Configurar serviços de correção com integração ISE e FirePower

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados Configurar Diagrama de Rede FireSight Management Center (Defense Center) Módulo de correção do ISE Política de correlação **ASA** ISE Configurar o NAD (Network Access Device, dispositivo de acesso à rede) Habilitar controle de rede adaptável DACL de quarentena Perfil de autorização para quarentena Regras de autorização Verificar O AnyConnect inicia a sessão de VPN do ASA Acerto na política de correlação do FireSight O ISE realiza a guarentena e envia CoA Sessão VPN desconectada Troubleshoot FireSight (Centro de defesa) ISE Bugs Informações Relacionadas

Introduction

Este documento descreve como usar o módulo de correção em um dispositivo Cisco FireSight para detectar ataques e corrigir automaticamente o invasor com o uso do Cisco Identity Service Engine (ISE) como servidor de políticas. O exemplo fornecido neste documento descreve o método usado para remediar um usuário remoto de VPN que se autentica via ISE, mas também pode ser usado para um usuário 802.1x/MAB/WebAuth com ou sem fio.

Note: O módulo de correção mencionado neste documento não é oficialmente suportado pela Cisco. Ele é compartilhado em um portal da comunidade e pode ser usado por qualquer pessoa. Nas versões 5.4 e posteriores, também há um módulo de correção mais recente disponível, baseado no protocolo *pxGrid*. Este módulo não é suportado na versão 6.0, mas está planejado para ser suportado em versões futuras.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN do Cisco Adaptive Security Appliance (ASA)
- Configuração do Cisco AnyConnect Secure Mobility Client
- Configuração básica do Cisco FireSight
- Configuração básica do Cisco FirePower
- configuração do Cisco ISE

Componentes Utilizados

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

- Microsoft Windows 7
- Cisco ASA versão 9.3 ou posterior
- Software Cisco ISE versões 1.3 e posteriores
- Cisco AnyConnect Secure Mobility Client versões 3.0 e posteriores
- Cisco FireSight Management Center versão 5.4
- Cisco FirePower versão 5.4 (máquina virtual (VM))

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Use as informações fornecidas nesta seção para configurar seu sistema.

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

Diagrama de Rede

O exemplo descrito neste documento usa esta configuração de rede:



Este é o fluxo para esta configuração de rede:

- 1. O usuário inicia uma sessão VPN remota com o ASA (via Cisco AnyConnect Secure Mobility Versão 4.0).
- 2. O usuário tenta acessar *http://172.16.32.1*. (O tráfego é movido pelo FirePower, que é instalado na VM e gerenciado pelo FireSight.)
- 3. O FirePower é configurado para bloquear (em linha) o tráfego específico (políticas de acesso), mas também tem uma Política de correlação que é acionada. Como resultado, ele inicia a correção do ISE por meio da REST Application Programming Interface (API) (o

método QuarantineByIP).

- Quando o ISE recebe a chamada da API REST, ele procura a sessão e envia uma Alteração de Autorização RADIUS (CoA - RADIUS Change of Authorization) para o ASA, que encerra essa sessão.
- 5. O ASA desconecta o usuário da VPN. Como o AnyConnect está configurado com acesso VPN sempre conectado, uma nova sessão é estabelecida; entretanto, desta vez, uma regra de autorização ISE diferente é combinada (para hosts em quarentena) e o acesso limitado à rede é fornecido. Neste estágio, não importa como o usuário se conecta e se autentica à rede; enquanto o ISE for usado para autenticação e autorização, o usuário terá acesso limitado à rede devido à quarentena.

Como mencionado anteriormente, esse cenário funciona para qualquer tipo de sessão autenticada (VPN, 802.1x/MAB/Webauth com fio, 802.1x/MAB/Webauth), desde que o ISE seja usado para autenticação e o dispositivo de acesso à rede ofereça suporte à CoA RADIUS (todos os dispositivos modernos da Cisco).

Tip: Para mover o usuário para fora da quarentena, você pode usar a GUI do ISE. Versões futuras do módulo de correção também podem suportá-lo.

