Fehlerbehebung bei ISE- und FirePOWER-Integration für Identity Services

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm 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-Debugaer** 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



FMC 172.16.31.206

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

- Für HTTP-Datenverkehr mit benutzerdefinierter URL verweigern (Attach-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):

▶ System ▼ Identity Management ▶ Network Resources ▶ Device Portal Management pxGrid Services ▶ Feed Service ▶ Identity Mapping ▶ Identities Groups External Identity Sources Identity Source Sequences > Settings External Identity Sources Identity Source Sequences > Settings Connection Authentication Domains Groups Attributes Advanced Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Settings Image: Configure Sequences > Secure Sequences Image: Configure Sequence Image: Configure Sequences > Secure Sequences > Secure Sequences > Secure Sequences Image: Configure Sequence Name SID Image: Configure Sequences > Secure Sequences Image: Configure Sequence Name SID Image: Configure Sequences > Secure S	cisco Identity Services Engine Home	Operations → Policy → Guest Access		
Identities Groups External Identity Sources Identity Sources Attributes Advanced Sett Image: Setting sett	► System Identity Management Network Re	sources Device Portal Management pxGrid	d Services	
External Identity Sources Connection Authentication Domains Groups Attributes Advanced Sett Image: Single com/Settion Profile Image: Single com/Setion Profile Im	Identities Groups External Identity Sources	Identity Source Sequences Settings		
	External Identity Sources	Connection Authentication I	Domains Groups Attributes Advanced Settin	tings
Image: Sample com/Users/Domain Computers S-1-5-21-914949383-2068843066-3727110587-51 example.com/Users/Domain Users S-1-5-21-914949383-2068843066-3727110587-51		Name example.com/Builtin/Administrators example.com/Builtin/Guests example.com/Builtin/IIS_IUSRS example.com/Builtin/Users example.com/Users/Domain Computers example.com/Users/Domain Users	 SID example.com/S-1-5-32-544 example.com/S-1-5-32-546 example.com/S-1-5-32-568 example.com/S-1-5-32-545 S-1-5-21-914949383-2068843066-3727110587-515 S-1-5-21-914949383-2068843066-3727110587-513 	15 13

Netzwerkzugriffsgerät

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

cisco Identity Services Engine	Home • Opera	tions Policy	 Guest Access 	 Administration 	 Work Centers 		
System Identity Management	Network Resources	Device Portal Ma	nagement pxGrid	Services Feed S	Service 🔹 Identity Mappin	g	
Network Devices Network Device	Groups Network Dev	vice Profiles Externa	I RADIUS Servers	RADIUS Server Sec	quences NAC Managers	External MDM	 Location Services
0							
Network devices	Network Devices List	> ASA Ces					
Default Device		* Nam	ο Δ5Δ				
		Descriptio	n				
		Decempto					
	* IP Address	: 172.16.31.100	/ 32				
			th oliver (
		* Device Profil	e asto CISCO V	,			
		Model Nam	e	<u>·</u>			
		Software Versio	n	r			
	* Network De	vice Group					
	Location	All Locations	📀 🛛 Set To Defa	ult			
	Device Type	ASA-VPN-Audit	📀 🛛 Set To Defa	ult			
	✓ RADIUS	Authentication Settings					
		Enable Aut	nentication Settings				
			Protocol	RADIUS			
			* Shared Secret	•••••	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:

cisco 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								
Deployment Licensing Certifica	ates ▶ Logging ▶ Maintenance Upgrade Backup & Restore ▶ Admin Access ▶ Settings								
G									
▼ 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	 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 								
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								
	Node(s) Generate CSR's for these Nodes:								
	Node CSR Friendly Name								
	Subject								
	Common Name (CN) \$FQDN\$								

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 Domänennamen (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:

a		Certificate Templates Console	
()	File Action View Help		
C	🗢 🔿 🕅 💥 🗐 🔒 🛛 🗊		_
	🖉 Certificate Templates (WIN-GIH Template 🛛	ISE-pxgrid Properties ? 🗙	nded Purpi 🔨
🔛 Das	Adminis 🖉		
Loc	Authent 🗐 🖉	Subject Name Issuance Requirements	
	🖉 Basic EF	General Compatibility Request Handling Cryptography Key Attestation	
All S	🖉 CA Exch	Superseded remplates Excisions Security Server	ate Key Arc
🖳 AD	EP End	To modify an extension, select it, and then click Edit.	
	Code Si		
	Comput	Extensions included in this template:	
AD 🖻		Application Policies	
😭 AD	2 Director	Basic Constraints	ctory Servi
	🖾 Domain	Esturicate Template Information	at Augth and
	Domain		nt Authent
🕒 File	🖾 EFS Reci		
IIS 🕲			=
	I Enrollini I Evchand		
	Exchang Exchang	Edit	
	Rechange Rechange	Description of Application Delivion	
		Description of Application Policies.	
		Secure Email	
	ISE-pyge	Encrypting File System	er Authent
	Rethero	(energe-warderige-bio))	nt Authent
	Rev Rec	▼	Recovery A
	I OCSP R		P Signing
	💷 RAS and		ht Authent
	🗔 Root Ce		
	🗵 Router (
	🚇 Smartca		
	💹 Smartca	OK Cancel Apply Help	

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:

