# Configurar a remediação do pxGrid de FirePOWER 6.1 com ISE

### Índice

Introdução Pré-requisitos Requisitos Componentes Utilizados Configurar Diagrama de Rede Configurar FirePOWER Configurar o ISE Verificar Troubleshooting Informações Relacionadas

# Introdução

Este documento descreve como configurar a remediação do pxGrid de FirePOWER 6.1 com Identity Services Engine (ISE). O módulo da remediação de FirePOWER 6.1+ ISE pode ser usado com serviço de proteção do valor-limite ISE (EP) para automatizar o qurantine/põr dos atacantes na camada de acesso de rede.

# Pré-requisitos

### Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Cisco ISE
- Cisco FirePOWER

#### **Componentes Utilizados**

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

- Correção de programa 4 da versão 2.0 de Cisco ISE
- Cisco FirePOWER 6.1.0
- Controlador virtual do Wireless LAN (vWLC) 8.3.102.0

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

Este artigo não cobre a configuração inicial da integração ISE com FirePOWER, integração ISE com diretório ativo (AD), integração de FirePOWER com AD. Para esta informação navegue à seção de referências. O módulo da remediação de FirePOWER 6.1 permite que o sistema de FirePOWER use capacidades ISE EP (quarentena, unquarantine, parada de porta) como uma remediação quando a regra da correlação é combinada.

Note: A parada de porta não está disponível para disposições wireless.

### Diagrama de Rede



A descrição do fluxo:

- 1. Um cliente conecta a uma rede, autentica com ISE e bate uma regra da autorização com um perfil da autorização que conceda o acesso irrestrito à rede.
- 2. O tráfego do cliente corre através então de um dispositivo de FirePOWER.
- 3. O usuário começa executar uma atividade mal-intencionada e bate uma regra da correlação que provoque por sua vez o centro de gerenciamento de FirePOWER (FMC) para fazer a remediação ISE através do pxGrid.
- 4. O ISE atribui uma quarentena de EPSStatus ao valor-limite e provoca a mudança do RAIO da autorização a um dispositivo do acesso de rede (WLC ou interruptor).

5. O cliente bate uma outra política da autorização que atribua um acesso restrito (as mudanças SGT ou reorientam ao portal ou negam o acesso).

**Note**: O dispositivo do acesso de rede (NAD) deve ser configurado para enviar o RAIO que explica ao ISE a fim fornecê-lo a informação do endereço IP de Um ou Mais Servidores Cisco ICM NT que é usada para traçar o endereço IP de Um ou Mais Servidores Cisco ICM NT a um valor-limite.

#### **Configurar FirePOWER**

Etapa 1. Configurar um exemplo da mitigação do pxGrid.

Navegue às **políticas > às ações > aos exemplos** e adicionar o exemplo da mitigação do pxGrid segundo as indicações da imagem.

Overview Analysis <b>Policies</b> Devices Objects AM	Ρ		Deploy 🌖 🏮	System	Help 🔻	admin 🔻
Access Control   Network Discovery Application Detectors	Correlation	Actions > Instances				
				Alerts I	Remediations	Groups
	Edit Instanc	e				
	Instance Name	ISE-NEW-INSTANCE				
	Module	pxGrid Mitigation(v1.0)				
	Description					
	Enable Logging	● On C Off				
		Create Cancel				

Etapa 2. Configurar uma remediação.

Há dois tipos disponíveis: Abrande o destino e abrande a fonte. Nesta fonte do exemplo a mitigação é usada. Escolha o tipo da remediação e o clique **adiciona** segundo as indicações da imagem:

Remediation Name	Remediation T	ype Description
No con	figured remediation	ns available
Add a new remediatio	on of type Mitigate	Destination 💌 🛛 Ad
Add a new remediatio	on of type   Mitigate   Mitigate	Destination 🗾

Atribua a ação da mitigação à remediação segundo as indicações da imagem:

Edit Remediation	
Remediation Name	QUARANTINE-SOURCE
Remediation Type	Mitigate Source
Description	
Mitigation Action	quarantine
<b>Whitelist</b> (an <i>optional</i> list of networks )	
	Create Cancel

Etapa 3. Configurar uma regra da correlação.

