# Probleemoplossing voor ISE en FirePOWERintegratie voor identiteitsservices

# Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configureren Netwerkdiagram ISE Actieve map Netwerktoegangsapparaat Certificaten voor pxGrid en MnT **PxGrid-service** machtigingsbeleid FMC Actieve map Certificaten voor Admin en PxGrid **ISE-integratie** identiteitsbeleid Toegangsbeheerbeleid Verifiëren **VPN-sessieinstelling** FMC krijgt sessiegegevens van MnT Onbevoorrechte en bevoorrechte netwerktoegang FMC-logtoegang Problemen oplossen **FMC-uiteinden** SGT query via pxGrid Session query via REST API voor MnT **ISE-debugs** Bugs Referenties

# Inleiding

Dit document beschrijft hoe u vertrouwen op TechSec kunt configureren en problemen oplossen bij Cisco Next Generation Inbraakpreventiesysteem (NGIPS). NGIPS versie 6.0 ondersteunt integratie met Identity Services Engine (ISE) zodat een bewust beleid op basis van identiteit kan worden ontwikkeld.

# Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco adaptieve security applicatie (ASA) VPN-configuratie
- Cisco AnyConnect Secure Mobility Client-configuratie
- Cisco FirePOWER Management Center basisconfiguratie
- Cisco ISE-configuratie
- Cisco TrustSec-oplossingen

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Microsoft Windows 2012 certificaatinstantie (CA)
- Cisco ASA versie 9.3
- Cisco ISE-softwareversies 1.4
- Cisco AnyConnect Secure Mobility Client versies 4.2
- Cisco FirePOWER Management Center (FMC) versie 6.0
- Cisco FirePOWER NGIPS versie 6.0

# Configureren

FirePower Management Center (FMC) is het beheerplatform voor FirePOWER. Er zijn twee soorten functies verbonden aan ISE-integratie:

- Remediation stelt het VCC in staat de aanslagpleger in quarantaine te plaatsen via ISE, die dynamisch de status van de vergunning verandert op toegangsapparaat dat beperkte toegang tot het netwerk biedt. Deze oplossing biedt twee generaties:
- 1. Verouderde populariteit bij gebruik van EPS API-aanroepen (Endpoint Protection Service) naar ISE.
- 2. Nieuwe module met behulp van pxGrid-protocolaanroep op ISE (deze module wordt alleen ondersteund in versie 5.4 niet ondersteund in 6.0, standaard ondersteuning gepland in 6.1).
- Beleid stelt FMC in staat om beleid te configureren op basis van Tabellen van de Veiligheidsgroep (SGT).

Dit artikel is gericht op de tweede functionaliteit. Lees voor een voorbeeld van verbetering de referenties

### Netwerkdiagram



FMC 172.16.31.206

FMC is ingesteld met een toegangscontrolebeleid dat twee regels bevat:

- Ontken voor HTTP-verkeer met aangepaste URL (aanval-URL)
- Sta voor HTTP-verkeer met aangepaste URL (aanval-URL) toe maar alleen als de gebruiker wordt toegewezen aan de SGT-tag (9) door ISE

ISE beslist de tag Audit toe te wijzen aan alle gebruikers van de Actieve Map die aan de groep van de Beheerder behoren en ASA-VPN voor netwerktoegang gebruiken.

Gebruiker heeft toegang tot een netwerk via VPN-verbinding op de ASA. De gebruiker probeert dan toegang te krijgen tot de Audated server via URL aanval-url, maar faalt omdat hij niet is toegewezen aan de Controlegroep SGT. Zodra dat is geregeld, is de verbinding succesvol.

### ISE

#### Actieve map

AD-integratie moet worden geconfigureerd en de juiste groepen moeten worden opgehaald (beheerdersgroep wordt gebruikt voor de vergunningsregel):

cisco Ide	ntity Service	es Engine	Home	<ul> <li>Operations</li> </ul>	Policy	Guest Access	<b>→</b> Admini	stration	Work C	enters	
<ul> <li>System</li> </ul>	▼Identity N	lanagement	Network R	esources De	evice Portal N	lanagement pxGri	d Services	Feed Ser	vice 🕨	Identity Mapping	
Identities	Groups	External Ider	ntity Sources	Identity Source	Sequences	Settings					
Extern	al Identity	Sources		Conne	ection	Authentication	Domains	Gro	ups	Attributes	Advanced Settings
<₽ ▼	ti -	estisatian Desfile	£3.+	/ Edit 🕂	Add 👻 🔀 D	elete Group Upda	te SID Value	es			
	ctive Directory			Name example	e.com/Builtin//	Administrators		•	SID examp	le.com/S-1-5-32-544	
• 📄	DAP			example	e.com/Builtin/	Guests			examp	le.com/S-1-5-32-546	
🕨 🧰 F	ADIUS Token			example	e.com/Builtin/I	IIS_IUSRS			examp	le.com/S-1-5-32-568	
🕨 🚞 F	SA SecurID			example	e.com/Builtin/	Users			examp	le.com/S-1-5-32-545	
🕨 📄 S	AML Id Provide	ers		example	e.com/Users/E	Domain Computers			S-1-5-2	21-914949383-20688	43066-3727110587-515
				example	e.com/Users/E	Domain Users			S-1-5-2	21-914949383-20688	43066-3727110587-513

#### Netwerktoegangsapparaat

ASA wordt toegevoegd als netwerkapparaat. Aangepaste groep ASA-VPN-Audit wordt gebruikt, zoals in deze afbeelding:

cisco	Identity Serv	vices Engine	Home	<ul> <li>Operati</li> </ul>	ons Policy	Guest Access	▼ Admin	istration	♦ Worl	k Centers		
<ul> <li>Syster</li> </ul>	m Identi	ty Management	▼Networ	k Resources	Device Portal Ma	nagement pxG	rid Services	Feed S	ervice	<ul> <li>Identity Mapping</li> </ul>		
✓ Netwo	ork Devices	Network Device	Groups	Network Devi	ce Profiles Externa	al RADIUS Servers	s RADIUS	Server Seq	uences	NAC Managers	External MDM	<ul> <li>Location Services</li> </ul>
		G										
Network d	devices		Netwo	work Devices List :	es							
Default De	evice				* Nam	ASA						
					Descriptio							
				* IP Address:	172.16.31.100	/ 32						
						11	<b></b>					
					* Device Profi	le 🐝 Cisco 🔻	0					
					Model Nam	ie	T					
					Software Versio	in	•					
			•	Network Devi	ce Group							
				Location	All Locations	😒 🛛 Set To De	efault					
			ſ	Device Type	ASA-VPN-Audit	Set To De	efault					
				L								
			✓	▼ RADIUS A	uthentication Settings	3						
					Enable Aut	hentication Setting	js					
						Protoc	ol RADIUS					
						* Shared Secr	et		Sł	how		

#### Certificaten voor pxGrid en MnT

FMC gebruikt beide services op ISE:

- pxGrid voor SGT en profilering van gegevens
- Monitoring and Reporting (MnT) voor bulksessiedownload

De beschikbaarheid van MnT is zeer belangrijk aangezien FMC op deze manier wordt geïnformeerd wat het IP-adres is van geauthenticeerde sessie, ook de gebruikersnaam en SGT tag. Op basis daarvan kan het juiste beleid worden toegepast. Merk op dat NGIPS Native SGT-

tags (inline tagging) zoals de ASA niet ondersteunt. Maar in tegenstelling tot ASA ondersteunt het SGT namen in plaats van alleen getallen.