	A0Z4skS+gVGuqYC4ls1jHcXGJejph2h2nd	dn/ri2J 🛆
Base-64-encoded	FibxEHkK1tAymQ9G6WXIELdA3XZzV6ilVr	nWFzLj3
certificate request	/E2PTchIgFk5zeyXConTNW4QIE/Robkd7[DIxduVC
(CMC or	6C6daW+GKhFTbQFjacvr15KlRWo4/XQZ50	5QZAzic 🔲
PKCS #10 or	pB+rRDT3dKQW	~
PKCS #7):	END CERTIFICATE REQUEST	\sim
-		$\langle \rangle$

Certificate Template:

ISE-pxgrid

Additional Attributes:

Attributes:		
	S	ubmit >

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

cisco Identity Services Engine	Home	Guest Access Administration	 Work Centers 					
System Hentity Management Network Resources Device Portal Management pxGrid Services Feed Service Hentity Mapping								
Deployment Licensing Certificate	es ▶Logging ▶Maintenance Upgra	ade Backup & Restore 🕨 Admin Ac	cess Settings					
0								
▼ Certificate Management	System Certificates 🔺 For disa	ster recovery it is recommended to expo	rt certificate and private key pairs of all sy	stem certificates.				
Overview	/ Edit Generate Self Signe	d Certificate] 🕂 Import] 🕼 Exp	port 🗙 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 $\operatorname{Group}(i)$	lise20.example.com	example-WIN-CA			
OCSP Client Profile	EAP	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

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

diadia cisco	Identi	ity Services I	Engine	Home 🔸	Operations	▶ Policy	In Guest Ac	ccess	▼Administration	• Work Ce	nters
▼ Syst	tem	Identity Mana	agement 🕨 N	Network Resc	urces De	evice Portal Ma	anagement	pxGrid	Services Feed S	Service 🕨 la	dentity Mapping
Deplo	yment	Licensing	 Certificates 	▶ Logging	Mainten	nance Upgr	ade Back	up & Res	tore 🕨 Admin Acc	ess 🕨 Settir	ngs

Deployment	Deployment Nodes List > $lise20$	
↓	Edit Node	
	General Settings	Profiling Configuration
🐝 PAN Failover		
	Hostname lise2	20
	FQDN lise2	20.example.com
	IP Address 172.	.16.31.210
	Node Type Iden	ntity Services Engine (ISE)
	Personas	
	☑ Administration	Role STANDALONE Make Primary
	☑ Monitoring	Role PRIMARY
	✓ Policy Service	
	✓ Enable Session Ser	vices
	Include Node	in Node Group v (i)
	✓ Enable Profiling Se	rvice
	Enable SXP Service	9
		Use Interface GigabitEthernet 0 (i)
	□ Enable Device Adm	in Service (i)
	Enable Identity Maj	pping (i)
	<mark>▼ pxGrid</mark> ①	

Die automatische Genehmigung muss aktiviert sein:

cisco Identity Services Engine Home Operations Police	cy • Guest Access • Admini	Istration • Work Centers			🧿 License Warning 🔥 🔍 🥹 🛔 🔅
System Identity Management Network Resources Device Port	al Management pxGrid Services	Feed Service Identity Mappin	ng		
Clients Live Log					⊕ Enable Auto-Registration Disable Auto-Registration View By Capabilities
🖋 Enable 🔗 Disable 🚱 Approve 😝 Group 👎 Decline 😵 Delete 👻	🛞 Refresh 🛛 Total Pending Appro	oval(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	

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:

cisco	Identity	Services Engin	e Hor	ne 🔸	Operations	 Policy 	Guest Access	 Administration 	 Work Centers 	
Auther	ntication	Authorization	Profiling	Posture	Client Provi	sioning 🕨	Policy Elements			
Autho	rizatio	n Policy								
Define ti For Polic	he Authori sy Export (ization Policy by c 30 to Administratic	onfiguring ru in > System :	les based > Backup &	on identity gro & Restore > Po	oups and/or o plicy Export P	ther conditions. Drag a age	and drop rules to chan	ge the order.	
First M	fatched	Rule Applies	*							
► Exc	eptions	(0)								
Star	ndard									
	Status	Rule Name			Condi	tions (identity	groups and other con	ditions)		Permissions
		ASA VPN			if <mark>(</mark> exam /Admin Types /	ole.com:Exter iistrators ANE ASA-VPN-Au	rnalGroups EQUALS e) DEVICE:Device Type udit)	example.com/Builtin	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

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						
* Required Field								

Es werden folgende Standardverzeichniseinstellungen verwendet:



Einige AD-Gruppen werden abgerufen (als zusätzliche Bedingung in Zugriffskontrollregeln zu verwenden):

Overview Analysis Policies Devices Obje	ects AMP
AD-Realm Enter a description	
Directory Realm Configuration User Download	
Download users and groups Begin automatic download at 12 V AM V America Download Now	a/New York Repeat Every 24 🕶 Hours
Available Groups C	Groups to Include (5)
 Search by name Terminal Server License Servers Access Control Assistance Operators Cryptographic Operators Network Configuration Operators 	Administrators Administrators Solutions S

Zertifikate für Admin und pxGrid

Internal CAs

Obwohl dies nicht erforderlich ist, empfiehlt es sich, CSR für den Administratorzugriff zu erstellen. Signieren Sie diese CSR-Anfrage mit vertrauenswürdigem AD, und importieren Sie das signierte Zertifikat zurück, wie in diesem Bild gezeigt:

Overview Analysis Policies D	evices Objects AMP											Deploy	S	<mark>/stem</mark> Help ▼	admin 🔻
							Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
												Generate Ne	w CSR	Import HTTPS (Certificate
Information	Current UTTOC Cost	10													
HTTPS Certificate	Current HTTPS Cert	incate													
External Database Access	Subject	commonName firepower.example.com	countryName PL	localityName Krakow	organizationName TAC	organizationalUnitName AAA	stateOrProvinceName Krakow								
Database Management Interfaces	Issuer	commonName	domainComponent												
Process		example-win-CA	example												
Remote Storage Device	Validity	Not Before Nov 29 12:23:55 2015 GMT	Not After Nov 28 12:23:55 20:	L6 GMT											
Change Reconciliation	Version	02													
Access Control Preferences	Serial Number	1700000008D385AAF7D2097	'EAE000000000008												
Access List	Signature Algorithm	sha1WithRS&Encryption													
Audit Log	orginator o regoritaria	Short in a manual point													
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															
Time Synchronization															
Shell Timeout															
Vulnerability Mapping															
VMware Tools															

Zertifizierungsstellenzertifikat muss einem vertrauenswürdigen Speicher hinzugefügt werden:

		and Trusted Dishiss	
Network	Name	AMP for Network Status Value A frepower.example.com - Cannot connect to	
Port Security Zones	VeriSign Class 3 Public Primary Certification Authority - G5	CN=VeriSign Class 3 Public Primary Certification Authority - GS, ORG=VeriSign, Inc., OU=(c) 2006 VeriSign, Inc For authorized use only c=03	~
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	/ 8
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	/ 🗊
Seolocation	Visa eCommerce Root	CN=VIsa eCommerce Root, ORG=VISA, OU=Visa International Service Association, C=US	/ 8
\$ Variable Set	Visa Information Delivery Root CA	CNVisa Information Delivery Root CA, ORG-VISA, OUVisa International Service Association, CUS	/ 🗊
Network Lists and Feeds	VRK Gov. Root CA	CN=VRK Gov. Root CA, ORG=Vaestorekisterikeskus CA, OU=Varmennepalvelut, C=FI	0
DNS Lists and Feeds	Wells Fargo Root Certificate Authority	CN=Weils Farge Root Certificate Authority, ORG=Weils Fargo, OU=Weils Fargo Certification Authority, C=US	/ 8
Sinkhole	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
Conner Suite List Distinguished Name	XRamp Global Certification Authority	CN=XRamp Global Certification Authority, ORG=XRamp Security Services Inc, OU=www.xrampsecurity.com, C=US	/ 0
🖽 Individual Objects Constant of the second secon			

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):

Overview Analysis Po	licie	s Devices Objects	АМР		
Object Management Ir	ntrus	ion Rules			
Network	Â	Name		Value	
J ^e Port	ш	pxgrid		CN=firepower.example.com, ORG=TAC, OU=pxgrid, C=PL	
Application Filters	ш				
S VLAN Tag	ш				
URL	ш			Add Known Internal Certificate	? ×
Geolocation	ш			Name: pxgrid	
\$ Variable Set	ш				
Security Intelligence				Certificate Data or, choose a file: Browse	
DNS Lists and Feeds	15			AwICAgCAMA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMCBzAKBggqhkiG9w0DBzANBgkq hkiG9w0BAQUFAAQCAQEASQbDPQ4nTYpH5Cbwz1nusKooPlUeYfHAJZU7TrgWb1WV	Â
URL Lists and Feeds	ш			XeJET3TrUj3ao9mu+t9jn4yoLC/+qygMl8U2lzb2bhLaxu336/oXGLy/A8S39gnh	
Sinkhole	ш			PZmDel5KfWLldWgyl4LgojlEtjiNgnd5XVHfkZdsgT1eV697dQLHRp+ff5BulYXu	
File List	ш			T8A1m694XbOG4a2GYVf9Jfgfrm1ctTa7ed6yB4oFc9bM8Nb60pxc5H/7r0TjDyuB OgnHOPnvdUIPd//En+dYWp3I/XoHMv4mR6br9fz6g==	
🔅 Cipher Suite List	ш			END CERTIFICATE)
Distinguished Name	ш				
Object Groups	ш			key or, choose a file:	•
⊿ <i>≫</i> PKI	ш			tHX8NilQM+NBUAtcEIUbVb78tkKNuPy5UT5KSBQ4i6E97z53haL4ISyqJYyTiRQa G5OqjWiMD085sUvCayzQh40QhpZf/cECggEAAUZ7CpeuUSdLIDSfKmlkTAbgbykN	
Internal CAs	ш			tGthr/T2p8/8++qF0F0mC+Gsq7PkaR1WLH/HFcFUMwP41Xd2WkiITNamVjopMZ80 0n//8oo/MNe460Kr1ZuToUWt9fD01JivzwTcTnIvZ5DSoXFmIwX2Tu6mSXWq6vcL	
Trusted CAs	ш			7/Ep6UdGhkJTdyU0FsJHT5W3dmnFkWerBS5Cw+eWqCOQacObx0tB5OpwDzw5PQ/G	
External Certs	ш			5VwssCFK0O4DVJhidH6jRqA3VFgvWL/psTUbWknMF8drv8lx4SF1dU4qoA==	
Internal Certs				END RSA PRIVATE KEY	\sim
Trusted CA Groups				Engranted and the parameter in .	
Internal Cert Groups				Chicrypted, and the password is:	
External Cert Groups				Save	Cancel

ISE-Integration

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

Overview Analysis Policies	Devices Objects A	MP		
Cisco CSI Realms Ident	ity Sources eStreamer	Host Input	Client	Smart Software Satellite
Identity Courses				
Identity Sources				_
Service Type	None Identity Servic	es Engine	User Agent	t
Primary Host Name/IP Address *	lise20.example.com			
Secondary Host Name/IP Address				
pxGrid Server CA *	Win2012	¥	0	
MNT Server CA *	Win2012	¥	0	
MC Server Certificate *	pxgrid	Y	•	
ISE Network Filter			ex. 10.8	9.31.0/24, 192.168.8.0/24,
			1	
* Required Field	Status	5		
		ISE connection	status:	
	4	Primary host: S	Success	
				OK I

