Integração ISE e de FirePOWER - exemplo do serviço da remediação

Índice

Introdução Pré-requisitos Requisitos **Componentes Utilizados** Configurar Diagrama de Rede **FirePOWER** Centro de gerenciamento de FireSIGHT (centro da defesa) Política do controle de acesso Módulo da remediação ISE Política da correlação **ASA** ISE Configurar o dispositivo do acesso de rede (o NAD) Permita o controle de rede adaptável **Quarantine DACL** Perfil da autorização para a quarentena Regras da autorização Verificar AnyConnect inicia a sessão de VPN ASA O usuário tenta o acesso Batida da política da correlação de FireSIGHT O ISE executa a guarentena e envia o CoA A sessão de VPN é desligada Sessão de VPN com acesso limitado (guarentena) Troubleshooting FireSIGHT (centro da defesa) ISE Erros Informações Relacionadas Cisco relacionado apoia discussões da comunidade

Introdução

Este documento descreve como usar o módulo da remediação em um dispositivo de Cisco FireSIGHT a fim detectar ataques e automaticamente remediate o atacante com o uso do motor do serviço da identidade de Cisco (ISE) como um servidor da política. O exemplo que é fornecido neste documento descreve-o o método que é usado para a remediação de um usuário remoto VPN que autentique através do ISE, mas pode igualmente ser usado para um 802.1x/MAB/WebAuth prendido ou o usuário Wireless.

Note: O módulo da remediação que é provido neste documento não é apoiado oficialmente por Cisco. É compartilhado em um portal da comunidade e pode ser usado por qualquer um. Nas versões 5.4 e mais recente, há igualmente um módulo mais novo da remediação disponível que seja baseado no protocolo do *pxGrid*. Este módulo não é apoiado na versão 6.0 mas é planejado ser apoiado nas versões futuras.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN adaptável da ferramenta de segurança de Cisco (ASA)
- Configuração de Cliente de mobilidade Cisco AnyConnect Secure
- Configuração básica de Cisco FireSIGHT
- Configuração básica de Cisco FirePOWER
- Configuração de Cisco ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Versão ASA 9.3 de Cisco ou mais atrasado
- Versões de software 1.3 de Cisco ISE e mais atrasado
- Versões 3.0 e mais recente do Cliente de mobilidade Cisco AnyConnect Secure
- Versão 5.4 do centro de gerenciamento de Cisco FireSIGHT
- Versão 5.4 de Cisco FirePOWER (máquina virtual (VM))

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Use a informação que é fornecida nesta seção a fim configurar seu sistema.

Note: Use a <u>Command Lookup Tool</u> (<u>somente clientes registrados</u>) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

O exemplo que é descrito neste documento usa esta instalação de rede:



172.16.31.206

Está aqui o fluxo para esta instalação de rede:

- 1. O usuário inicia uma sessão de VPN remota com o ASA (através da versão 4.0 segura da mobilidade de Cisco AnyConnect).
- 2. O usuário tenta alcançar *http://172.16.32.1*. (O tráfego se move através de FirePOWER, que é instalado no VM e controlado por FireSIGHT.)
- 3. FirePOWER é configurado de modo que obstrua que (inline) o tráfego específico (políticas

de acesso), mas ele igualmente tem uma política da correlação que seja provocada. Em consequência, inicia a remediação ISE através da interface de programação de aplicativo do RESTO (API) (o método de *QuarantineByIP*).

- 4. Uma vez que o ISE recebe o atendimento do RESTO API, olha acima para a sessão e envia uma mudança do RAIO da autorização (CoA) ao ASA, que termina essa sessão.
- 5. O ASA desliga o usuário VPN. Desde que AnyConnect é configurado com Sempre-em acesso VPN, uma sessão nova é estabelecida; contudo, esta vez uma regra diferente da autorização ISE é combinada (para anfitriões quarantined) e o acesso de rede limitado é fornecido. Nesta fase, não importa como o usuário conecta e autentica à rede; enquanto o ISE é usado para a authentication e autorização, o usuário limitou o acesso de rede devendo quarantine.