Vanwege deze vereisten moeten zowel ISE als FMC elkaar vertrouwen (certificaat). MnT gebruikt enkel server side certificaat, pxGrid gebruikt zowel client als server side certificaat.

Microsoft CA wordt gebruikt om alle certificaten te ondertekenen.

Voor MnT (Admin-rol) moet ISE certificaat signaalaanvraag (CSR) genereren, zoals in deze afbeelding wordt getoond:

dentity Services Engine	Home  ◆ Operations  ◆ Policy  ◆ Guest Access  ▼Administration  ◆ Work Centers						
System Identity Management	Network Resources     Device Portal Management     pxGrid Services     Feed Service     Identity Mapping						
Deployment Licensing Certifica	ates ▶ Logging ▶ Maintenance Upgrade Backup & Restore ▶ Admin Access ▶ Settings						
0							
▼ Certificate Management	Certificate Signing Request						
Overview	Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:						
System Certificates	ISE Identity Certificates:						
Endpoint Certificates	Admin - Server Authentication						
Trusted Certificates	EAP Authentication - Server Authentication     Portal - Server Authentication						
OCSP Client Profile	pxGrid - Client and Server Authentication						
Certificate Signing Requests	ISE Certificate Authority Certificates:						
Certificate Periodic Check Settings	<ul> <li>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.</li> <li>ISE Intermediate CA - This is an Intermediate CA Signing Request</li> </ul>						
Certificate Authority	Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by						
	the ISE Root CA/ISE Intermediate CA.						
	Usage						
	Certificate(s) will be used for Admin						
	Allow Wildcard   Gertificates						
	Node(s)						
	Generate CSR's for these Nodes:						
	Node CSR Friendly Name						
	☐ lise20 lise20#∆dmin						
	Subject						
	Common Name (CN) \$FQDN\$						

Nadat u door Microsoft CA bent ondertekend, moet u het product via de optie **Bind**- certificaat importeren.

Een soortgelijk proces moet worden gevolgd voor de PxGrid-service. **Certificaat(en) worden gebruikt voor de** optie moet PxGrid zijn geselecteerd.

Aangezien er geen twee certificaten met identieke Onderwerp-naam kunnen zijn, is het volledig aanvaardbaar om verschillende waarde toe te voegen voor OU- of O-sectie (bijvoorbeeld pxGrid).

Opmerking: Zorg ervoor dat voor elke FQDN-naam (Full Qualified Domain Name, FQDN) voor zowel ISE als FMC, de juiste DNS-record is ingesteld op DNS-server.

Het enige verschil tussen Admin en pxGrid certificaat is bij het ondertekenen van proces. Aangezien pxGrid-certificaten uitgebreide toetsuitbreidingsopties voor zowel client- als serververificatie op Microsoft CA moeten zijn gebruikt, kan hiervoor worden gebruikt:

<b>a</b>		Certificate Templates Console
( )	File Action View Help	
	🗢 🔿 🔲 🗶 🗐 🔂	
	🗟 Certificate Templates (WIN-GIH Templa	e 🕻 ISE-pxgrid Properties ? 🗙 nded Purpu 🔿
📕 Das	Adm 🖳	nis
	Auth 🖳	ent Subject Name Issuance Requirements
LOC	🖳 🖳 Basio	EF General Compatibility Request Handling Cryptography Key Attestation
All S	CA E	ch Superseded Templates Extensions Security Server ate Key Arc
🖳 AD	CEP	ind To modify an extension, select it, and then click Edit.
	Cod	Si
	2 Corr	Dur Extensions included in this template:
AD 🖬	Cros	C Application Policies
	🖳 🖳 Direc	tor 🔄 🔄 Basic Constraints 👘 👘 ctory Servi
	2 Dom	ain Certificate Template Information
📸 DNS	l 🖳 Dom	ain Issuance Policies It Authent
📑 File	EFS F	ec Key Usage
	Enro 🖳	lm 📔 📃 🚍
113	Enro 🖳	
	Exch	ng Edit
	Exch	ng
	Exch	ng Description of Application Policies:
	IPSer	Server Authentication
	IPSer	(C) Secure Email Encrypting File System
	ISE-p	Kgt Client Authentication er Authent
	🖉 Kerb	ro ht Authent
	🖉 Key I	ec Recovery A
	l 🖉 ocs	R P Signing
	RAS	nd ht Authent
	Root	Ce
	Rout	er (
	Sma	
	🛛 🔤 Sma	tca Cancel Apply Help

Hoe u Microsoft Web Service gebruikt om pxGrid CSR te ondertekenen wordt in deze afbeelding getoond:

### Submit a Certificate Request or Renewal Request

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

#### Saved Request:

	A0Z4skS+gVGuqYC4ls1jHcXGJejph2h2ndn/ri2J	~
Base-64-encoded	FibxEHkK1tAymQ9G6WXIELdA3XZzV6ilVnWFzLj3	
certificate request	/E2PTchIgFk5zeyXConTNW4QIE/Robkd7DIxduVC	
(CMC or	6C6daW+GKhFTbQFjacvr15KlRWo4/XQZ56QZAzic	1
PKCS #10 or	pB+rRDT3dKQW	ζ.
PKCS #7):	END CERTIFICATE REQUEST	1
-		

#### Certificate Template:

ISE-pxgrid

#### Additional Attributes:

Attributes:		
	Su	bmit >

Aan het eind moet ISE Admin en pxGrid certificaten hebben die door de vertrouwde CA (Microsoft) worden ondertekend zoals in deze afbeelding:

cisco Identity Services Engine	Home	Guest Access     Administration	Mork Centers					
▼System ► Identity Management	▼System → Identity Management → Network Resources → Device Portal Management pxGrid Services → Feed Service → Identity Mapping							
Deployment Licensing Certificate	Deployment Licensing ▼Certificates ) Logging ) Maintenance Upgrade Backup & Restore ) Admin Access ) Settings							
0								
▼ Certificate Management								
Overview	Overview 📝 Edit 🔂 Generate Self Signed Certificate 🔂 Import 🗭 Export 🗙 Delete 🔎 View							
System Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By			
Endpoint Certificates	▼ lise20							
Trusted Certificates	Admin	Admin, Portal	Default Portal Certificate Group	lise20.example.com	example-WIN-CA			
OCSP Client Profile	OCSP Client Profile EAP Authentication lise20.example.com example-WIN-CA							
Certificate Signing Requests	pxgrid	pxGrid		lise20.example.com	example-WIN-CA			
Certificate Periodic Check Settings								