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:

Overvi	Overview Analysis Policies Devices Objects AMP												
Access	Control + Identity	Network Discovery	Application Detectors	Correlation	Actions 🔻								
ISEP(Enter a d	escription												
Rules	Active Authentication												
											Add Category	Add Rule	
#	Name		Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Src Ports	Dest Ports	Realm	Action		
Administ	rator Rules												
This categ	tory is empty												
Standard	Rules												
1	Rule-AD		any	any	any	any	any	any	any	AD-Realm	Passive A	Authentication	
Root Rule	15												
This categ	ory is empty												

Zugriffskontrollrichtlinie

Für dieses Beispiel wurde die benutzerdefinierte URL erstellt:

Overview Analysis Policie	es Devices Objects AMP	
Object Management Intru	usion Rules	
Network	Name	Value
Port	Name	Value
Security Zones	attack-url	attack-url
Application Filters		
📎 VLAN Tag	Edit URL Objects ? ×	
WRL	Nama	
Seolocation	attack-uri	
💲 Variable Set	Description:	
Security Intelligence		
Network Lists and Feeds		
DNS Lists and Feeds	URL: attack-url	
URL Lists and Feeds	Allow Overrides:	
Sinkhole	Save Garcel 1	
List		

Die beiden Regeln in der benutzerdefinierten Zugriffskontrollrichtlinie:

Overv	iew Analysis Polici	es Devices Objec	ts AMP										System Hel	p v ad	imin 🔻
Acces	s Control + Access Cont	rol Network Discove	ery Application Det	ectors Correlation	Actions 🔻										
Cust Enter a	CustomPolicy														
Rules	Ittly Policy SSL Policy: None Ittly Policy Security Intelligence Market Advanced														
册 Filt	ter by Device									0	Add Category 📀 Add	Rule Search Rules			X
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	U 🛯		
👻 Ma	ndatory - CustomPolicy (1														
1	PermitPrivileged-HTTP	any	any	any	any	any	🝰 AD-Realm/Administra	st 🛅 HTTP	any	any	attack-url	🖋 Allow	V 🗅 🛛	0	0
2	DenyUnprivileged-HTTP	any	any	any	any	any	any	П НТТР	any	any	attack-url	💢 Block with reset	U 🗅 🖡	0	J
🔻 De	fault - CustomPolicy (-)														
There	are no rules in this section.	Add Rule or Add Category													
Defau	It Action										Access Control: Trust All	Traffic			× 🗌

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:

Overview Analysis Polic	ties Devices Ob										admin 🔻
Access Control > Access Con	trol Network Disc	overy Applicati	ion Detectors Correlation Actions •								
CustomPolicy										Save (Cancel
Identity Policy: ISEPolicy Rules Security Intelligence	SSL Policy: M	Advanced							Inheritance Setting	is 🖳 Policy Assign	nments (1)
B Filter by Device			Editing Rule - PermitPrivileged-HTTP				? × .	Add Category 🕓 Add	Rule Search Rules		×
# Name	Source Zones	Dest Zones	Name PermitPrivileged-HTTP	Enabled	Move			URLs	Action		
➡ Mandatory - CustomPolicy (Action 🖋 Allow	✓ IPS: no policies Variables: n/a File	es: no inspection Logging:	connections: Event Viewer					
1 PermitPrivileged-HTTP			Zones Networks VLAN Tags Users	Applications Ports URLs ISE A	lttributes	Inspection Logging Comm	ents	attack-url	Allow	U 🗅 🖉 •	6
2 DenyUnprivileged-HTTP			Available ISE Session Attributes	Available ISE Metadata 🗯	s	Selected Source ISE Metadata (1)		attack-url	X Block with rese	00000	68
➡ Default - CustomPolicy (-)			Search by name or value	Search by name or value		Auditors	6				
There are no rules in this section.	Add Rule or Add Catego	vγ	🚅 Security Group Tag	🚅 ANY	Â		- 11				
Default Action			Sa Device type	Auditors			- 11	Access Control: Trust All	Traffic		× 1
			Decation IP	BYOD			- 11				
				Contractors Developers	Add to Rule		- 11				
				Development Servers			- 11				
				Employees			- 11				
				- Guests			- 11				
				Potwork_Services							
				PCI_Servers	v	Add a Location IP Address	Add				
						011					