FirePower

Note: Um dispositivo VM é usado para o exemplo descrito neste documento. Somente a configuração inicial é executada via CLI. Todas as políticas são configuradas no Cisco Defense Center. Para obter mais detalhes, consulte a seção <u>Informações Relacionadas</u> deste documento.

A VM tem três interfaces, uma para gerenciamento e duas para inspeção em linha (interna/externa).

Todo o tráfego dos usuários da VPN se move pelo FirePower.

FireSight Management Center (Defense Center)

Política de controle de acesso

Depois de instalar as licenças corretas e adicionar o dispositivo FirePower, navegue até **Policies > Access Control** e crie a política de acesso usada para descartar o tráfego HTTP para 172.16.32.1:

Overview Analysis Polici	es Devices Ob	ects AMP								1	😔 Heath 🛛 S	ystern Ha	ov a	dinin v
Access Control Intrusion *	Files Networ	k Discovery SSL	Application Dete	stors Users	Correlation	Actions *								
AccessPolicy											ina 🛛 🔘 G	resi 📝	Save and	d App Is
Enter a description	- Intelligence 1077	Descenaria delune	- And											
B Film in Design	y anseigence - MTT	Presponses Police	cad .						O ANI CI	And the	Search Rules			×
									· ·····				_	
e Name	Secres James	Deat Zones	Searce Networks	Dest Natworks	VLAN Tage	Users	Applications	Sec Parts	Deat Parts	URLa	Action			
Astroinisterator Balan														
This category is empty														
Standard Rales														
3 Drap#DP80	any .	aty	any .	# 172.15.32.1	WV.	#09	any	MP.	P BITTP	any .	🗶 Black		a 🔝	10
Root Rules														
This category is empty														
Defea 8 Addres									Selevators 1	Prevention: Deletion Deca	By and Garray	aver,	-	\$

Todo o tráfego restante é aceito.

Módulo de correção do ISE

A versão atual do módulo ISE que é compartilhada no portal da comunidade é *ISE 1.2 Remediation Beta 1.3.19*:



Navegue até Policies > Actions > Remediations > Modules e instale o arquivo:

Overview Analysis Policies Devices Objects A	AMP				
Access Control Intrusion Files Network Discovery	SSL Application Detector	ors 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 a	ddress in a Cisco IO	05 router	
Cisco PIX Shun	1.1	Shun an IP a	ddress in the PIX fi	rewall	
ISE 1.2 Remediation	1.3.19	Quarantine II	addresses using 3	dentity Services Engine 1.2	
Nmap Remediation	2.0	Perform an N	map Scan		
Set Attribute Value	1.0	Set an Attrib	ute Value		

A instância correta deve ser criada. Navegue até **Policies > Actions > Remediations > Instances** e forneça o endereço IP do Policy Administration Node (PAN), juntamente com as credenciais administrativas do ISE necessárias para a API REST (um usuário separado com a função *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 (invasor) também deve ser usado para correção:

Configured Remediations								
Remediation Name Remediation Type Description								
No conf	igured remediations availab	le						
Add a new remediation of	type Quarantine Source IP	V Add						

Agora você deve configurar uma regra de correlação específica. Esta regra é acionada no início da conexão que corresponde à regra de controle de acesso configurada anteriormente (*DropTCP80*). Para configurar a regra, navegue para **Políticas > Correlação > Gerenciamento de regras**:

Overview Analy	sis Policies	Devices Obj	ects AMP					
Access Control	Intrusion V Fil	es Network E	Discovery SS	L Application E	Detectors	Users	Correlation	Actions 🔻
Policy Managen	nent Rule M	anagement	White List	Traffic Profiles	:			
Rule Informat	ion							
Rule Name	CorrelateTCP	30Block						
Rule Description								
Rule Group	Ungrouped	~						
Select the typ	e of event for	this rule						
If a connection	event occurs 🗸	at the beginning of	f the connection	v	and it mee	ts the fol	lowing condition	15:
() A	Add condition	Add complex o	ondition					
×	Access Control Rul	e Name 🗸 🗸	contains the stri	ng 🗸 DropTCP80				
Rule Options								
Snooze	If this rule g	enerates an event,	snooze for 0	hours v				
Inactive Periods	There are no	defined inactive pe	eriods. To add an	inactive period, click	Add Inactiv	e Period".		