Navegue às **políticas > ao Gerenciamento da correlação > da regra** e o clique **cria a** regra da correlação da **regra** é o disparador para que a remediação aconteça. A regra da correlação pode conter diversas circunstâncias. Nesta regra da correlação do exemplo **PingDC** está batido se o evento da intrusão ocorre e o endereço IP de destino é 192.168.0.121. A regra feita sob encomenda da intrusão que combina a resposta de eco ICMP é configurada com a finalidade do teste segundo as indicações da imagem:

Overview Analysis Policies Devices Objects AMP	Deploy 🄑 System Help 🔻 admin 🕇
Access Control • Network Discovery Application Detectors Correlation Actions •	
	Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles	
Rule Information SAdd User Q	Qualification 3 Add Host Profile Qualification
Rule Name PingDC	
Rule Description	
Rule Group Ungrouped	
Select the type of event for this rule	
If an intrusion event occurs 🕙 and it meets the following conditions:	
Add condition     Add complex condition	
X Destination IP is I192.168.0.121	
Rule Options	O Add Inactive Period
Snooze If this rule generates an event, snooze for 0 hours	
Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".	

Etapa 4. Configurar uma política da correlação.

Navegue às **políticas > à correlação > ao Gerenciamento de políticas** e o clique **cria a política**, adiciona a regra à política e atribui a resposta a ele segundo as indicações da imagem:

Overview Analysis	Policies Devices O	Objects AM	P			Deploy	0	System	Help 🔻	admin 🔻
Access Control • Netwo	ork Discovery Applicat	ion Detectors	Correlation	Actions <b>v</b>						
								Alerts F	Remediatio	ns Groups
Policy Management	Rule Management	White List	Traffic Profile	es						
Correlation Policy Ir	nformation					You have unsa	ved cha	inges	Save	Cancel
Policy Name	ise_corellation_policy									
Policy Description										
Default Priority	None 💌									
Policy Rules									Ac	dd Rules
Rule		Response	s					Prior	rity	
PingDC		QUARANTI	NE-SOURCE (Reme	liation)				Defa	ault 💌	1

Permita a política da correlação segundo as indicações da imagem:

Overview Analysis Policies Devices Objects AMP	Deploy	🔑 System	Help 🔻 a	dmin 🔻
Access Control V Network Discovery Application Detectors Correlation Actions V				
		Alerts R	emediations	Groups
Policy Management Rule Management White List Traffic Profiles				
			🔾 Create	Policy
Name		So	rt by State	•
ise corellation policy			🕶 🦉 🕻	

### Configurar o ISE

Etapa 1. Configurar a política da autorização.

Navegue à **política > à autorização** e adicionar uma política nova da autorização que seja batida depois que a remediação ocorre. **Sessão do** uso: **EPSStatus IGUALA a quarentena** como a circunstância. Há diversas opções que podem ser usadas em consequência:

- Permita o acesso e atribua SGT diferente (reforce a limitação do controle de acesso em dispositivos de rede)
- Negue o acesso (o usuário deve ser retrocedido fora da rede e não deve poder conectar outra vez)
- Reoriente a um portal da lista negra (neste portal feito sob encomenda do ponto quente da encenação é configurado por esse motivo

identity Se	ervices Engine Home → Op	erations  → Policy → Guest Access → Administration → Work G	Centers 🚺 License Warning	j 🔺 🔍 🕘 🛓 🌣				
Authentication	Authorization Profiling Posture	Client Provisioning						
Authorization P Define the Authoriza For Policy Export go First Matched Rule	Authorization Policy Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page First Matched Rule Applies							
▼ Exceptions (	(3)							
Status F	Rule Name	Conditions (identity groups and other conditions)	Permissions					
🖉 🗹 🛛 A	AssignSGTBlockOnFP	Session:EPSStatus EQUALS Quarantine	then MaliciousUser AND PermitAccess	Edit   🕶				
	BlockOnISE	if Session:EPSStatus EQUALS Quarantine	then DenyAccess	Edit   🕶				
	BlockOnISE_copy	if Session:EPSStatus EQUALS Quarantine	then blacklist_redirect	Edit   🕶				

#### Configuração portal feita sob encomenda

Neste exemplo, o portal do ponto quente é configurado como uma **lista negra**. Há somente uma página da política de uso aceitável (AUP) com texto feito sob encomenda e não há nenhuma possibilidade para aceitar o AUP (este é feito com Javascript). A fim conseguir isto, você precisa primeiramente de permitir o Javascript e de colar então um código que esconda o botão e os controles AUP na configuração portal da personalização.