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

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

Überprüfen

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

vices Engine	Home • O	perations Po	licy I Gues	Access - Ac	Iministration	Work Centers	
ty Management 🔹 🕨	Network Resour	ces I Device Po	rtal Managemen	t pxGrid Servic	es Feed S	ervice 🔹 Identity Mappi	ng
Live Log							
le 🕜 Approve 🧉	Group 🛛 👎 De	line 🔞 Delete	🖌 🍕 Refresh	Total Pending A	pproval(0) 👻		
	Client Descrip	tion	Capabilities		Status		Client Group(s)
e20			Capabilities	(4 Pub, 2 Sub)	Online		Administrator
D			Capabilities	(2 Pub, 1 Sub)	Online		Administrator
ower.example.co			Capabilities	(0 Pub, 3 Sub)	Online		Session
st-firepower.exampl			Capabilities	(0 Pub, 0 Sub)	Offline		Session
ii F	vices Engine ity Management Live Log ble Approve se20 co power.example.co st-firepower.exampl	vices Engine Home Op ity Management Network Resourd Live Log ble Approve Group Dec Client Descrip se20 20 power.example.co st-firepower.exampl	vices Engine Home > Operations > Po ity Management > Network Resources > Device Po Live Log ble ⓒ Approve ⓒ Group ♥ Decline ⓒ Delete ♥ Client Description se20 20 power.example.co st-firepower.exampl	vices Engine Home > Operations > Policy → Guess ity Management > Network Resources > Device Portal Management Live Log ble ⓒ Approve @ Group ♥ Decline ⓒ Delete ♥ 餐 Refresh Client Description Capabilities ee20 Capabilities se20 Capabilities se20 Capabilities se30 Capabilities se40 Capabilities	vices Engine Home Operations Policy Guest Access Additional and the policy ity Management Network Resources Device Portal Management pxGrid Service Live Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log Itive Log	vices Engine Home Operations Policy Guest Access Administration ity Management Network Resources Device Portal Management pxGrid Services Feed Services Live Log ble Group Decline Device Portal Management Total Pending Approval(0) + client Description Capabilities Status client Description Capabilities(2 Pub, 1 Sub) Online cover,example.co Capabilities(0 Pub, 3 Sub) Online st-frepower,exampl Capabilities(0 Pub, 0 Sub) Offline	vices Engine Home Operations Policy Guest Access Administration Work Centers Itive Log Live Log Client Description Client Description Capabilities(4 Pub, 2 Sub) Online

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

cisco Ide	ntity Services Engine	Home	Operation:	s Policy	In Guest A	ccess	▼ Admin	istration	♦ Wor	k Cent
 System 	 Identity Management 	Network F	Resources •	Device Portal M	lanagement	pxGrid	Services	In Feed €	Service	▶ lde

Clients Live Log	iseagent-firepower.example.com-0739edea820cc77e04cc7c44200f661e										
S Clear Logs S Resync S Refresh											
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								

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:

Scisco AnyConnect Secure Mobility Client ((beta)				
ululu AnyConnec	t Secure Mobi	lity Client		0	
Status Overview	Virtual Private Network	k (VPN)			
VPN >	Preferences Statistics Route	e Details Firewall Mess	age History		
Network	Connection Information		🔇 Cisco AnyCo	nnect Secure Mobility Client	
	State: Tunnel Mode (IPv4): Tunnel Mode (IPv6): Duration: Address Information Client (IPv4):	Connected Tunnel All Traffic Drop All Traffic 00:00:34	00:00:34	VPN: Connected to 172.16.32.100. San Jose - SSL	Disconnect IPv4
	Client (IPv6): Server: Bytes	Not Available 172.16.32.100	Ľ	Network: Connected (192, 168, 10, 67)	
	Sent: Received:	20791 20120	-	wired	کې 🗕 📰
Collect diagnostic information for all installed components.	Frames		‡ 🗊		altaba cisco
Diagnostics					