Esta regra é usada na Política de correlação. Navegue até **Policies > Correlation > Policy Management** para criar uma nova política e adicione a regra configurada. Clique em **Corrigir** à direita e adicione duas ações: **correção para sourceIP** (configurado anteriormente) e **syslog**:

Overview Analysis Po	ficies Devices Objects AMP		🖲 Health - System - Heip 🖲	edirelin v
Access Control Enclusion	Files Retwork Discovery Sol. Application Detectors: Users	Certwation Adapter		
			Auto Familiato	FR GENER
Polics Henagement	Rule Management Write List Traffic Profiles			
Correlation Policy 3rd	ormotic n		Sere	Cancal
Policy Name	Constant on Parlies			
Petroy Description				
Default Priority	Bet M			
Policy Rules			0.4	do Rules
Bala		Bargeroon .	Priority	
Correlate 762908lock		mellog (Stelling) SourcatP-Ramot also: phonocatorio	[Mat v	4 3
		spannes for translation statement (1997) (19		

Assegure-se de habilitar a política de correlação:



ASA

Um ASA que atua como um gateway VPN é configurado para usar o ISE para autenticação. É também necessário habilitar a contabilidade e o RADIUS CoA:

```
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 NAD (Network Access Device, dispositivo de acesso à rede)

Navegue até **Administration > Network Devices** e adicione o ASA que atua como um cliente RADIUS.

Habilitar controle de rede adaptável

Navegue até Administration > System > Settings > Adaptive Network Control para ativar a API de quarentena e a funcionalidade:



Note: Nas versões 1.3 e anteriores, esse recurso é chamado de *Serviço de proteção de endpoint*.

DACL de quarentena

Para criar uma Lista de Controle de Acesso (DACL - Access Control List) para download usada para os hosts em quarentena, navegue para **Política > Resultados > Autorização > ACL para download**.

Perfil de autorização para quarentena

Navegue até **Policy > Results > Authorization > Authorization Profile** e crie um perfil de autorização com o novo DACL:

cisco Identity Services Engine	1	Home	Operations 🔻	Policy 🔻	Guest Access
Authentication 👩 Authorization	🔀 Profiling 🛛 👩 F	osture	딣 Client Prov	isioning	🚉 TrustSec
Dictionaries Conditions Results					
Results	Authorization Prof Authorization * Name Description * Access Type Service Template	iles > Limi Profile	Access Access	Ţ	
 Client Provisioning 	▼ Common Ta	sks			
 TrustSec 	Z DACL Name		DE	ENY_ALL_QUA	ARANTINE T

Regras de autorização

Você deve criar duas regras de autorização. A primeira regra (ASA-VPN) fornece acesso total para todas as sessões de VPN terminadas no ASA. A regra *ASA-VPN_quarantine* é acessada para a sessão VPN reautenticada quando o host já está em quarentena (o acesso limitado à rede é fornecido).

Para criar essas regras, navegue para Política > Autorização:

alialia cucco Ide	antity Corvices Engine					_		
CISCO 10	entity Services Engine		1 Home	Operations V	Policy 🔻	Guest Access 🔻	Ac	Iministration 🔻
💄 Authenti	cation o Authorization	K Profiling	Rosture	Client Provi	sioning	🚊 TrustSec	🐥 Pol	licy Elements
Authorizati	ion Policy							
Define the Auth For Policy Expo First Matche	orization Policy by configuring rules of the state of the second s	based on identity gr > Backup & Rest	oups and/or other tore > Policy Exp	conditions. Drag a port Page	and drop rules	to change the order.		
Exception	s (0)							
Standard								
Status	Rule Name	Condi	itions (identity grou	ps and other con	ditions)			Permissions
	ASA-VPN_quarantine	if (DEVI Sessio	CE:Device Type E0 on:EPSStatus EQU	UALS All Device ALS Quarantine)	Types#ASA-	PN AND	then	LimitedAccess
	ASA-VPN	If DEVIC	E:Device Type EQ	UALS All Device	Types#ASA-V	PN	then	PermitAccess

Verificar

Use as informações fornecidas nesta seção para verificar se a configuração funciona corretamente.

O AnyConnect inicia a sessão de VPN do 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)			alhalh cisco

O ASA cria a sessão sem qualquer DACL (acesso total à rede):

asav# show vpn-sessiondb details anyconnect

Session Type: AnyConnect Index : 37 Username : cisco Assigned IP : 172.16.50.50 Public IP : 192.168.10.21 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel : AnyConnect Essentials License 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 : 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 VLAN : none VLAN Mapping : N/A Audt Sess ID : ac10206400025000555bf975 Security Grp : none DTLS-Tunnel: <some output omitted for clarity>

O usuário tenta acessar

Quando o usuário tenta acessar http://172.16.32.1, a política de acesso é atingida, o tráfego correspondente é bloqueado inline e a mensagem de syslog é enviada do endereço IP de gerenciamento do 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,
```