Como mencionado previamente, esta encenação trabalha para qualquer tipo da sessão autenticada (VPN, 802.1x/MAB/Webauth prendido, Sem fio 802.1x/MAB/Webauth) enquanto o ISE é usado para a autenticação e os suportes do dispositivo do acesso de rede o CoA do RAIO (todos os dispositivos Cisco modernos).

Tip: A fim mover o usuário fora da quarentena, você pode usar o ISE GUI. As versões futuras do módulo da remediação puderam igualmente apoiá-lo.

FirePOWER

Note: Um dispositivo VM é usado para o exemplo que é descrito neste documento. Somente a configuração inicial é executada através do CLI. Todas as políticas são configuradas do centro da defesa de Cisco. Para mais detalhes, refira a <u>seção Informação Relacionada</u> <u>d</u>este documento.

O VM tem três relações, uma para o Gerenciamento e dois para a inspeção inline (interno/externo).

Todo o tráfego dos usuários VPN move-se através de FirePOWER.

Centro de gerenciamento de FireSIGHT (centro da defesa)

Política do controle de acesso

Depois que você instala as licenças corretas e adiciona o dispositivo de FirePOWER, navegue às **políticas > ao controle de acesso** e crie a política de acesso que é usada a fim deixar cair o tráfego de HTTP a 172.16.32.1:

Overview Analysis Polic	Devices Ob	ects AMP									😔 Heath – Sy	stem Help	v ad	nin v
Access Control Intrusion	Files Network	k Discovery SSL	Application Deb	ectors Users	Correlation Ac	ttipes =								
AccessPolicy	AccessPolicy													
Rulas Targets (1) Securit	Targets (1) Security Intelligence HTTP Responses Advanced													
🏥 Filer by Derice									Q AH CI	legery 🤤 Add Rate	Search Rales			×
e Name	Searce Zenes	Deat Zones	Searce Networks	Deal Natworks	VLAN Tage	Users	Applications	See Parts	Deat Parts	URL	Action			
Astenia intrator Balas														
This category is empty														
Standard Rales														
1 Dropf/DR0	40y	any	any .	# 172.16.32.1	WV.	101	any .	any.	P BITP	102	💢 Black	0.01	3 D	/ 8
Roat Rules														
We category a empty														
Defeall Adam									Brirvalure	Prevention: Datascent Deca	By and Carried	vily		

Todo tráfego restante é aceitado.

Módulo da remediação ISE

A versão atual do módulo ISE que é compartilhado no portal da comunidade é a *remediação beta 1.3.19 ISE 1.2*:



This community supported remediation module allows for the automated interaction with Cisco Identity Services Engine (ISE) version 1.2. This interaction performs a quarantine of the desired IP (Source or Destination) based on the user configuration of the remediation. This quarantine action can be triggered by any event that occurs on the Sourcefre Defense Center that contains a source or destination IP address.

Navegue às políticas > às ações > às remediações > aos módulos e instale o arquivo:

Overview Analysis Policies Devices Objects A	AMP			
Access Control Intrusion • Files Network Discovery	SSL Application Detecto	rs Users	Correlation	Actions + Modules
			Success	×
			Module succe	ssfully installed
Installed Remediation Modules				
Module Name	Version	Description		
Cisco IOS Null Route	1.0	Block an IP ad	dress in a Cisco IO	05 router
Cisco PIX Shun	1.1	Shun an IP ad	dress in the PIX fi	rewall
ISE 1.2 Remediation	1.3.19	Quarantine IP	addresses using I	dentity Services Engine 1.2
Nmap Remediation	2.0	Perform an Nr	nap Scan	
Set Attribute Value	1.0	Set an Attribut	te Value	

O exemplo correto deve então ser criado. Navegue às **políticas > às ações > às remediações > aos exemplos** e forneça o endereço IP de Um ou Mais Servidores Cisco ICM NT do nó da administração de política (BANDEJA), junto com as credenciais administrativas ISE que são precisadas para o RESTO API (um usuário separado com o papel *ERS Admin* é recomendado):