 $\sim$ 

#### PxGrid-service

Met de juiste certificaten moet de pxGrid-rol voor specifiek knooppunt zijn ingeschakeld, zoals in deze afbeelding:

uluulu cisco	Identi	ity Services E	Engine H	Home 🔸	Operations	▶ Policy	• Guest Acces	ss 🗸 🗸 Adm	ninistration	Work Centers
▼ Syst	tem	Identity Mana	agement 🕨 N	letwork Resc	urces 🕨 De	vice Portal Ma	nagement p	xGrid Services	s ▶ Feed S	ervice Identity Mapping
Deplo	yment	Licensing	Certificates	▶ Logging	Mainten	ance Upgra	ade Backup &	& Restore	Admin Acce	ss 🕨 Settings

Deployment	Deployment Nodes List > $lise20$		
	Edit Node		
o     Opployment	General Settings	Profiling Configuration	
N Failover			
	Hostname lis	se20	
	FQDN lis	se20.example.com	
	IP Address 17	72.16.31.210	
	Node Type <b>Id</b>	lentity Services Engine (ISE)	
	Personas		
	✓ Administration	Role STANDALONE Make Primary	7
	✓ Monitoring	Role PRIMARY	onitoring Node
	✓ Policy Service		
	✓ Enable Session S	Services	
	Include No	ode in Node Group None 🔻 🤅	D
	✓ Enable Profiling	Service	
	Enable SXP Servi	ice	
		Use Interface GigabitEthernet 0 +	
	□ Enable Device Ac	dmin Service (i)	
	□ Enable Identity N	Mapping (i)	
	☑ pxGrid ①		

De automatische goedkeuring moet worden ingesteld op:

cisco Identity Services Engine Home   Operations  Police	cy Guest Access Admini	stration			🧿 License Warning 🔺 🔍 🥹 😩 🔅
System Identity Management Network Resources Device Port	al Management pxGrid Services	Feed Service      Identity Mapping	g		
Clients Live Log					⊕ Enable Auto-Registration Disable Auto-Registration View By Capabilities
🖋 Enable 🔗 Disable 🚱 Approve 😝 Group 👎 Decline 😵 Delete 👻	😵 Refresh 🛛 Total Pending Appro	val(0) 💌			1-4 of 4 Show 25 ▼ perpage Page 1 +
Client Name Client Description	Capabilities	Status	Client Group(s)	Log	
□ ▶ ise-admin-lise20	Capabilities(4 Pub, 2 Sub)	Online	Administrator	View	
▶ ise-mnt-lise20	Capabilities(2 Pub, 1 Sub)	Online	Administrator	View	
iseagent-firepower.example.co	Capabilities(0 Pub, 3 Sub)	Online	Session	View	
Firesightisetest-firepower.exampl	Capabilities(0 Pub, 0 Sub)	Offline	Session	View	

#### machtigingsbeleid

Standaard authenticatiebeleid wordt gebruikt (AD raadpleging wordt uitgevoerd als lokale gebruiker niet gevonden wordt).

Het machtigingsbeleid is ingesteld om volledige toegang tot het netwerk te verlenen (Toestemming: PermitAccess) voor gebruikers die zich via ASA-VPN authentiseren en behoren tot Active Directory Group Administrator's - voor deze gebruikers wordt de SGT-tag-accountants teruggegeven:

cisco	Identity	Services Engin	e Home	e • Oper	rations	<ul> <li>Policy</li> </ul>	Guest Access	Administration	<ul> <li>Work Centers</li> </ul>	
Authe	ntication	Authorization	Profiling F	Posture Cl	ient Provisio	ning 🕨	Policy Elements			
Autho	Authorization Policy									
Define t For Poli	iefine the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. or Policy Export go to Administration > System > Backup & Restore > Policy Export Page									
First 1	First Matched Rule Applies									
► Exc	eptions	(0)								
Star	ndard									
	Status	Rule Name			Condition	ns (identity	y groups and other cor	iditions)		Permissions
	<b>~</b>	ASA VPN		it	example /Administr Types#AS	com:Exte ators ANE A-VPN-A	rnalGroups EQUALS e DEVICE:Device Type udit)	example.com/Builtin EQUALS All Device	then	PermitAccess AND Auditors

### FMC

#### Actieve map

Omgekeerde configuratie is vereist om met ISE-integratie te kunnen werken (om identiteitsbeleid te gebruiken en groepslidmaatschap voor passief gewaarmerkte gebruikers terug te halen). Realm kan worden ingesteld voor Active Directory of Lichtgewicht Directory Access Protocol (LDAP). In dit voorbeeld wordt AD gebruikt. Via **systeem > Integratie > Realm**:

### AD-Realm

Enter a description

Directory Realm Configuration User Download									
AD Primary Domain *	example.com	ex: domain.com							
Directory Username *	Administrator@example.com	ex: user@domain							
Directory Password *	•••••								
Base DN *	CN=users,DC=example,DC=com	ex: ou=user,dc=cisco,dc=com							
Group DN *	DC=example,DC=com	ex: ou=group,dc=cisco,dc=com							
Group Attribute	Member 💙								
User Session Timeout									
Authenticated Users	1440	minutes							
Failed Authentication Users	1440	minutes							
Guest Users	1440	minutes							
* Dequired Field									

Standaardindexinstellingen worden gebruikt:



En sommige AD groepen worden opgeroepen (te gebruiken als extra voorwaarde in toegangscontroleregels):

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										
L Download Now										
Available Groups 👛	Groups to Include (5)									
Search by name	🝰 Administrators									
A Terminal Server License Servers	de Users									
Access Control Assistance Operators	Domain Admins									
A Cryptographic Operators	A Domain Users									
A Network Configuration Operators	Admins & Enterprise Admins									

#### Certificaten voor Admin en PxGrid

Internal CAs

Hoewel niet vereist, is het een goede praktijk om CSR te genereren voor toegang tot de beheerder. Meld aan dat CSR gebruikmaakt van een betrouwbaar AD en het ondertekende certificaat terugimporteert, zoals in deze afbeelding:

Overview Analysis Policies D	verview Analysis Policies Devices Objects   AMP Deploy 🛕 System Help 🖲 admin 🗸															
							Configu	ration	Users	Domains	Integration	Updates	Licenses •	Health 🔻	Monitoring	Tools •
													Generate I	New CSR	Import HTTPS	Certificate
Information	Current HTTPS Cort	lificato														
► HTTPS Certificate	Current HTTP5 Cert	lincate														
External Database Access	Subject	commonName firepower.example.com	countryName PL	localityName Krakow	organizationName TAC	organizationalUnitName AAA	stateOrProvince Krakow	Name								
Management Interfaces	Issuer	commonName example-WIN-CA	domainComponent example													
Process	Validity	Not Before	Not After													
Change Reconciliation	Version	Nov 29 12:23:55 2015 GMT 02	Nov 28 12:23:55 20	L6 GMT												
Access Control Preferences	Serial Number	1700000008D385AAF7D2097	EAE000000000008													
Access List Audit Log	Signature Algorithm	sha1WithRSAEncryption														
Dashboard	HTTPS Client Certifi	icate Settings														
DNS Cache Email Notification	Enable Client Certificates															
Intrusion Policy Preferences		Save														
Language																
Login Banner																
Network Analysis Policy Preferences																
SNMP																
STIG Compliance																
Time Constrantian																
Shall Timeout																
Vulnerability Mapping																
VMware Tools																