Acerto na política de correlação do FireSight

A Política de correlação do gerenciamento do FireSight (Defense Center) é atingida, o que é relatado pela mensagem de syslog enviada do Defense Center:

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)

Neste estágio, o Defense Center usa a chamada REST API (quarentena) para o ISE, que é uma sessão HTTPS e pode ser descriptografada no Wireshark (com o plug-in Secure Sockets Layer (SSL) e a chave privada do certificado administrativo PAN):

120 172.16.31.206	5 172,16,31,202	TLSv1	583 Client Hello
121 172.16.31.202	2 172,16,31,206	TCP	66 https > 48046 [ACK] Seq=1 Ack=518 Win=15516 Len=0 TSval=389165857 TSecr=97280105
122 172.16.31.202	2 172.16.31.206	TCP	2962 [TCP segment of a reassembled PDU]
123 172.16.31.202	2 172.16.31.206	T_Sv1	681 Server Hello, Certificate, Certificate Request, Server Hello Done
124 172.16.31.206	6 172.16.31.202	TCP	66 48046 > https [ACK] Seq=518 Ack=1449 Win=17536 Len=0 TSval=97280106 TSecr=389165957
125 172.16.31.206	6 172.16.31.202	TCP	66 48046 > https [ACK] Seq=518 Ack=2897 Win=20480 Len=0 TSval=97280106 TSecr=389165957
126 172.16.31.206	6 172.16.31.202	TCP	66 48046 > https [ACK] Seq=518 Ack=3512 Win=23296 Len=0 TSval=97280106 TSecr=389165858
127 172.16.31.206	6 172.16.31.202	T_Sv1	404 Certificate, Client Key Exchange, Change Cipher Spec, Finished
128 172.16.31.202	2 172.16.31.206	T_Sv1	72 Change Cipher Spec
129 172.16.31.202	2 172.16.31.206	T_Sv1	119 Finished
130 172.16.31.206	i 172.16.31.202	TCP	66 48046 > https [ACK] Seq=856 Ack=3571 Win=23296 Len=0 TSval=97280107 TSecr=389165962
131 172.16.31.206	i 172.16.31.202	HITP	295 GET /ise/eps/QuarantineByIP/172.16.50.50 HTTP/1.1
132 172.16.31.202	2 172.16.31.206	TCP	66 https > 48046 [ACK] Seq=3571 Ack=1085 Win=17792 Len=0 TSval=389166020 TSecr=97280111
135 172.16.31.202	2 172.16.31.206	HTTP/XML	423 HTTP/1.1 200 OK
			MARTINE HALL INTER TITLES TOTAL MARTINE MARTINE CONTRACT TOTAL CONTRACTOR

> Secure Sockets Layer > TLSv1 Record Layer: Application Data Protocol: http Content Type: Application Data (23) Version: TLS 1.0 (0x0301) Length: 224 Encrypted Application Data: elde29Faa3ceF63e9Sdc97eDe9F9Fdd21c9441cd117cb7e9... > Hypertext Transfer Protocol > GET /ise/eps/QuarantineByTP/172.16.50.50 HTTP/1.1\r\n TE: deflate,gzip;q=0.3\r\n Connection: TE, close\r\n > Authorization: Basic YWRt#V46S3Dha293MTI2\r\n Host: 172.16.31.202\r\n User-Agent: Libwww-per1/6.05\r\n \r\n [Full request LRI: http://172.16.31.202/ise/eps/QuarantineByTP/172.16.50.50]

Na solicitação GET para o endereço IP do invasor, passa (172.16.50.50) e esse host é colocado em quarentena pelo ISE.