Edit Instance	
Instance Name	ise-instance
Module	ISE 1.2 Remediation (v1.3.19)
Description	
Primary Admin Node IP	172.16.31.202
Secondary Admin Node IP (optional)	
Username	admin
Password Retype to confirm	•••••
SYSLOG Logging	💿 On 🔵 Off
White List (an <i>optional</i> list of networks)	
	Create Cancel

O endereço IP de origem (atacante) deve igualmente ser usado para a remediação:

Configured Remediations								
Remediation Name	Remediation Type	Description						
No configured remediations available								
Add a new remediation of	type Quarantine Source IP	V Add						

Política da correlação

Você deve agora configurar uma regra específica da correlação. Esta regra é provocada no início da conexão que combina a regra previamente configurada do controle de acesso (*DropTCP80*). A fim configurar a regra, navegue às **políticas > ao Gerenciamento da correlação > da regra**:

Overview Analysis	Policies Devices	Objects AMP									
Access Control Intr	usion • Files Net	vork Discovery SSI	. Application D	etectors	Users	Correlation	Actions 🔻				
Policy Managemen	it Rule Managemer	t White List	Traffic Profiles								
Rule Information	I										
Rule Name	CorrelateTCP80Block										
Rule Description											
Rule Group	Ungrouped V										
Select the type o	Select the type of event for this rule										
If a connection eve	ent occurs 🗸 (at the begins	ning of the connection	~	and it meet	s the foll	owing condition	15:				
💿 Add	condition O Add com	plex condition									
X	cess Control Rule Name	✓ contains the strin	g 🗸 DropTCP80								
Rule Options											
Snooze	If this rule generates an	event, snooze for 0	hours 🗸								
Inactive Periods	There are no defined inac	tive periods. To add an i	nactive period, click	"Add Inactive	Period".						

Esta regra é usada na política da correlação. Navegue às **políticas > à correlação > ao Gerenciamento de políticas** a fim criar uma política nova, e adicionar então a regra configurada. Clique **Remediate** à direita e adicionar duas ações: **remediação para o sourceIP** (configurado mais cedo) e o **Syslog**:

Overview Analysis 💌	ficter Devices Objects AHP		💩 mactin - Sa	sten Telp 🔻	admin 1
Polics Henegement	Falls Paragement Write List Traffic Profiles	ALERX COTTINUEDON ACTOON *	2	ira kenedabo	a oraga
Correlation Policy Inf Policy Mane Policy Description	ermeditie in Constale onhibits			Ser.	<u>(1993)</u>
Outsuit Priority Policy Rulies	Part of			0.0	N RAIL
Correlate 762808004		avelae (Denag)		Delet w	* 0
		Responses for Examination Responses Assigned Responses Devoltance Responses Entry	1		
		Unassigned Responses			
		Update	Canal .		

Assegure-se de que você permita a política da correlação:



ASA

Um ASA que atue como um gateway de VPN é configurado a fim usar o ISE para a autenticação. É igualmente necessário permitir a contabilidade e o CoA do RAIO:

```
tunnel-group SSLVPN-FIRESIGHT general-attributes
address-pool POOL-VPN
authentication-server-group ISE
accounting-server-group ISE
default-group-policy POLICY
aaa-server ISE protocol radius
interim-accounting-update periodic 1
dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
key *****
webvpn
enable outside
enable inside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable
error-recovery disable
```

ISE

Configurar o dispositivo do acesso de rede (o NAD)

Navegue à **administração > aos dispositivos de rede** e adicionar o ASA que atua como um cliente RADIUS.

Permita o controle de rede adaptável

Navegue à **administração > ao sistema > aos ajustes > controle de rede adaptável** a fim permitir a quarentena API e a funcionalidade:



Note: Nas versões 1.3 e anterior, esta característica é chamada *serviço de proteção de Valor-limite*.

Quarentena DACL

A fim criar um Access Control List carregável (DACL) que é usado para os anfitriões quarantined, navegue à **política > aos resultados > à autorização > ACL baixável**.