Etapa 1. Permita o Javascript.

Navegue à administração > ao sistema > aos ajustes Admin Access> > personalização portal. Escolha permitem a personalização portal com HTML e Javascript e clicam a salvaguarda.

diable Identity Services Engine	Home → Operations → Policy → Guest Access → Administration → Work Centers	1	License Warning 🔺	୍	0	4	\$		
System      Identity Management      Network Resources      Device Portal Management      pxGrid Services      Feed Service      Identity Mapping									
Deployment Licensing + Certificates + Logging + Maintenance Upgrade Backup & Restore - Admin Access - Settings									
G									
Authentication	▼ Portal Customization								
Authorization	O Enable Portal Customization with HTML								
➤ Administrators	Enable Portal Customization with HTML and JavaScript								
✓ Settings	Save								
Access									
Session									
Portal Customization									

Etapa 2. Crie um portal do ponto quente.

Navegue ao **acesso do convidado > configuram > portais do convidado** e o clique **cria**, a seguir escolhe o tipo do ponto quente.

ethidhi ctsco Identity Services Engine Home → Operations → Policy		Work Centers	License Warning 🔺	୍ ଡ	1 ¢			
Overview Guest Portals Guest Types Sponsor Groups Sponsor Port	als							
Guest Portals								
Choose one of the three pre-defined portal types, which you can edit, customize	e, and authorize for guest access.							
Create Edit Duplicate Delete								

Etapa 3. Configurar a personalização portal.

Navegue à **personalização portal da página** e mude títulos e índice para fornecer um aviso apropriado ao usuário.

dialo Ident	ity Services E	ngine	Home	<ul> <li>Operations</li> </ul>	Policy		<ul> <li>Administration</li> </ul>	Work Centers		1	License Warning 🔺			
✓ Configure	Manage Acc	ounts 🕨	Settings											
Overview	Guest Portals	Guest Ty	/pes Spo	nsor Groups S	oonsor Portals									
Pages				Page	Customization	s								
▼ Pa	ges			Browser Pa	ge Title ED ACCESS						Preview Settings			
Acc	thentication Su	Iccess		Optional Co	ntent 1	▼ Size	• 🛆 •   B I	U   ≣ ∦≣   Ø •	, ,	liulu R		ESS		
Err	or			X - [1]	<b>D</b>					RESTRI	CTED ACCESS			
<b>▼</b> Me	essages									You have maliciou	e been identified as s user and blocked	sa 1.		
Err	or Messages													
				(text or HTM	L) Click Previe	w to test HTML render	ring.		]					
				Content Title RESTRICTI	e ED ACCESS									
				Instructional	Text			TT   1- 1-   22	1					
				X + D	) an identified a	Size	• A • B I	⊻   ≔ }=   🌌 ▼						
				Tou have be	ien identified a	is a mailcious user a	na biockea.							

O rolo ao índice 2 da opção, fonte de alavanca do clique HTML, e cola o interior do script:

<script> (function() { jQuery('.cisco-ise-aup-text').hide(); jQuery('.cisco-ise-aupcontrols').hide(); setTimeout(function() { jQuery('#portal-session-timeout-popup-screen, #portalsession-timeout-popup-popup, #portal-session-timeout-popup').remove(); }, 100); })(); </script>

Fonte de Untoggle HTML do clique.