# Een CA-certificaat moet worden toegevoegd aan een vertrouwde winkel:

Object Management	Intru	usion Rules		
			C Add Trusted Dismiss	
Retwork	ĉ	Name	Value AMP for Network Status	
Port Security Zones		VeriSign Class 3 Public Primary Certification Authority - G5	CN=VeriSign Class 3 Public Primary Certification Authority - G5, ORG=VeriSign, Inc., OU=(c) 2006 VeriSign, Inc For authorized use only, C=05	<i>a</i> a a a a a a a a a a a a a a a a a a
Application Filters		VeriSign Class 4 Public Primary Certification Authority - G3	CN=VeriSign Class 4 Public Primary Certification Authority - G3, ORG=VeriSign, Inc., OU=(c) 1999 VeriSign, Inc For authorized use only, C=US	6
VLAN Tag		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	0
Seolocation		Visa eCommerce Root	CN=Visa eCommerce Root, ORG=VISA, OU=Visa International Service Association, C=US	0
\$ Variable Set		Visa Information Delivery Root CA	CN=Visa Information Delivery Root CA, ORG=VISA, OU=Visa International Service Association, C=US	0
Network Lists and	Feeds	VRK Gov. Root CA	CN=VRK Gov. Root CA, ORG=Vaestorekisterikeskus CA, OU=Varmennepalvelut, C=FI	08
DNS Lists and Fee	is	Wells Fargo Root Certificate Authority	CN=Wells Fargo Root Certificate Authority, ORG=Wells Fargo, OU=Wells Fargo Certification Authority, C=US	0
Sinkhole	15	WellsSecure Public Root Certificate Authority	CN=WellsSecure Public Root Certificate Authority, ORG=Wells Fargo WellsSecure, OU=Wells Fargo Bank NA, C=US	0
File List		Win2012	CN=example-WIN-CA	6
Opher Suite List     Opher Suite List		XRamp Global Certification Authority	CN=XRamp Global Certification Authority, ORG=XRamp Security Services Inc, OU=www.xrampsecurity.com, C=US	0
🛄 Individual Objects 🔁 Object Groups				

Deploy 🛕 System Help 🔻 admin 🔻

De laatste stap is het genereren van het PxGrid-certificaat dat door FMC gebruikt wordt om toestemming te geven aan ISE PxGrid-service. Om CSR CLI te genereren moet worden gebruikt (of een andere externe machine met openssl-gereedschap).

```
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:~#
```

Zodra het vuur.csr is gegenereerd, teken het met Microsoft CA (pxGrid-sjabloon). Import van privé-sleutel (Fire.key) en ondertekend certificaat (fire.pem) naar FMC Interne certificaatwinkel. Gebruik voor privé-toets het wachtwoord dat is ingesteld tijdens het genereren van de toets ( openssl genrsa opdracht):

Overview Analysis Police	les Devices Objects	АМР		
Object Management Intr	usion Rules			
Network	Name		Value	
/Port	pxgrid		CN=firepower.example.com, ORG=TAC, OU=pxgrid, C=PL	
Application Filters				
VLAN Tag				
() URL			Add Known Internal Certificate	? ×
Geolocation			Name: nyorid	
💲 Variable Set			Name. Dagna	
4 💭 Security Intelligence			Certificate Data or, choose a file: Browse	
Network Lists and Feeds			AwICAgCAMA4GCCqGSlb3DQMEAgIAgDAHBgUrDgMCBzAKBggqhkiG9w0DBzANBgkq	<u>^</u>
DNS Lists and Feeds			hkiG9w0BAQUFAAOCAQEASObDPO4nTYpH5Cbwz1nusKooPlUeYtHAJZU7TrgWb1WV XeJET3TrUj3ao9mu+t9jn4yoLC/+qygMl8U2lzb2bhLaxu336/oXGLy/A8S39gnh	
Sinkhole			NZRPXrI11dSYOkfTzWW22yuDvyoTGWnPxF3VGeKfgCZXx9l4SpbNPeWrChx0ku7l PZmDel5KftMi IdWavi4i apilEtiiMand5YVHft/ZdegT1eV69ZdOLHBp4f5BuUYYu	
File List			T8A1m694XbOG4a2GYVf9Jfgfrm1ctTa7ed6yB4oFc9bM8Nb60pxc5H/7r0TjDyuB	
Cipher Suite List			OgnHOPnvdUIPdl/En+dYW/p3l/XoHMv4mR6br9fz6g== END CERTIFICATE	Ň
a 🧃 Distinguished Name				$\sim$
Individual Objects			Key or, choose a file: Browse	
🖶 Object Groups			tHX8NilQM+NBUAtcElUbVb78tkKNuPy5UT5KSBQ4i6E97z53haL4ISyqJYyTiRQa	^
a 🖉 pki			G5OqjWiMD085sUvCayzQh40QhpZf/cECggEAAUZ7CpeuUSdLIDSfKmlkTAbgbykN	
Internal CAs			0n//8oo/MNe46OKr1ZuToUWt9fD01JjvzwTcTnIyZ5DSoXFmIwX2Tu6mSXWq6ycL	
Trusted CAs			7/Ep6UdGhkJTdyU0FsJHT5W3dmnFkWerBS5Cw+eWqCOQacObx0tB5OpwDzw5PQ/G om+WZNf+2LWLvM2dh2dATdywrad0ZjG7RpdV5uYfPkSZOWLigJHI1m+3FpILiMIT	
External Certs			5VwssCFK004DVJhidH6jRqA3VFgvWL/psTUbWknMF8drv8lx4SF1dU4qoA==	
Internal CA Groups				$\sim$
Trusted CA Groups			Encrypted, and the password is:	
Thternal Cert Groups				
External Cert Groups			Save Can	ncel

#### **ISE-integratie**

Nadat alle certificaten zijn geïnstalleerd moet u ISE-integratie vanaf **System > Integration** configureren:

Overview Analysis Policies	Devices Ob	jects AM	Р			
Cisco CSI Realms Identi	ty Sources	eStreamer	Host Inpu	t Client	Smart Soft	ware Satellite
Identity Sources						
Service Type	None Id	entity Services	Engine	User Age	nt	
				_		
Primary Host Name/IP Address *	lise20.example.	.com				
Secondary Host Name/IP Address						
pxGrid Server CA *	Win2012					
MNT Server CA *	Win2012			0		
MC Server Certificate *	pxgrid			0		
ISE Network Filter				ex. 10.	89.31.0/24, 192	.168.8.0/24,
* Required Field	Test	Status				
		i) I	SE connectio	n status:		
			rimary nost:	Success		
					OK	

Gebruik de geïmporteerde CA voor zowel PxGrid- als MnT-servicecertificaten. Gebruik voor Management Console (MC) intern certificaat dat gegenereerd is voor pxGrid.