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
```

:

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:

cisco Identity Se	rvices Engine	Home	▼Operations	▶ Policy	▶ Guest Access	 Administration 	Work Cent	ers			
RADIUS Livelog	TACACS Livelog	Reports	Troubleshoot	Adaptive	Network Control						
Misconfigured Supplicants ① O				Misconfigured Network Devices ${}^{(i)}$ ${f 0}$			RADIUS	Client Stopped Res O			
💼 Show Live Ses	sions 🙀 Add or	Remove Co	lumns 🔻 🛞 Refr	resh 🕐 Re	set Repeat Counts						Refresh
Time	▼ Status All ▼ De	t Repe	at C		uthentication Policy	Auth	orization Policy	Authorization Profiles (Network Device	Server 0	Event ()
2015-12-01 23:3	7:31 🕕	ò	0 Adminis	trator De	efault >> Default >>	> Default Defa	ult >> ASA VPN	PermitAccess,Auditors		lise20	Session State is Started
2015-12-01 23:3	7:26 🔽	ò	Adminis	trator De	efault >> Default >>	> Default Defa	ult >> ASA VPN	PermitAccess,Auditors	ASA	lise20	Authentication succeeded
2015-12-01 23:3	5:19 🗹	Q	Adminis	trator De	efault >> Default >>	> Default Defa	ult >> 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):

🔼 Ci	isco AnyConr	ect VPN Virte	ial Miniport A	dapter for V	Vindows x64	4: \Device	\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> aptu	re <u>A</u> nalyze	<u>S</u> tatistics	Telephony	<u>T</u> ools	Internals <u>H</u> elp
	1 0 0	X E	🖥 🗶 🔁		🗢 🔿	n 🗘	보 🗐 🗐 오. Q. 🔍 🎬 🗹 🥵 🔆 💢
Filter	:						Expression Clear Apply Save
No.	Source		Destin	ation		Protocol	Length Info
	1 172.16	.50.50	192.	168.10.1	.51	тср	66 59916 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1346 WS=4 SACK_PERM=1
	2 172.16	.50.50	172.	16.34.10)0	тср	66 59917 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1346 WS=4 SACK_PERM=1
	3 172.16	.34.100	172.	16.50.50)	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.	16.34.10)0	тср	54 59917 > http [ACK] Seq=1 Ack=1 Win=65952 Len=0
	5 172.16	.50.50	172.	16.34.10	00	HTTP	588 GET /attack-url HTTP/1.1
	6 172 16	24 100	170	1 C EO EC	`		and the second from the second of the second second
	01/2.10	. 54.100	172.	10.30.30	,	TCP	54 http > 59917 [RST, ACK] Seq=1 Ack=535 Win=0 Len=0
🗄 Fr	ame 5: 58	8 bytes	on wire (4704 bit	s), 588	bytes	54 http > 5991/ [RST, ACK] Seq=1 ACK=535 Win=0 Len=0 captured (4704 bits) on interface 0
Fr Et	ame 5: 58	8 bytes , Src: C	on wire (isco_3c:7	4704 bit a:00 (00	s), 588):05:9a:	bytes Bc:7a:0	54 http > 5991/ [RST, ACK] Seq=1 ACK=535 Win=0 Len=0 captured (4704 bits) on interface 0 00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
	ame 5: 58 hernet II	8 bytes , src: C otocol V	on wire (isco_3c:7 ersion 4,	4704 bit a:00 (00 src: 17	s), 588 1:05:9a: 2.16.50	bytes 3c:7a:0 .50 (17	<pre>>4 http > Sy91/ [RST, ACK] Seq=1 ACK=SSS win=0 Len=0 captured (4704 bits) on interface 0 >00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) '2:16.50.50), Dst: 172.16.34.100 (172.16.34.100)</pre>
	ame 5: 58 hernet II nternet Pr ansmissio	8 bytes 5, Src: C otocol V on Contro	on wire (isco_3c:7 ersion 4, l Protoco	4704 bit a:00 (00 src: 17 l, src P	(5), 588 (105:9a) (2.16.50 (0rt: 59)	bytes 3c:7a:0 .50 (17 917 (59	34 http > 3991/ [RST, ACK] Seq=1 ACK=535 Win=0 Len=0 captured (4704 bits) on interface 0 00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) ?2:16.50.50), Dst: 172.16.34.100 (172.16.34.100) 9917), Dst Port: http (80), Seq: 1, Ack: 1, Len: 534
 ➡ Fr ➡ Et ➡ In ➡ Tr ➡ Hy 	ame 5: 58 hernet II nternet Pr ansmissio pertext 1	8 bytes , Src: C otocol V on Contro ransfer	on wire (isco_3c:7 ersion 4, l Protoco Protocol	4704 bit a:00 (00 Src: 17 l, Src P	s), 588 1:05:9a: 2.16.50 Port: 59	bytes 3c:7a:0 .50 (17 917 (59	34 http > 3991/ [RST, ACK] Seq=1 ACK=535 Win=0 Len=0 captured (4704 bits) on interface 0 30), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 72.16.50.50), Dst: 172.16.34.100 (172.16.34.100) 39917), Dst Port: http (80), Seq: 1, Ack: 1, Len: 534
	ame 5: 58 hernet II iternet Pr ansmissic pertext 1 GET /atta	8 bytes 5, Src: C otocol V on Contro Transfer ack-url H	Dn wire (isco_3c:7 ersion 4, l Protoco Protocol FTP/1.1\r	4704 bit a:00 (00 Src: 17 l, src P \n	s), 588 :05:9a: 2.16.50 ort: 59	bytes 3c:7a:0 .50 (17 917 (59	S4 http > S991/ [RST, ACK] Seq=1 ACK=S3S Win=0 Len=0 captured (4704 bits) on interface 0 30), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 32:16.50.50), Dst: 172:16.34.100 (172:16.34.100) 3917), Dst Port: http (80), Seq: 1, Ack: 1, Len: 534
	ame 5: 58 hernet II iternet Pr ansmissic pertext 1 GET /atta Accept: a	88 bytes 5, Src: C 50tocol V 50n Contro 7ransfer 6ck-url H 6pplicati	n wire (isco_3c:7 ersion 4, Protoco Protocol TTP/1.1\r pn/x-ms-a	4704 bit a:00 (00 Src: 17 l, Src P \n pplicati	s), 588):05:9a: 2.16.50 Port: 59 on, ima	bytes 3c:7a:0 .50 (17 917 (59 ge/jpeg	<u>S4 http > S991/ [RST, ACK] Seq=1 ACk=S3S Win=0 Len=0</u> captured (4704 bits) on interface 0 00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 22:16.50.50), Dst: 172.16.34.100 (172.16.34.100) 3917), Dst Port: http (80), seq: 1, Ack: 1, Len: 534 9, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-
