisiert wird, während die Regel in der Zugriffskontrollrichtlinie hinzugefügt wird.

```
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>fella
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>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>]

```

Für eine bessere Ansicht können XML-Inhalte aus diesem Protokoll in XML-Dateien kopiert und von einem Webbrowser geöffnet werden. Sie können bestätigen, dass sowohl ein bestimmtes SGT (Audit) als auch alle anderen auf der ISE definierten SGT empfangen werden:



```

- <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>

```

Sitzungsabfrage über REST-API zu MnT

Dies ist auch Teil des Test-Vorgangs (beachten Sie, dass der MnT-Hostname und der Port über pxGrid übergeben werden). Massensitzungsdownload wird verwendet:


```

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>UGVybw10QWNjZXNzLEF1ZGl0b3Jz</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>UGVybw10QWNjZXNzLEF1ZGl0b3Jz</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>

```

Analysiertes Ergebnis (1 aktive Sitzung erhalten):

```

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

```

In dieser Phase versucht NGIPS, diesen Benutzernamen (und die Domäne) mit dem Benutzernamen für das Realm-AD zu korrelieren:

```

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 wird verwendet, um einen Benutzer und eine Gruppenmitgliedschaft zu finden:

```

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-Debugging

Nach Aktivierung des TRACE-Level-Debug für die pxGrid-Komponente ist es möglich, jeden Vorgang zu überprüfen (aber ohne Payload/Daten wie auf FMC).

Beispiel für den Abruf von SGT-Tags:

```
2015-12-02 00:05:39,352 DEBUG [pool-1-thread-14][]
cisco.pxgrid.controller.query.CoreAuthorizationManager -::
:::- checking core authorization (topic=TrustSecMetaData, user=firesightisetest-
firepower.example.com
-0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com, operation=subscribe)...
2015-12-02 00:05:39,358 TRACE [pool-1-thread-14][] cisco.pxgrid.controller.common.
LogAdvice -:::-- args: [TrustSecMetaData, subscribe, firesightisetest-firepower.example.com-
0739edea820cc77e04cc7c44200f661e@xg
rid.cisco.com]
2015-12-02 00:05:39,359 DEBUG [pool-1-thread-14][] cisco.pxgrid.controller.persistence.
XgridDaoImpl -:::-- groups [Any, Session] found for client firesightisetest-firepower.
example.com-0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com
2015-12-02 00:05:39,360 DEBUG [pool-1-thread-14][] cisco.pxgrid.controller.persistence.
XgridDaoImpl -:::-- permitted rule found for Session TrustSecMetaData subscribe.
total rules found 1
```

Bug

[CSCuv32295](#) - ISE kann Domäneninformationen in Benutzernamenfeldern senden

[CSCus53796](#) - FQDN des Hosts kann für REST-Massenabfrage nicht abgerufen werden

[CSCuv43145](#) - PXGRID & Identity Mapping Service Restart, Import/Löschen von Trust Store

Referenzen

- [Konfigurieren von Problembehebungsservices mit ISE- und FirePower-Integration](#)
- [Konfigurieren von pxGrid in einer verteilten ISE-Umgebung](#)
- [So stellen Sie Zertifikate mit Cisco pxGrid bereit: Konfigurieren der CA-signierten ISE pxGrid Node und des CA-signierten pxGrid Clients](#)
- [ISE Version 1.3 pxGrid-Integration mit IPS pxLog-Anwendung](#)
- [Administratoranleitung für Cisco Identity Services Engine, Version 2.0](#)
- [Cisco Identity Services Engine API Referenzhandbuch, Version 1.2 - Einführung in External RESTful S...](#)
- [Cisco Identity Services Engine API-Referenzhandbuch, Version 1.2 - Einführung in das Monitoring RES ...](#)
- [Administratoranleitung für Cisco Identity Services Engine, Version 1.3](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)