#### identiteitsbeleid

Configureer het identiteitsbeleid dat eerder ingesteld AD-teken gebruikt voor passieve verificatie:



#### Toegangsbeheerbeleid

Dit voorbeeld is de aangepaste URL gemaakt:



#### En de twee regels in het douanebeleid van toegangscontrole:

	Overview Analysis Policies Devices Objects   AMP Deploy 🛕 System Help 🕶 admin 🔻													
	Access Control ► Access Co	ntrol Network Discov	ery Application Def	ectors Correlation	Actions •									
	CustomPolicy													
	Identity Pelicy     SSL Pelicy:     Image: SSL Pelicy:       Rules     Security Intelligence     HTTP Responses     Advanced													
	B Filter by Device									G	Add Category 📀 Add	Rule Search Rules		×
	# Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	• • •	
	<ul> <li>Mandatory - CustomPolicy</li> </ul>	(1-2)												
	1 PermitPrivileged-HTTP	any	any	any	any	any	🝰 AD-Realm/Administra	t 📩 HTTP	any	any	attack-url	🖋 Allow	🗇 🐚 📕 o	J 🖉
	2 DenyUnprivileged-HTTP	any	any	any	any	any	any	HTTP HTTP	any	any	attack-url	💢 Block with reset	0 🗋 🖉 0	a 🖉
	▼ Default - CustomPolicy (-)													
	There are no rules in this section. Add Rule or Add Category													
- 1	Default Action										Access Control: Trust Al	Traffic		× 1

PermitPrivileged-HTTP-regel staat alle gebruikers toe die tot AD Administrators groep behoren die SGT-tag hebben gekregen. Accountants om HTTP-aanval op alle doelen uit te voeren.

DenyUnbevoorrechte-HTTP ontkent die actie aan alle andere gebruikers.

Let ook op dat het vorige Identity Policy is toegewezen aan dit Access Control Policy.

Op dit tabblad is het niet mogelijk om SGT-tags te zien, maar deze zijn zichtbaar tijdens het maken of bewerken van specifieke regels:

Overview Analysis Policies Devices Objects AMP				Deploy 🛕 System Help 🔻 admin 🔻
Access Control > Access Control Network Discovery Applica	tion Detectors Correlation Actions •			
CustomPolicy Enter a description Identity Policy: <u>EERdicy</u> SSL Policy: <u>None</u>				Cancel
Rules Security Intelligence HTTP Responses Advanced				Theritance Settings   R Policy Assignments (1)
Filter by Device	Editing Rule - PermitPrivileged-HTTP		? ×	Add Category O Add Rule Search Rules
# Name Source Dest Zones Zones	Name PermitPrivileged-HTTP	C Enabled	Move	URLs Action 🖉 🐚 🔳 🛡
▼ Mandatory - CustomPolicy (1-2)	Action 🖌 Allow	✓ IPS: no policies Variables: n/a Files: no	inspection Logging: connections: Event Viewer	
1 PermitPrivileged-HTTP any any	Zones Networks VLAN Tags Users	Applications Ports URLs ISE Attribut	Inspection Logging Comments	🝙 attack-url 🕜 Allow 🔍 🐚 📑 0 🥥 🗒
2 DenyUnprivileged-HTTP any any	Available ISE Session Attributes	Available ISE Metadata 🗳	Selected Source ISE Metadata (1)	🐵 attack-url 🗱 Block with reset 🗇 🗋 🔒 🥔 🗒
▼ Default - CustomPolicy (-)	Search by name or value	Search by name or value	🛃 Auditors 🗍	
There are no rules in this section. Add Rule or Add Category	P Security Group Tag	any 🔒		
Default Action	bevice type	Auditors		Access Control: Trust All Traffic 🛛 👻 🔳
	Location IP	BYOD		
		Contractors		
		Development Servers		
		Employees		
		Guests		
		Potwork_Services		
		PCI_Servers	Add a Location IP Address Add	
			OK Cancel	

Zorg ervoor dat het beleid aan het NGIPS wordt toegewezen en alle wijzigingen worden uitgevoerd:

Overview Analysis Policies	Devices Objects	АМР			
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions 🔻	
Access Control Policy					Status
CustomPolicy					Targeting 1 devices Up-to-date on all targeted devices

## Verifiëren

Nadat alles correct is geconfigureerd zou ISE PxGrid-client moeten intekenen voor een sessieservice (status online).

Home	ns Policy	Guest Access	<ul> <li>Administration</li> </ul>	Work Centers	
letwork Resources	<ul> <li>Device Portal Man</li> </ul>	agement pxGrid	Services Feed	Service 🔹 Identity Mappin	g
Group 🏾 👎 Decline	🛞 Delete 👻 🛞 Re	efresh Total Per	nding Approval(0) 🔻		
Client Description	Cap	abilities	Status		Client Group(s)
	Сар	abilities(4 Pub, 2 S	Sub) Online		Administrator
	Сар	abilities(2 Pub, 1 S	Sub) Online		Administrator
	Cap	abilities(0 Pub, 3 S	Sub) Online		Session
	Home • Operation	Home → Operations → Policy letwork Resources → Device Portal Man Group ● Decline ② Delete ▼ ③ Re Client Description Cap Cap Cap Cap	Home → Operations → Policy → Guest Access Network Resources → Device Portal Management pxGrid Group ● Decline ② Delete ♥ ③ Refresh Total Per Client Description Capabilities Capabilities(4 Pub, 2 S Capabilities(2 Pub, 1 S Capabilities(0 Pub, 3 S	Home <ul> <li>Operations</li> <li>Policy</li> <li>Guest Access</li> <li>Administration</li> <li>Feed</li> <li>Feed</li> <li>Group</li> <li>Decline</li> <li>Delete</li> <li>Refresh</li> <li>Total Pending Approval(0)</li> <li>Client Description</li> <li>Capabilities</li> <li>Status</li> <li>Capabilities(2 Pub, 1 Sub)</li> <li>Online</li> <li>Capabilities(0 Pub, 3 Sub)</li> <li>Online</li> <li>Online</li> <li>Capabilities(0 Pub, 3 Sub)</li> <li>Online</li> <li>Capabilities(0 Pub, 3 Sub)</li> <li>Online</li> <li>Operation</li>         &lt;</ul>	Home <ul> <li>Operations</li> <li>Policy</li> <li>Guest Access</li> <li>Administration</li> <li>Work Centers</li> <li>Feed Service</li> <li>Identity Mappin</li> <li>Feed Service</li> <li>Identity Mappin</li> <li>Group</li> <li>Decline</li> <li>Delete</li> <li>Refresh</li> <li>Total Pending Approval(0)</li> <li>Client Description</li> <li>Capabilities(4 Pub, 2 Sub)</li> <li>Online</li> <li>Capabilities(2 Pub, 1 Sub)</li> <li>Online</li> <li>Capabilities(0 Pub, 3 Sub)</li> <li>Online</li> <li>Online</li> <li>Capabilities(0 Pub, 3 Sub)</li> <li>Online</li>         &lt;</ul>