	ame 5: 58 thernet II ternet Pr ansmissic pertext 1 GET /atta Accept: a Accept-La	88 bytes 5, Src: C otocol V on Contro Transfer ack-url H application	pn wire (isco_3c:7 ersion 4, l Protoco protocol TTP/1.1\r pn/x-ms-a pl-PL\r\n	4704 bit a:00 (00 src: 17 l, src P \n pplicati	s), 588 9:05:9a: 2.16.50 Port: 59 on, imag	bytes 3c:7a:0 .50 (17 917 (59 ge/jpeg	<u>S4 http > S991/ [RST, ACK] Seq=1 ACK=S3S Win=0 Len=0</u> captured (4704 bits) on interface 0 00) Dst: Cimsys_33:44:55 (00:11:22:33:44:55) '2.16.50.50), Dst: 172.16.34.100 (172.16.34.100) 19917), Dst Port: http (80), Seq: 1, ACK: 1, Len: 534 g, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms-
<pre> Fr Et Fr Fr</pre>	ame 5: 58 chernet II nternet Pr cansmissio (pertext 1 GET /atta Accept: a Accept-La User-Ager	8 bytes 5, Src: C Totocol V Transfer Tack-url H Applicati Unguage: T: Mozil	1/2. on wire (isco_3c:7 ersion 4, l Protocol Protocol FTP/1.1\r on/x-ms-a ol-PL\r\n la/4.0 (c	4704 bit a:00 (00 src: 17 l, src P \n pplicati	s), 588 2:05:9a: 2:16.50 Port: 59 on, ima e; MSIE	bytes 3c:7a:0 .50 (17 917 (59 ge/jpeg 8.0; w	<u>S4 http > S9917 [RST, ACK] Seq=1 ACK=S35 Win=0 Len=0</u> captured (4704 bits) on interface 0 D0) Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 72:16.50.50), Dst: 172.16.34.100 (172.16.34.100) D917), Dst Port: http (80), Seq: 1, Ack: 1, Len: 534 g, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms- vindows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLF
Fr + Et + In + Tr - Hy +	ame 5: 58 hernet II ternet Pr ansmissio pertext 1 GET /atta Accept-La User-Ager Accept-Er	8 bytes 5, Src: C otocol V on Contro Transfer ack-url H upplicati unguage: nt: Mozil acoding:	1/2. pn wire (isco_3c:7 ersion 4, l Protocol protocol TTP/1.1\r pn/x-ms-a pl-PL\r\n la/4.0 (c gzip, def	4704 bit a:00 (00 src: 17 l, src P \n pplicati ompatibl late\r\r	s), 588 2:05:9a: 2:16.50 Port: 59 on, ima e; MSIE	bytes 3c:7a:0 .50 (17 917 (59 ge/jpeg 8.0; w	<u>S4 http > S991/ [RST, ACK] Seq=1 ACK=S35 Win=0 Len=0</u> captured (4704 bits) on interface 0 00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 22:16.50.50), Dst: 172.16.34.100 (172.16.34.100) 9917), Dst Port: http (80), seq: 1, Ack: 1, Len: 534 g, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms- vindows NT 6.1; w0w64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLF
Fr Et In Tr Hy W	ame 5: 58 thernet II tternet Pr ansmissic pertext I GET /atta Accept-La User-Ager Host: 172	8 bytes 5, Src: C otocol V on Contro ransfer ack-url H applicati inguage: it: Mozil acoding: 2.16.34.1	1/2. on wire (isco_3c:7 ersion 4, l Protocol protocol TTP/1.1\r pon/x-ms-a ol-PL\r\n la/4.0 (c gzip, def 00\r\n	4704 bit a:00 (00 src: 17 l, src P \n pplicati late\r\r	s), 588 9:05:9a: 2.16.50 Port: 59 on, ima e; MSIE	bytes 3c:7a:0 .50 (17 917 (59 ge/jpeg 8.0; W	<u>S4 http > S991/ [RST, ACK] Seq=1 ACK=S35 Win=0 Len=0</u> captured (4704 bits) on interface 0 00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 22:16.50.50), Dst: 172.16.34.100 (172.16.34.100) 0917), Dst Port: http (80), seq: 1, Ack: 1, Len: 534 g, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms- vindows NT 6.1; wow64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLF
<pre></pre>	ame 5: 58 thernet II ternet Pr ansmissio pertext 1 GET /atta Accept: a Accept-La User-Ager Accept-Er Host: 172 Connectio	<pre>by the second seco</pre>	1/2. on wire (isco_3c:7 ersion 4, l Protocol Protocol Protocol TTP/1.1\r on/x-ms-a ol-PL\r\n la/4.0 (cc gzip, def O0\r\n Alive\r\n	4704 bit a:00 (00 src: 17 l, src F \n pplicati late\r\r	s), 588 9:05:9a: 2.16.50 Port: 59 on, ima e; MSIE	bytes 3c:7a:0 .50 (17 917 (59 ge/jpeg 8.0; w	<u>S4 http > S9917 [RST, ACK] Seq=1 ACK=S3S Win=0 Len=0</u> captured (4704 bits) on interface 0 D0), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 22.16.50.50), Dst: 172.16.34.100 (172.16.34.100) D917), Dst Port: http (80), Seq: 1, ACK: 1, Len: 534 g, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms- vindows NT 6.1; w0w64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLF
Fr ⊕ Et ⊕ In ⊕ Tr Hy ⊕	ame 5: 58 hernet II ternet Pr ansmissic ypertext 1 GET /atta Accept - La User - Ager Accept - Er Host: 172 Connectic \r\n	8 bytes 5, Src: C otocol v on Contro ransfer tck-url H upplicati unguage: nt: Mozil coding: 2.16.34.1 on: Keep-	1/2. on wire (isco_3c:7 ersion 4, l Protoco Protocol TTP/1.1\T on/x-ms-a ol-PL\T\n la/4.0 (c gzip, def 00\r\n alive\r\n	4704 bit a:00 (00 src: 17 l, src P \n pplicati ompatibl late\r\r	s), 588 205:9a: 22.16.50 Port: 59 on, ima e; MSIE	bytes 3c:7a:0 .50 (17 917 (59 ge/jpeg 8.0; W	<u>S4 http > S9917 [RST, ACK] Seq=1 ACK=S35 Win=0 Len=0</u> captured (4704 bits) on interface 0 00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55) 22:16.50.50), Dst: 172.16.34.100 (172.16.34.100) 9917), Dst Port: http (80), seq: 1, Ack: 1, Len: 534 g, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, application/vnd.ms- vindows NT 6.1; wow64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLF

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-T	unnel								
License	: AnyConnect Essentials										
Encryption	: AnyConnect-Parent: (1):	none SSL-Tun	nel: (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 :
VLAN Mapping : N/A
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:

cisco Identity Se	ervices Engine	Home	▼Operations	Policy	Guest Access	Administration	Work Cent	ers			