**Optional Content 2** 

Font	Size	<u>A</u> - B	I U 🗄 🗄 🖉 🕶 📔
X - 🔲 🖸			
<script></th><th></th><th></th><th></th></tr><tr><th>(function(){</th><th></th><th></th><th></th></tr><tr><th>jQuery('.cisco-is</th><th>e-aup-text').hide();</th><th></th><th></th></tr><tr><th>jQuery('.cisco-is</th><th>e-aup-controls').hide();</th><th></th><th></th></tr><tr><th>setTimeout(functio</th><th>on(){ jQuery('#portal-sessi</th><th>on-timeout-popup-scr</th><th>een, #portal-session-</th></tr><tr><th>timeout-popup-pop</th><th>pup, #portal-session-time</th><th>out-popup').remove();</th><th>}, 100);</th></tr><tr><th>3)O:</th><th></th><th></th><th></th></tr><tr><th></script>			
 <th>ogus_node="TRUE" /&gt;</th> <th></th> <th></th>	ogus_node="TRUE" />		
(text or HTML) Clic	k Preview to test HTML re	nderina.	

### Verificar

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

#### **FirePOWER**

O disparador para que a remediação aconteça é uma batida da política/regra da correlação. Navegue à **análise > à correlação > aos eventos da correlação** e verifique que o evento da correlação aconteceu.



#### ISE

O ISE deve então provocar o raio: O CoA e autenticar novamente o usuário, estes eventos pode ser verificado na **operação > no RAIO Livelog.** 

2017-02-16 13:26:22.894		0	alice	E4:B3:18:69:EB:8C	Windows10-Workst Default >> Dot1X >> D Default >> AssignSGT MaliciousUser,PermitAcc v	vWLC
2017-02-16 13:26:21.040	<b>~</b>	à		E4:B3:18:69:EB:8C	v	v₩LC
2017-02-16 13:25:29.036	<b>~</b>	0	alice	E4:B3:18:69:EB:8C	Windows10-Workst Default >> Dot1X >> D Default >> Standard R PermitAccess,Administra v	vWLC

Neste exemplo, o ISE atribuiu SGT diferente **MaliciousUser ao** valor-limite. No caso de **negue o** perfil que da autorização de **acesso o** usuário perde a conexão Wireless e não pode conectar outra vez.

A remediação com portal da lista negra. Se a regra da autorização da remediação é configurada para reorientar ao portal, deve olhar como esta da perspectiva do atacante:



### Troubleshooting

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

Navegue à **análise > à correlação > ao estado** segundo as indicações desta imagem.

Overview <mark>Analysis</mark> Policies Devices Objects AMP													stem Help	🔻 admin 🔻
Context Explorer	Connections •	Intrusions 🔻	Files 🔻	Hosts 🔻	Users 🔻	Vulnerabilities <b>•</b>	Correlation • Status	Custom •	Lookup 🔻	Search				
											Bookmark This Page	Report Designe	r View Book	marks Search
Remediation	n Status <sub>Idiations</sub>										20	7-02-16 14:25:0	00 - 2017-02	- <u>16 14:27:00</u> ⊘ Static
No Search Constraints ( <u>Edit Search</u> )														
Jump to •														
Time ×				iation Name	×		Policy ×	Rule ×		Result Message ×				
2017-02-16 14:26:19			QUARANTINE-SOURCE				ise corellation policy	PingDC		Successful completion of remediation				
< <page 1="" of="">&gt;  Displaying row 1 of 1 rows</page>														
View	Delete													
View All	Delete All													

A mensagem do resultado deve retornar a **conclusão bem sucedida da** mensagem da **remediação** ou de erro particular. Verifique o Syslog: **O sistema > a monitoração > o Syslog** e o filtro output com **pxgrid**. Os mesmos logs podem ser verificados em **/var/log/messages.** 

### Informações Relacionadas

- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html
- https://communities.cisco.com/docs/DOC-68284
- <u>https://communities.cisco.com/docs/DOC-68285</u>
- <u>https://communities.cisco.com/thread/64870?start=0&tstart=0</u>
- <u>http://www.cisco.com/c/en/us/td/docs/security/ise/2-</u> 0/admin\_guide/b\_ise\_admin\_guide\_20.html
- http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-configguide-v61.html