Uit de logbestanden kan ook worden bevestigd dat FMC zich heeft geabonneerd voor de service TrustSecMetaData (SGT-tags) - alle tags heeft ontvangen en niet heeft geabonneerd.

cisco Ide	ntity Services Engine	Home	<ul> <li>Operation</li> </ul>	ns Policy	<ul> <li>Guest A</li> </ul>	ccess	▼ Admin	istration	♦ Wor	k Cent
<ul> <li>System</li> </ul>	<ul> <li>Identity Management</li> </ul>	Network R	esources	Device Portal M	anagement	pxGrid	Services	In Feed €	Service	Ide

Clients Live Log	iseagent-firepower.exam	ple.com-0739edea820cc77e04cc	7c44200f661e
🔇 Clear Logs 📎 Resync 🥳 Re	efresh		
Client Name	Capability Name	Event Type	Timestamp
firesightisetest-firepower.exampl		Client offline	11:53:14 PM CET, Dec 1 2015
firesightisetest-firepower.exampl	TrustSecMetaData-1.0	Client unsubscribed	11:53:14 PM CET, Dec 1 2015
firesightisetest-firepower.exampl	SessionDirectory-1.0	Client unsubscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl	EndpointProfileMetaData-1.0	Client unsubscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl	SessionDirectory-1.0	Client subscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl	TrustSecMetaData-1.0	Client subscribed	11:53:13 PM CET, Dec 1 2015
firesightisetest-firepower.exampl	EndpointProfileMetaData-1.0	Client subscribed	11:53:12 PM CET, Dec 1 2015
firesightisetest-firepower.exampl		Client online	11:53:12 PM CET, Dec 1 2015

#### **VPN-sessieinstelling**

De eerste test wordt uitgevoerd bij een scenario waarbij de vergunning op ISE niet de juiste SGTtag teruggeeft (NGIPS staat geen audittests toe). Zodra VPN-sessie is UP kan AnyConnect User Interface (UI) meer details bieden:

S Cisco AnyConnect Secure Mobility Client (	beta)				3
ululu AnyConnec	t Secure Mobil	ity Client		1	
Status Overview	Virtual Private Network	(VPN)			
VPN >	Preferences Statistics Route	Details Firewall Mess	age History		
Network	Connection Information -		🕥 Cisco AnyCo	onnect Secure Mobility Client	
Collect discreptic information for all	State: Tunnel Mode (IPv4): Tunnel Mode (IPv6): Duration: Address Information Client (IPv4): Client (IPv6): Server: Bytes Sent: Received: Frames	Connected Tunnel All Traffic Drop All Traffic 00:00:34 172.16.50.50 Not Available 172.16.32.100 20791 20120	00:00:34	VPN: Connected to 172.16.32.100. San Jose - SSL Network: Connected (192.168.10.67) wired	
installed components.			ن 🗘		altalta cisco
Diagnostics		_			

ASA kan bevestigen dat de sessie is vastgesteld:

#### asav# show vpn-sessiondb anyconnect

Session Type: AnyConnect

```
Username : Administrator
Assigned IP : 172.16.50.50
                                      Index : 1
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
```

Merk op dat ASA een SGT-tag voor deze verificatie ziet. ASA is niet ingesteld voor TrustSec - dus wordt de informatie toch overgeslagen.

ISE rapporteert ook over een succesvolle vergunning (het logboek om 23:36:19) - er is geen SGTtag teruggegeven:

cisco Identity Se	ervices Engine	Home	▼Operations	▶ Policy	Guest Access	Administration	n → Work Cente	ers			
RADIUS Livelog	TACACS Livelog	Reports	Troubleshoot	Adaptive	Network Control						
Mi	sconfigured Supp	licants 🔅			Misconfigured Netv	vork Devices 🛈		RADIUS	Client Stopped Res		
	0			0			27	0			
Show Live See	sions 🙀 Add or	Remove Co	lumns 🔻 🛞 Ref	resh 🚯 Re	set Repeat Counts						Refresh
Time	▼ Status All ▼ De	et Repe	at C	y () AI	uthentication Policy	Aut	norization Policy	Authorization Profiles	Network Device	Server ()	Event (
2015-12-01 23:3	7:31 🍈	à	0 Admini	strator De	efault >> Default >:	> Default Defa	ult >> ASA VPN	PermitAccess, Auditors		lise20	Session State is Started
2015-12-01 23:3	7:26 🔽	0	Admini	strator De	efault >> Default >:	> Default Defa	ult >> ASA VPN	PermitAccess,Auditors	ASA	lise20	Authentication succeeded
2015-12-01 23:3	6:19 🗹	Q	Admini	strator De	efault >> Default >:	> Default Defa	ult >> ASA VPN	PermitAccess	ASA	lise20	Authentication succeeded

#### FMC krijgt sessiegegevens van MnT

In die fase rapporteert FMC in /var/log/messen een nieuwe sessie (ontvangen als abonnee voor pxGrid-service) voor Administrator-gebruikersnaam en AD-raadpleging voor groepslidmaatschap:

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

#### Onbevoorrechte en bevoorrechte netwerktoegang

Wanneer de gebruiker in dat stadium probeert een webbrowser te openen en een door een toegangscontrole gecontroleerde server te openen, wordt de verbinding beëindigd:



Het kan worden bevestigd door de pakketvastlegging die van de client is genomen (TCP RST verzenden als per FMC-configuratie):

n	Cisco	AnyConr	ect VPN V	/irtual N	/liniport A	dapter for V	Vindows x	64: \Device	ice\NPF_{BF9293D2-3A19-4BB9-86B6-5CFC21A64AA6} [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]	
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o <u>C</u> a	pture	<u>A</u> nalyze	<u>S</u> tatistics	Telephor	n <u>y T</u> ools	ls <u>I</u> nternals <u>H</u> elp	
	١.	9	💓   E	3 🔒	* 2	8   Q	🔶 🔿	ي 🔄	7 ½   🗐 🗐   Q, Q, Q, 💟   👪 🗵 畅 %   💢	
Filte	er:								Expression Clear Apply Save	
No.		Source			Destina	ation		Protocol	ol Length Info	
	1	172.16	.50.50		192.3	168.10.1	.51	TCP	66 59916 > http [SYN] Seq=0 Win=8192 Len=0 MS5=1346 WS=4 SACK_PERM=1	
	2	172.16	.50.50		172.3	16.34.10	00	TCP	66 59917 > http [SYN] Seq=0 win=8192 Len=0 MSS=1346 WS=4 SACK_PERM=1	
	3	172.16	.34.10	0	172.3	16.50.50	)	тср	66 http > 59917 [SYN, ACK] seq=0 Ack=1 win=29200 Len=0 MSS=1346 SACK_PERM=1 WS=	128
	4	172.16	.50.50		172.3	16.34.10	)0	тср	54 59917 > http [ACK] Seq=1 Ack=1 Win=65952 Len=0	
	5	172.16	.50.50		172.3	16.34.10	00	HTTP	588 GET /attack-url HTTP/1.1	
	6	172.16	.34.10	0	172.3	16.50.50	)	ТСР	54 http > 59917 [RST, ACK] Seq=1 Ack=535 Win=0 Len=0	
🖽 F	rame	5: 58	8 byte	s on	wire (4	4704 bit	s), 58	8 bytes	s captured (4704 bits) on interface 0	
+ E	ther	net II	, Src:	Cisc	o_3c:7a	a:00 (00	:05:9a	:3c:7a:	::00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)	
+ 1	nter	net Pr	otocol	Vers	ion 4,	Src: 17	2.16.5	0.50 (1	172.16.50.50), Dst: 172.16.34.100 (172.16.34.100)	
+ T	rans	missio	on Cont	rol P	rotoco	l, Src P	ort: 5	9917 (5	59917), Dst Port: http (80), Seq: 1, Ack: 1, Len: 534	
	lyper	text 1	ransfe	r Pro	tocol					
B	GET	⁻/atta	ick-url	HTTP	/1.1\r`	\n				
	Aco	ept: a	upplica	tion/	x-ms-ap	oplicati	on, im	age/jpe	eg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.	ms-
	Aco	ept-La	inguage	: pl-	PL\r\n					
	Use	er – Ager	nt: Moz	illa/	4.0 (co	ompatibl	e; MSI	E 8.0;	Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET	CLR
	Aco	ept-Er	ncoding	: gzi	p, def	late\r\n	1			
	Hos	t: 172	.16.34	.100\	r \n					
	Cor	nectio	on: Kee	p-Ali	ve\r\n					
	\r\	n,							22	
	<u>  Fi</u>	ill rec	uest U	RI: h	ttp://:	L/2.16.3	4.100/	<u>attack-</u>	<u>-urii</u>	