RADIUS Livelog	TACACS Livelog	Reports	Troubleshoot	Adaptive	Network Control						
Misconfigured Supplicants (2)					Misconfigured Network Devices $@$ 0			RADIUS 27	Client Stopped Res O		
🗂 Show Live Se	ssions 🙀 Add or	Remove Co	lumns 👻 🛞 Refr	resh 💿 Re	eset Repeat Counts						Refresh
Time	▼ Status All ▼ De	et Repe	at C		uthentication Policy	Auth	orization Policy	Authorization Profiles	Network Device	Server ①	Event ()
2015-12-01 23:3	7:31 🍈	0	0 Adminis	trator De	efault >> Default >>	Default Defa	ult >> ASA VPN	PermitAccess,Auditors		lise20	Session State is Started
2015-12-01 23:3	7:26 🔽	0	Adminis	trator De	efault >> Default >>	Default Defa	ult >> ASA VPN	PermitAccess,Auditors	ASA	lise20	Authentication succeeded
2015-12-01 23:3	6:19 🔽	ò	Adminis	trator De	efault >> Default >>	Default Defa	ult >> ASA VPN	PermitAccess	ASA	lise20	Authentication succeeded

Der Benutzer kann auf den genannten Service zugreifen:

http://172.16.34.100/attack-url - Windows Internet Explorer									
@ •	http://172.16.3	34.100/a	ttack-url						
File Edit	View Favorites	Tools	Help						
🚖 Favorites	🏉 http://172.3	16.34.100	0/attack-url						
succeeded									

Zugriff auf FMC-Protokollierung

Diese Aktivität kann im Connection Event-Bericht bestätigt werden:

Overview Analysis Polic	ies Devices (Objects AMP										Deploy A	System Help 🔻	admin 🔻
Context Explorer Connection	ons ► Events	Intrusions File	es ▼ Hosts ▼ Users ▼	Vulnerabilities • 0	Correlation Cu	ustom Searc	ch							
										Bookmark Thi	s Page Report De	signer Dashboard	View Bookmarks	Search 🔻
Connection Events	(switch workflow)													
					Info		×							
					Deleted 9 0	Connection(s)								
Connections with Application Details	> Table View of C	Connection Events										2015-12-01 21:24	:00 - 2015-12-01 2	3:46:59
													E	cpanding
 Search Constraints (Edit Search) 	save Search)												Disable	ea Columns
Jump to 🔻														
→ Last Packet ×	Action ×	Initiator IP ×	Initiator User ×	Responder × IP	Ingress Security Zone	× Application Protocol	Access Control Policy	× Access Control × Rule	Security × Group Tag	Ingress X Interface	<u>NetBIOS</u> × <u>Domain</u>	Initiator × Packets	Initiator × Bytes	Count
J 2015-12-01 23:38:1	9 Allow	i <u>172.16.50.50</u>	AD-Realm\administrator (LDA	P) 📑 <u>172.16.34.100</u>	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors e	eth1		10	<u>1,680</u>	1
♣2015-12-01_23:38:0	5 <u>Allow</u>	172.16.50.50	AD-Realm\administrator (LDA	P) 🐖 <u>172.16.34.100</u>	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	<u>Auditors</u>	eth1		<u>12</u>	<u>1.512</u>	1
J 2015-12-01 23:26:1	<u>B</u> <u>Allow</u>	172.16.50.50	AD-Realm\administrator (LDA	P) 📑 <u>172.16.34.100</u>	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors	eth1		<u>8</u>	<u>1,312</u>	1
J <u>2015-12-01-23:25:1</u>	1 Allow	i <u>172.16.50.50</u>	AD-Realm\administrator (LDA	P) 🛒 <u>172.16.34.100</u>	Internal	HTTP	CustomPolicy	PermitPrivileged-HTTP	Auditors	eth1		22	3,752	1
¥ 🔲	Block with reset	172.16.50.50	AD-Realm\administrator (LDA	P) 🖷 172.16.34.100	Internal	HTTP	CustomPolicy	DenyUnprivileged-HTTP	5	eth1		25	3,938	5
$ \langle \langle Page \ 1 \ of \ 1 \rangle \rangle $ Displa	ying rows 1-5 of 5 r	rows												
View Delete														
View All Delete All														

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.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 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-Abfrace über pyGrid

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 returns [OK] 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: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:taq>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-11e5-978e-005056bf2f0a</ns5:id><ns5:name>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:description>Point_of_Sale_Systems</ns5:name><ns5:name><ns5:name><ns 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: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:

) 🛞 file:///tmp/x.xml

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</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>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E 6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceAgmtIntfID></deviceAttachPt</pre> ></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>UGVybWl0QWNjZXNzLEF1ZGl0b3Jz</attribute></extraAt tributes><state>Started</state><RADIUSAttrs><attrName>Acct-Session-Id</attrName><attrValue>91200007</attrValue></RADIUSAttrs><interface><ipIntfID><ipAddress xmlns='http://www.cisco.com/pxgrid'>172.16.50.50</ipAddress></ipIntfID><macAddress>08:00:27:23:E 6:F2</macAddress><deviceAttachPt><deviceMgmtIntfID><ipAddress xmlns='http://www.cisco.com/pxgrid'>172.16.31.100</ipAddress></deviceAgmtIntfID></deviceAttachPt</pre> ></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>

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.
XgridDaoImp1 -::::- 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.
XgridDaoImp1 -::::- 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
- <u>Administratoranleitung für Cisco Identity Services Engine, Version 2.0</u>
- 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