Perfil da autorização para a quarentena

Navegue à **política > aos resultados > à autorização > ao perfil da autorização** e crie um perfil da autorização com o DACL novo:

cisco Identity Services Engine		🏠 Home	Operations 🔻	Policy 🔻	Guest Access
Authentication S Authorization	🔏 Profiling	💽 Posture	😡 Client Provi	sioning	📑 TrustSec
Dictionaries Conditions Results					
Results	Authorization Authorizat * N Descri * Access Service Tem	Profiles > Limited	Access Access	Ţ	
Client Provisioning	▼ Commor	n Tasks			
TrustSec	Z DACL N	ame	DE	NY_ALL_QUA	ARANTINE 🍷

Regras da autorização

Você deve criar duas regras da autorização. A primeira regra (ASA-VPN) fornece o acesso direto para todas as sessões de VPN que são terminadas no ASA. A regra *ASA-VPN_quarantine* está batida para a sessão de VPN reauthenticated quando o host está já na quarentena (o acesso de rede limitado está fornecido).

A fim criar estas regras, navegue à **política > à autorização**:

ahaha											
cisco Ide	ntity Services Engine		☆ Home	Operations 🔻	Policy	Guest Access		Iministration			
💄 Authentic	ation 🥑 Authorization	Read Profiling	Posture	👸 Client Provi	sioning	🚊 TrustSec	🔒 Po	licy Elements			
Authorization Policy											
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.											
For Poincy Export go to Administration > System > Dataup & Restore > Poincy Export Page											
First Matched	rirst Matchea Rule Applies *										
Exception:	s (0)										
Standard											
Status	Rule Name	Con	ditions (identity gro	ups and other cond	litions)			Permissions			
	ASA-VPN_quarantine	if (DEV	/ICE:Device Type E	QUALS All Device	Types#ASA-	VPN AND	then	LimitedAccess			
	ACA VDN	Sess	ion:EPSStatus EQ	JALS Quarantine)	Smer#ARA 1	(BN)	then	ParmitAccess			
E 🗹	ADA-VEN	DEV	ICE.Device Type E	QUALS All Device	урсэ#АЗА-У	1719		PerminAccess			

Verificar

Use a informação que é fornecida nesta seção a fim verificar que sua configuração trabalha corretamente.

AnyConnect inicia a sessão de VPN ASA

🕥 Cisco AnyCo	nnect Secure Mobility Client		
	VPN: Connected to 172.16.31.100. 172.16.31.100	Disco	onnect
00:00:09			IPv4
۞ (i)			altalta cisco

O ASA cria a sessão sem nenhum DACL (acesso de rede completo):

asav# show vpn-sessiondb details anyconnect

: cisco Index : 37 Username Assigned IP : 172.16.50.50 Public IP : 192.168.10.21 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Essentials Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Hashing Hashing : AnyCon Bytes Tx : 18706 Bytes Rx : 14619 Group Policy : POLICY Tunnel Group : SSLVPN-FIRESIGHT Login Time : 03:03:17 UTC Wed May 20 2015 Duration : 0h:01m:12s Inactivity : 0h:00m:00s : none VLAN Mapping : N/A VLAN Audt Sess ID : ac10206400025000555bf975 Security Grp : none DTLS-Tunnel: <some output omitted for clarity>

O usuário tenta o acesso

Uma vez que o usuário tenta alcançar http://172.16.32.1, a política de acesso está batida, o tráfego que corresponde é obstruído inline, e o mensagem do syslog é enviado do endereço IP de gerenciamento de FirePOWER:

May 24 09:38:05 172.16.31.205 SFIMS: [Primary Detection Engine (cbe45720-f0bf-11e4-a9f6-bc538df1390b)][AccessPolicy] Connection Type: Start, User: Unknown, Client: Unknown, Application Protocol: Unknown, Web App: Unknown, Access Control Rule Name: DropTCP80, Access Control Rule Action: Block, Access Control Rule Reasons: Unknown, URL Category: Unknown, URL Reputation: Risk unknown, URL: Unknown, Interface Ingress: eth1, Interface Egress: eth2, Security Zone Ingress: Internal, Security Zone Egress: External, Security Intelligence Matching IP: None, Security Intelligence Category: None, Client Version: (null), Number of File Events: 0, Number of IPS Events: 0, TCP Flags: 0x0, NetBIOS Domain: (null), Initiator Packets: 1, Responder Packets: 0, Initiator Bytes: 66, Responder Bytes: 0, Context: Unknown, SSL Rule Name: N/A, SSL Flow Status: N/A, SSL Subject CN: N/A, SSL Subject Country: N/A, SSL Subject OU: N/A, SSL Subject Org: N/A, SSL Issuer CN: N/A, SSL Issuer Country: N/A, SSL Issuer OU: N/A, SSL Issuer Org: N/A, SSL Valid Start Date: N/A, SSL Valid End Date: N/A, SSL Version: N/A, SSL Server Certificate Status: N/A, SSL Actual Action: N/A, SSL Expected Action: N/A, SSL Server Name: (null), SSL URL Category: N/A, SSL Session ID:

Batida da política da correlação de FireSIGHT

A política da correlação do Gerenciamento de FireSIGHT (centro da defesa) é batida, que é relatada pelo mensagem do syslog que é enviado do centro da defesa:

May 24 09:37:10 172.16.31.206 SFIMS: Correlation Event: CorrelateTCP80Block/CorrelationPolicy at Sun May 24 09:37:10 2015 UTCConnection Type: FireSIGHT 172.16.50.50:49415 (unknown) -> 172.16.32.1:80 (unknown) (tcp)

Nesta fase, o centro da defesa usa o atendimento do RESTO API (quarentena) ao ISE, que é uma sessão HTTPS e pode ser decifrado em Wireshark (com o secure sockets layer (SSL) de encaixe e a chave privada do certificado administrativo da BANDEJA):

17	0 172.16.31.206	172.16.31.202	LSv1	83 Client Hello					
12	1 172.16.31.202	172.16.31.206	TCP	66 https > 48046 [ACK] Seq=1 Ack=518 Win=15516 Len=0 TSval=389165957 TSecr=97280105					
12	2 172.16.31.202	172.16.31.206	TCP 2	952 [TCP segment of a reassembled PDU]					
12	3 172.16.31.202	172.16.31.206	TLSv1	381 Server Hello, Certificate, Certificate Request, Server Hello Done					
12	4 172.16.31.206	172.16.31.202	TOP	66 48046 > https [ACK] Seq=518 Ack=1449 Win=17536 Len=0 TSval=97280106 TSecr=389165957					
12	5 172.16.31.206	172.16.31.202	TCP	66 48046 > https [ACK] Seq=518 Ack=2897 Win=20480 Len=0 TSval=97280106 TSecr=389165857					
12	6 172.16.31.206	172.16.31.202	TOP	66 48046 > https [ACK] Seq=518 Ack=3512 Win=23296 Len=0 TSval=97280106 TSecr=389165958					
12	7 172.16.31.206	172.16.31.202	TLSv1	04 Certificate, Client Key Exchange, Change Cipher Spec, Finished					
12	8 172.16.31.202	172.16.31.206	T_Sv1	72 Change Cipher Spec					
12	9 172.16.31.202	172.16.31.206	TLSv1	19 Finished					
13	0 172.16.31.206	172.16.31.202	TCP	66 48046 > https [ACK] Seq=856 Ack=3571 Win=23296 Len=D TSval=97280107 TSecr=389165962					
13	31 172.16.31.206	172.16.31.202	HITP	295 GET /ise/eps/QuarantineByTP/172.16.50.50 HTTP/1.1					
13	2 172.16.31.202	172.16.31.206	TOP	66 https > 48046 [ACK] Seq=3571 Ack=1085 Win=17792 Len=0 TSval=389166020 TSecr=97280111					
13	5 172.16.31.202	172.16.31.206	HTTP/XML	123 HTTP/1.1 200 OK					
P Prov	en Contrata Lavar	accent, or e rail	CT 10010 T 1001	ay beciver, need thay only boar new bary contera					
✓ secu D	re sockets Layer	hantination Data	Contrard , bit						
ΥIL	Svi Hecono Layer: / Content Turna, Amel	Application Data	Protocal: htt						
	Content Type: Appl:	ication Data (23)							
	Version: TLS 1.0 (0	0x0301)							
	Length: 224								
	Encrypted Applicat:	ion Data: elde29F	aa3ce163e999dc	7e0e9F9Fdd21c9441cd117cb7e9					
🗢 Нуре	rtext Transfer Pro	tocol							
- ▶ GE	T /ise/eps/Quarant:	ineByTP/172.16.50	D.50 HTTP/1.1∖	-\n					
TE	: deflate,gzip;q=0	.3\r\n							
0	nnection: TE, close	e/r/n							
⊳ Au	Authorization: Basic YWRt#W46S3Cha293MTIz\r\n								
Ho	st: 172.16.31.202\	r\n							
Us	er-Agent: libww-p	erl/6.06\r∖n							
١٢	\r\n								
10	ull request URI: h	ttp://172.16.31.2	202/ise/eps/Qu	rantineByIP/172.16.50.50]					