Zodra ISE is ingesteld om terug te keren, meldt de ASA-sessie van de audit:

asav# show vpn-sessiondb anyconnect

```
Session Type: AnyConnect

        Username
        : Administrator
        Index
        : 1

        Assigned IP
        : 172.16.50.50
        Public IP
        : 192.168.10.67

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License
            : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel:
(1)AES128
Hashing : AnyConnect-Parent: (1) none SSL-Tunnel: (1) SHA1 DTLS-Tunnel:
(1) SHA1
Bytes Tx : 11428
                                       Bytes Rx
                                                     :
24604
Group Policy : POLICY Tunnel Group :
SSLVPN
Login Time : 12:22:59 UTC Wed Dec 2
2015
Duration :
0h:01m:49s
Inactivity :
0h:00m:00s
VLAN Mapping : N/A
                                       VLAN :
none
Audt Sess ID : ac101f6400001000565ee2a3
Security Grp : 9
ISE meldt ook een geslaagde vergunning (het logboek om 23:37:26) - SGT-tag Auditor wordt
```

#### teruggegeven:

cisco Identity S	ervices Engine	Home	✓Operation:	Policy	→ Guest Access	Administrati	ion 🔹 Work Cente	ers			
RADIUS Livelog	TACACS Livelog	Reports	Troublesho	ot 🕨 Adaptive	e Network Control						
м	isconfigured Supp	olicants 🔅			Misconfigured Netw	ork Devices	1)	RADIUS I	Client Stopped Res		
	0				0			27	0		
<u> </u> Show Live Se	ssions 🙀 Add or	Remove Co	olumns 🔻 🛞 I	lefresh 🛛 😨 R	Reset Repeat Counts						Refresh
Time	▼ Status All ▼ D	et Repe	eat C	itity 🕐 🔺	Authentication Policy	(i) Au	thorization Policy	Authorization Profiles (	Network Device	Server (i)	Event ()
2015-12-01 23:3	37:31 🍈	<u> </u>	0 Adm	inistrator D	)efault >> Default >>	> Default De	fault >> ASA VPN	PermitAccess,Auditors		lise20	Session State is Started
2015-12-01 23:3	37:26 🔽	0	Adm	inistrator D	)efault >> Default >>	> Default De	fault >> ASA VPN	PermitAccess,Auditors	ASA	lise20	Authentication succeeded
2015-12-01 23:3	6:19	6	Adm	inistrator D	)efault >> Default >>	Default De	fault >> ASA VPN	PermitAccess	ASA	lise20	Authentication succeeded

En de gebruiker kan de genoemde service benaderen:

S → F http://172.16.34.100/attack-url	
File Edit View Favorites Tools Help	
Favorites Attp://172.16.34.100/attack-url	
succeeded	

#### FMC-logtoegang

Deze activiteit kan worden bevestigd door het verbindingsrapport:

														_			
Overview	Analysis Policie	es Devices C	Objects AMP											D	eploy 🛕 S	ystem Help 🔻	admin 🔻
Context Exp	lorer Connection	is ► Events	Intrusions • Fil	es ♥ Hosts ♥ Users ♥ V	ulnerabilities • 0	Correlation 🔻	Custom 🔻	Search									
												Bookmark 1	This Page Repor	t Desig	gner Dashboard	View Bookmarks	Search 🔻
Connection Events (antch workflow)																	
						Info			×								
						Deleted	9 Connectio	n(s)									
Connections with Application Details > Table View of Connection Events														<u>20</u>	015-12-01 21:24:	00 - 2015-12-01	23:46:59
Search Cor	straints (Edit Search Sa	ve Search)														Disab	oled Columns
Jump to	*																
	★ Last Packet ×	Action ×	Initiator IP ×	Initiator User ×	Responder × IP	Ingress Security Zone	× A	pplication >> rotocol	Access Control >	Access Control X Rule	Security X Group Tag	Ingress × Interface	NetBIOS Domain	×	Initiator × Packets	Initiator × Bytes	Count
1	2015-12-01 23:38:19	Allow	172.16.50.50	AD-Realm\administrator (LDAP)	i <u>172.16.34.100</u>	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			<u>12</u>	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
4	2015-12-01 23:25:11	Allow	172.16.50.50	AD-Realm\administrator (LDAP)	172.16.34.100	Internal		HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors	eth1			22	3,752	1
+		Block with reset	172.16.50.50	AD-Realm\administrator (LDAP)	172.16.34.100	Internal		HTTP	CustomPolicy	DenyUnprivileged-HTTP		eth1			25	3,938	5
I< < Page	1 of $1 > > $ Displayi	ng rows 1-5 of 5 r	rows														
View	Delete																
Marris Al	Delete All																

Eerst had de gebruiker geen SGT-tag toegewezen en pakte hij de DenyUnbevoorrechte-HTTPregel in. Zodra de tag van de auditor door ISE (en opgehaald door FMC) is toegewezen, wordt PermitPrivileged-HTTP gebruikt en is toegang toegestaan. Merk ook op dat om de weergave te hebben, meerdere kolommen zijn verwijderd omdat normaal gesproken toegangscontroleregel en beveiligingsgroepmarkering worden weergegeven als een van de laatste kolommen (en er moet een horizontale schuifbalk worden gebruikt). Deze aangepaste weergave kan in de toekomst worden opgeslagen en opnieuw worden gebruikt.