Navegue até Análise > Correlação > Status para confirmar a correção bem-sucedida:

Overview Analy	ysis Policies	Devices Object	ts AMP						
Context Explorer	Connections *	Intrusions •	Files * Hosts *	Users • \	Vulnerabilities *	Correlation + Status	Custom •	Search	
									Bookmark This Page
Remediation	diations								II 2215
No Search Constraints	(Edit Search)								
Jump to *									
Time >	¢		Remediation N	ame ×		Pellicy ×		Rule *	Result Message *
4 📃 2015-0	1-24 10:55:37		Source@-Remed	ation		Correlation Policy		Correlated O'00Block	Successful completion of remediation
4 📃 2015-00	5-24 10:47:08		SourcelP-Remet	ation		Correlation Policy		CorrelateF 09818lock	Successful completion of remediation
IK < Page 1 of 1	>>I Displaying ro	ows 1-2 of 2 rows							
View View All	Delete Delete All								

O ISE realiza a quarentena e envia CoA

Neste estágio, o ISE prrt-management.log notifica que o CoA deve ser enviado:

O tempo de execução (prrt-server.log) envia a mensagem *de terminação* de CoA ao NAD, que encerra a sessão (ASA):

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 para **Operations > Authentication**, ele deve mostrar *Dynamic Authorization bem-sucedido*.

O usuário final envia uma notificação para indicar que a sessão está desconectada (para 802.1x/MAB/convidado com fio/sem fio, este processo é transparente):

🕥 Cisco AnyCo	nnect Secure Mobility Clie	nt		X
	VPN: The secure gateway has te The following message was 172.16.31.100	rminated the VPI received from th	N connection. ne secure Connect	
\$ (i)			_	altalta cisco

Os detalhes dos registros do Cisco AnyConnect mostram:

```
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 VPN com acesso limitado (quarentena)

Como a *VPN sempre ativa* está configurada, a nova sessão é criada imediatamente. Desta vez, a regra *ASA-VPN_quarantine* do ISE é atingida, o que fornece o acesso limitado à rede:

🔜 Authenticutions 🕺 😤 Reports 👘 Adaptive Network Control 💦 Troubleshoot												
Misconfigured Supplicants 🛞				Ð	Misco	nfigured Network Devi	ces 🕅	RADIUS Drops 🛞	Client Stopped			
0					0		0	0				
🖬 Show Live Sessions 🖓 Add or Remove Columns 🔹 🏀 Refresh 👔 Reset Repeat Counts 🔹 😵 Refresh 👔 Reset Repeat Counts												
Time	•	Status Ali 👻	Det	Repeat C	Identity D	Endpoint ID	Authorization Policy	Authorization Profiles	Event ①			
2015-05-	2410:51:40	0	ò	0	cisco	192,168,10,21			Session State Is Started			
2015-05-	2410:51:35	2	ò		#ACSACL#+P	-D			DACL Download Succeeded			
2015-05-	2410:51:35	×	ò		cisco	192,169,10,21	Default >> ASA-VPN_quarantine	UmitedAccess	Authentication succeeded			
2015-05-	2410:51:17	1	ò			08:00:27:DA/ER.AD			Dynamic Authorization succeeded			
2015-05-	2410:46:01	1	ò		cisco	192,169,10,21	Default >> ASA-VPN	PermitAccess	Authentication succeeded			

Note: O DACL é baixado em uma solicitação RADIUS separada.

Uma sessão com acesso limitado pode ser verificada no ASA com o comando CLI show vpnsessiondb detail anyconnect:

```
asav# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
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
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx
           : 11436
                                   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
Duration : 0h:00m:10s
Inactivity : 0h:00m:00s
                          VLAN : none
VLAN Mapping : N/A
Audt Sess ID : ac10206400027000555c02e8
Security Grp : none
. . . . . .
DTLS-Tunnel:
 <some output ommited for clarity>
 Filter Name : #ACSACL#-IP-DENY_ALL_QUARANTINE-5561da76
```

Troubleshoot

Esta seção fornece informações que você pode usar para solucionar problemas de sua configuração.

FireSight (Centro de defesa)

O script de correção do ISE reside neste local:

```
root@Defence:/var/sf/remediations/ISE_1.3.19# ls
_lib_ ise-instance ise-test.pl ise.pl module.template
```

Este é um script de *perl* que usa o subsistema de registro padrão SourceFire (SF). Depois que a correção for executada, você poderá confirmar os resultados por meio do */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 habilite o serviço de controle de rede adaptável no ISE. Para visualizar os registros detalhados em um processo de tempo de execução (*prrt-management.log* e *prrt-server.log*), você deve habilitar o nível DEBUG para Runtime-AAA. Navegue até Administration > System > Logging > Debug Log Configuration para habilitar as depurações.

Você também pode navegar para **Operations > Reports > Endpoint and Users > Adaptive Network Control Audit** para exibir as informações de todas as tentativas e resultados de uma solicitação de quarentena:

cisco Identity Services Engine	A Hon	BR Operations V	Policy + Gui	nt Access 💌	Administration ¥			
Authentications 📑 Reports 🔯 Au	dapitve Network 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	:36:21 PM					
► Auth Services Status	Logged At	Endpoint ID	IP Address	Operation	Operation	Operation ID	Audit Session Admin	Admin IP
B reports	2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	512	ac1020640002	
12 reports	2015-05-24 21:30:32.3	192.168.10.21	172.16.50.50	Quarantine	RUNNING	512	ac1020640005 admin	172.16.31.206
▼ Endpoints and Users	2015-05-24 21:29:47.5	08:00:27:DA:EF:A		Unquarantine	SUCCESS	507	ac1020640005	
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:DA:EF:A		Quarantine	FAILURE	480	ac1020640005	
Adaptive Network Control Aude	2015-05-24 21:18:25.2	08:00.27:DA:EF:A		Quarantine	RUNNING	480	ac1020640005 admin	172.16.31.202
🖓 Aters 🚽	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
Burn	2015-05-24 21:10:13:5	192.168.10.21	172.16.50.50	Unquarantine	SUCCESS	462	ac1020640005	
	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 Management	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
Too Authorizations by Endpoint	2015-05-24 13:40:56.4	192.168.10.21	172.16.50.50	Quarantine	SUCCESS	291	ac1020640005	
The Automation by the second	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 Authorizations 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	ac1020640005	
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	
h Guard Arrange Barrate	2015-05-24 10:55:29.7	08:00:27:DA:EF:A		Unquarantine	RUNNING	206	ac1020640005 admin	172.16.31.202
 Guest Access Reports 5 reports 	2015-05-24 10:51:17.2	08:00:27:0A-EF-A		Quarantine	SUCCESS	189	ac1020640002	
Saved and Scheduled Reports	2015-05-24 10:51:17.2	08:00:27:DA-EF-A		Quarantine	RUNNING	189	ac1020640005 admin	172.16.31.202

Bugs

Consulte o bug da Cisco ID <u>CSCuu41058</u> (inconsistência de quarentena de endpoint ISE 1.4 e falha de VPN) para obter informações sobre um bug do ISE relacionado a falhas de sessão VPN (802.1x/MAB funciona bem).

Informações Relacionadas

- <u>Configurar a integração do WSA com o ISE para serviços cientes do TrustSec</u>
- Integração do ISE versão 1.3 pxGrid com aplicativo IPS pxLog
- <u>Cisco Identity Services Engine Administrator Guide, versão 1.4 Setup Adaptive Network</u>
 <u>Control</u>
- Guia de referência de API do Cisco Identity Services Engine, versão 1.2 Introdução à API de Serviços RESTful Externos
- Guia de referência da API do Cisco Identity Services Engine, versão 1.2 Introdução às APIs REST de monitoramento
- Guia do administrador do Cisco Identity Services Engine, versão 1.3

Suporte técnico e documentação - Cisco Systems