No GET o pedido para o endereço IP de Um ou Mais Servidores Cisco ICM NT do atacante é passado (172.16.50.50), e esse host quarantined pelo ISE.

Navegue à análise > à correlação > ao estado a fim confirmar a remediação bem sucedida:

Overview Analysis Policies Devices Objects AMP											
Context Explorer	Connections *	Intrusions •	Files •	Hosts •	Users ¥	Vulnerabilities •	Correlation + Status	Custom •	Search		
										Bookmark This Page	
Remediation Status Date: View of Remediations											
No Search Constraints	is Search Constraints (<u>Edit Search</u>)										
Jump to *											
Time ×			Re	mediation N	ame ×		Pallicy ×		Rule *	Result Message ×	
4 📃 2015-05	-24 10:55:37		50.	rosP-Rered	lation		Correlation Policy		Correlatel CP80Block	Successful completion of remediation	
4 📃 2015-05	-24.10:47:08		500	rcelP-Remeti	ation		Correlation Policy		CorrelateTCP818lock	Successful completion of remediation	
$ C < Page _ 1]$ of 1	>>I Displaying r	ows 1-2 of 2 rows									
View	Delete										
View At	Delete All										

O ISE executa a quarentena e envia o CoA

Nesta fase, o ISE prrt-management.log notifica que o CoA deve ser enviado:

O tempo de execução (prrt-server.log) envia o terminatemessage CoA ao NAD, que termina a sessão (ASA):

```
DEBUG,0x7fad17847700,cntx=0000010786,CPMSessionID=2e8cdb62-bc0a-4d3d-a63e-f42ef8774893,
CallingStationID=08:00:27:DA:EF:AD, RADIUS PACKET: Code=40 (
DisconnectRequest) Identifier=9 Length=124
  [4] NAS-IP-Address - value: [172.16.31.100]
  [31] Calling-Station-ID - value: [08:00:27:DA:EF:AD]
  [49] Acct-Terminate-Cause - value: [Admin Reset]
  [55] Event-Timestamp - value: [1432457729]
  [80] Message-Authenticator - value:
[00:00:00:00:00:00:00:00:00:00:00:00:00]
  [26] cisco-av-pair - value: [audit-session-id=ac10206400021000555b9d36],
RadiusClientHandler.cpp:47
O ise.psc envia uma notificação similar a esta:
```

INFO [admin-http-pool51][] cisco.cpm.eps.prrt.PrrtManager -:::::- PrrtManager disconnect session=Session CallingStationID=192.168.10.21 FramedIPAddress=172.16.50.50 AuditSessionID=ac10206400021000555b9d36 UserName=cisco PDPIPAddress=172.16.31.202 NASIPAddress=172.16.31.100 NASPortID=null option=PortDefault

Quando você navega às **operações > à autenticação**, deve mostrar a *autorização dinâmica sucedida*.