### Problemen oplossen

#### **FMC-uiteinden**

U kunt de loggen van de adi-component die verantwoordelijk is voor de identiteitsdiensten, als volgt controleren:

```
[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<sup>M</sup>'
[8893] ADI:ADI [INFO] : sub command emits: 'Host: lise20.example.com:8910^M'
[8893] ADI:ADI [INFO] : sub command emits: 'Accept: */*^M'
[8893] ADI:ADI [INFO] : sub command emits: 'Content-Type: application/xml^M'
[8893] ADI:ADI [INFO] : sub command emits: 'user:firesightisetest-firepower.example.com-
0739edea820cc77e04cc7c44200f661e@xgrid.cisco.com^M'
[8893] ADI: ADI [INFO] : sub command emits: 'Content-Length: 269^M'
[8893] ADI:ADI [INFO] : sub command emits: '^M'
[8893] ADI:ADI [INFO] : sub command emits: '* upload completely sent off: 269 out of 269 bytes'
[8893] ADI:ADI [INFO] : sub command emits: '< HTTP/1.1 200 OK^M'
[8893] ADI:ADI [INFO] : sub command emits: '< Date: Tue, 01 Dec 2015 23:10:45 GMT^M'
[8893] ADI:ADI [INFO] : sub command emits: '< Content-Type: application/xml^M'
[8893] ADI:ADI [INFO] : sub command emits: '< Content-Length: 1287^M'
[8893] ADI: ADI [INFO] : sub command emits: '< Server: ^M'
[8893] ADI:ADI [INFO] : sub command emits: '< ^M'
[8893] ADI:ADI [INFO] : sub command emits: '* Connection #0 to host lise20.example.com left
intact'
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] bulk download processed 0 entries.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] disconnecting pxgrid
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: Starting reconnection stop
[23510] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: _reconnection_thread exited
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: stream closed; err_dom=(null) 2015-12-01T23:10:45 [ INFO]: clientDisconnectedCb ->
destroying client object
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: pxgrid connection shutdown done successfully
[23511] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: Exiting from event base loop
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: successfully disconnected
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: connection disconnect done .....
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying pxgrid reconnection
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying underlying pxgrid
connection
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] destroying pxgrid config
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] ISE identity feed destructor called
[23509] ADI_ISE_Test_Help:ADI_ISE_Test_Help [INFO] /usr/local/sf/bin/adi_iseTestHelp cleanly
exits.
[23509] ADI_ISE_Test_Help:adi.ISEConnection [INFO] Captured Jabberwerx log:2015-12-01T23:10:45 [
INFO]: pxgrid library has been uninitialized
[8893] ADI:ADI [INFO] Parent done waiting, child completed with integer status 0
```

Om gedetailleerdere uitwerpselen te krijgen is het mogelijk om adi-proces te doden (van wortel na eind) en het te draaien met debug argument:

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 query via pxGrid

De bewerking wordt uitgevoerd wanneer op de **Test**-knop wordt gedrukt in **ISE Integration** sectie of wanneer de SGT-lijst wordt ververst, terwijl regels in Access Control Policy worden toegevoegd.

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] 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: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: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:taq>5</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: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: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: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: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: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-11e5-978e005056bf2f0a</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:SecurityGroup><ns5:SecurityGroup><ns5:id>fe62d8 f0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Quarantined\_Systems</ns5:name><ns5:description>Quarantine Security Group</ns5:description><ns5:tag>255</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe7d 3ec0-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Test\_Servers</ns5:name><ns5:description>Test Servers Security Group</ns5:description><ns5:tag>13</ns5:tag></ns5:SecurityGroup><ns5:SecurityGroup><ns5:id>fe99c 770-6d8f-11e5-978e-005056bf2f0a</ns5:id><ns5:name>TrustSec\_Devices</ns5:name><ns5:description>TrustSec Devices Security Group</ns5:description><ns5:tag>2</ns5:SecurityGroup></ns5:SecurityGroup></ns5:description><ns5:getSecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5:SecurityGroup></ns5 urityGroupListResponse>]

Voor een beter beeld kunt u de inhoud van xml uit dat logbestand kopiëren naar xml-bestand en openen door een webbrowser. U kunt bevestigen dat specifieke SGT (audit) wordt ontvangen evenals alle andere SGT die op ISE is gedefinieerd:

```
-<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>
```

#### Session query via REST API voor MnT

Dat is ook een onderdeel van Test operation (noteer dat MnT hostname en poort via pxGrid wordt doorgegeven). Downloadsessie:

```
Dec 01 23:14:39 firepower SF-IMS[24106]: [24143] ADI:adi.pxGridAdapter [DEBUG]
adi.cpp:319:HandleLog(): returns [OK, p_node*:0x7f0ea6ffa8a8(<session
xmlns='http://www.cisco.com/pxgrid/net'><gid
xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime
xmlns='http://www.cisco.com/pxgrid'>2015-12-
01T23:37:31.191+01:00</lastUpdateTime><extraAttributes
xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt
tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-
Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress
xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceMgmtIntfID></deviceAttachPt
></interface><user><name</pre>
```

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</pre> xmlns='http://www.cisco.com/pxgrid'>ac101f6400007000565d597f</gid><lastUpdateTime</pre> xmlns='http://www.cisco.com/pxgrid'>2015-12-01T23:37:31.191+01:00</lastUpdateTime><extraAttributes xmlns='http://www.cisco.com/pxgrid'><attribute>UGVybWl0QWNjZXNzLEF1ZG10b3Jz</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>

#### En ontkoppeld resultaat (1 actieve sessie ontvangen):

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 die fase probeert NGIPS die gebruikersnaam (en domein) te correleren met Realm-ADgebruikersnaam:

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 wordt gebruikt om een gebruiker- en groepslidmaatschap te vinden:

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-debugs**

Nadat u TRACE level-debug voor pxGrid-component hebt ingeschakeld, kan deze elke handeling controleren (maar zonder payload/data zoals op FMC).

Voorbeeld met SGT-tagophalen:

```
-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
```

# Bugs

CSCuv3295 - ISE kan domeininformatie in gebruikersnaam-velden verzenden

CSCus53796 - Kan geen FQDN van host voor REST-bulkquery krijgen

<u>CSCuv43145</u> - PXGRID & Identity mapping Service opnieuw opstarten, importeren/verwijderen van een trustwinkel

## Referenties

- <u>Remediatieservices met ISE en FirePower-integratie configureren</u>
- PxGrid configureren in een gedistribueerde ISE-omgeving
- Hoe u certificaten kunt implementeren met Cisco PxGrid: De configuratie van CA-Ondertekende ISE PxGrid-knooppunt en CA-ondertekende PxGrid-client
- ISE versie 1.3 pxGrid-integratie met IPS PxLog toepassing
- Administrator-gids voor Cisco Identity Services Engine, release 2.0
- Referentiegids voor Cisco Identity Services Engine API, release 1.2 Inleiding naar extern
   RESTful S...
- <u>Referentiegids voor Cisco Identity Services Engine API, release 1.2 Inleiding over de</u>
   <u>bewaking van SRE...</u>
- Administrator-gids voor Cisco Identity Services Engine, release 1.3
- Technische ondersteuning en documentatie Cisco-systemen