A sessão de VPN é desligada

O utilizador final envia uma notificação a fim indicar que a sessão está desligada (para 802.1x/MAB/guest prendido/Sem fio, este processo é transparente):



Detalhes da mostra dos logs de Cisco AnyConnect:

10:48:05 AM Establishing VPN... 10:48:05 AM Connected to 172.16.31.100. 10:48:20 AM Disconnect in progress, please wait... 10:51:20 AM The secure gateway has terminated the VPN connection. The following message was received from the secure gateway: COA initiated

Sessão de VPN com acesso limitado (quarentena)

Porque sempre-no VPN é configurado, a sessão nova é construída imediatamente. Esta vez, a

regra ISE ASA-VPN_quarantine é batida, que fornece o acesso de rede limitado:

Authentiestions	👖 👖 Rep	porta	Adaptive	Network Central	Troubleshoot			
Misconfig	jured Suppl	cants (Ð.	Misco	nfigured Network Devic	es @	RADIUS Drops 🛞	Client Stopped
	0				0		0	0
🚮 Show Live Sessi	ons 🙀 Add	or Rema	ove Columns 🔻	🔗 Refresh	🚯 Reset Repeat Counts			Refresh Every 1
Time	T Status	Det	Repeat C	Identity D	Endpoint ID	Authorization Policy	Authorization Profiles	Event ①
2015-05-2410:51:	10 🕦	6	0	cisco	192,169,10,21			Session State Is Started
2015-05-2410:51:3	is 🔽	ò		#ACSACL#HP	Ð			DACL Download Succeeded
2015-05-2410:51:3	is 🔽	ò		cisco	192,169,10,21	${\tt Default} >> {\tt ASA-VPN}_quarantine$	UmitedAccess	Authentication succeeded
2015-05-24 10:51:	7 🔽	ò			08:00:27:DA/ER/AD			Dynamic Authorization succeeded
2015-05-24 10:48:0)1 🔽	ò		cisco	192,168,10,21	Default >> ASA-VPN	PermitAccess	Authentication succeeded

Note: O DACL é transferido em uma requisição RADIUS separada.

Uma sessão com acesso limitado pode ser verificada no ASA com o comando CLI do **anyconnect do detalhe da mostra VPN-sessiondb**:

```
asav# show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
                                   Index : 39
Public IP : 192.168.10.21
Username
           : cisco
Assigned IP : 172.16.50.50
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
           : 11436
Bytes Tx
                                    Bytes Rx : 4084
Pkts Tx : 8
                                    Pkts Rx
                                                : 36
Pkts Tx Drop : 0
                                   Pkts Rx Drop : 0
Group Policy : POLICY
                                    Tunnel Group : SSLVPN-FIRESIGHT
Login Time : 03:43:36 UTC Wed May 20 2015
           : 0h:00m:10s
Duration
Inactivity : 0h:00m:00s
                                              : none
VLAN Mapping : N/A
                                    VLAN
Audt Sess ID : ac10206400027000555c02e8
Security Grp : none
. . . . . .
DTLS-Tunnel:
<some output ommited for clarity>
Filter Name : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

Troubleshooting

Esta seção fornece a informação que você pode usar a fim pesquisar defeitos sua configuração.

FireSIGHT (centro da defesa)

O script da remediação ISE reside neste lugar:

Este é um script simples *Perl* que usa o subsistema de registro padrão de SourceFire (SF). Uma vez que a remediação é executada, você pode confirmar os resultados através de */var/log/messages*:

May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) Starting remediation
May 24 19:30:13 Defence SF-IMS[2414]: ise.pl:SourceIP-Remediation [INFO] [2414]
quar_ip:172.16.50.50 (1->3 sid:1) 172.16.31.202 - Success 200 OK - Quarantined
172.16.50.50 as admin

ISE

Éimportante que você permite o serviço de controle de rede adaptável no ISE. A fim ver o detalhado entra um processo do tempo de execução (*prrt-management.log* e *prrt-server.log*), você deve permitir o nível de debug para o Runtime-AAA. Navegue à **administração > ao sistema > registrando > debugam a configuração do log** a fim permitir debuga.

Você pode igualmente navegar às **operações > aos relatórios > ao valor-limite e aos usuários > auditoria adaptável do controle de rede** a fim ver a informação para cada tentativa e o resultado de um pedido da quarentena:

cisco Identity Services Engine			-					
	The Hos	BR Operations •	Policy * G	Auent Access *	Administration ¥			
Authentications Reports Control Troubleshoot								
Report Selector	Adaptive Network Co	ntrol Audit						
Favorites								
ISE Reports	From 05/24/2015 12:00:00	AM to 05/24/2015 09	138:21 PM					
Auth Services Status	Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session Admin	Admin IP
b reports Deployment Status	2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	512	ac1020640005	
12 reports	2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	512	ac102064000\$ admin	172.16.31.206
▼ Endpoints and Users	2015-05-24 21:29:47.5	08:00:27:DA:EF:A		Unquarantine	SUCCESS	507	ec102064000\$	
Client Provisioning	2015-05-24 21:29:47.4	08:00:27:DA:EF:A		Unquarantine	RUNNING	507	ac1020640005 admin	172.16.31.202
Current Active Sessions	2015-05-24 21:18:25.2	08:00:27:0A:EF:A		Quarantine	FALURE	480	ac1020640005	
Adaptive Network Control Audit	2015-05-24 21:18:25.2	08:00:27:DA:EF:A		Quarantine	RUNNING	480	ac1020640005 admin	172.16.31.202
🖓 Alters 🐷	2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	SUCCESS	471	ac1020640005	
* Time Range Today *	2015-05-24 21:11:19.8	08:00:27:DA:EF:A		Unquarantine	RUNNING	471	ac1020640005 admin	172.16.31.202
Bun	2015-05-24 21:10:13:5	192.168.10.21	172.16.50.50	Unquarantine	SUCCESS	462	ac1020640005	
Edama Mahila Davisa Managament	2015-05-24 21:10:13.5	192.168.10.21	172.16.50.50	Unquarantine	RUNNING	462	ac1020640005 admin	172.16.31.202
External Mobile Device Hanagemerk	2015-05-24 18:05:10.7	08:00.27:DA.EF.A		Quarantine	SUCCESS	337	ac1020640005	
Posture Detail Assessment	2015-05-24 18:05:10.7	08:00:27:DA:EF:A		Quarantine	RUNNING	337	ac1020640005 admin	172.16.31.202
Profiled Endpoints Summary	2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	330	ac1020640005	
Endpoint Profile Changes	2015-05-24 18:00:05.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	330	ac1020640005 admin	172.16.31.206
Top Authorizations by Endpoint	2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	291	ac1020640005	
Too & thorizations by liser	2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	RUNNING	291	ac1020640005 admin	172.16.31.206
Top excitorizations by user	2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	250	ac1020640005	
User Change Password Audit	2015-05-24 11:37:29.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	250	ac1020640005 admin	172.16.31.206
Supplicant Provisioning	2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	207	ac1020640002	
Registered Endpoints	2015-05-24 10:55:55.8	192.168.10.21	172.16.50.50	Quarantine	RUNNING	207	ac1020640005 admin	172.16.31.206
Endpoints Purge Activities	2015-05-24 10:55:29.7	08:00:27:DA-EF-A		Unquarantine	SUCCESS	206	ac1020640005	
Guest Access Reports Sirecorts	2015-05-24 10:55:29.7	08:00:27:DA-EF-A		Unquarantine	RUNNING	206	ac1020640005 admin	172.16.31.202
	2015-05-24 10:51:17.2	08:00:27:DA-EF-A		Quarantine	SUCCESS	189	ac1020640005	
Saved and Scheduled Reports	2015-05-24 10:51:17.2	08-00-27-04-FF-M		Quarantine	RUNNING	189	ac1020640002 admin	172.16.31.202

Erros

Refira a identificação de bug Cisco <u>CSCuu41058</u> (inconsistência da quarentena do valor-limite ISE 1.4 e falha VPN) para obter informações sobre de um erro ISE que seja relacionado às falhas da sessão de VPN (trabalhos 802.1x/MAB muito bem).

Informações Relacionadas

٠

- Integração do pxGrid da versão 1.3 ISE com aplicativo do pxLog IPS
- Guia do administrador do Cisco Identity Services Engine, liberação 1.4 Controle de rede adaptável da instalação
- Guia de referência do Cisco Identity Services Engine API, liberação 1.2 Introdução aos serviços repousantes externos API
- <u>Guia de referência do Cisco Identity Services Engine API, liberação 1.2 Introdução ao</u> <u>RESTO API da monitoração</u>
- Guia do administrador do Cisco Identity Services Engine, liberação 1.3
- Suporte Técnico e Documentação Cisco Systems