Integre vários clusters ISE com o Secure Web Appliance para políticas baseadas em TrustSec

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Limitações Diagrama de Rede Configurar Configuração do ISE Habilitar SXP Configurar o SXP nos nós do cluster Configurar o SXP no nó de agregação Ativar o pxGrid no nó de agregação Aprovação automática do pxGrid Configurações do TrustSec dos dispositivos de rede Autorização de dispositivo de rede SGT Política de Autorização Ativação do ERS no nó de agregação do ISE (opcional) Adicionar usuário ao grupo ESR Admin (Opcional) Configuração segura de dispositivo da Web Certificado pxGrid Ativar SXP e ERS no Secure Web Appliance Perfil de identificação Política de descriptografia baseada em SGT Configuração do Switch AAA **TrustSec** Verificar Informações Relacionadas

Introduction

Este documento descreve o procedimento para enviar informações de Security Group Tag (SGT) de várias implantações do ISE para um único Cisco Secure Web Appliance (Formalmente Web Security Appliance WSA) através do pxGrid para aproveitar as políticas de acesso à Web baseadas em SGT em uma implantação do TrustSec.

Antes da versão 14.5, o Secure Web Appliance só pode ser integrado a um único cluster do ISE para políticas de identidade baseadas em SGT. Com a introdução dessa nova versão, o Secure

Web Appliance agora pode interoperar com informações de vários clusters do ISE com um nó separado do ISE que se agrega entre eles. Isso traz grandes benefícios e nos permite exportar dados de usuários de diferentes clusters do ISE e a liberdade de controlar o ponto de saída que um usuário pode usar sem a necessidade de uma integração de 1:1.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity services engine (ISE)
- Dispositivo da Web seguro
- protocolo RADIUS
- TrustSec
- pxGrid

Componentes Utilizados

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

- Secure Web Appliance 14.5
- ISE versão 3.1 P3

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Limitações

- 1. Todos os clusters do ISE precisam manter mapeamentos uniformes para SGTs.
- 2. O nó de agregação do ISE deve ter o nome/número de SGTs do restante dos clusters do ISE.
- 3. O Secure Web Appliance só pode identificar a política (Acesso/Descriptografia/Roteamento) com base na tag SGT e não no grupo nem no nome de usuário.
- 4. Relatórios e rastreamento são baseados em SGT.
- 5. Os parâmetros de dimensionamento do ISE/Secure Web Appliance existentes continuam a ser aplicados a este recurso.

Diagrama de Rede



Processo:

1. Quando o usuário final se conecta à rede, ele recebe um SGT baseado em políticas de autorização no ISE.

2. Em seguida, os diferentes clusters do ISE enviam essas informações de SGT na forma de mapeamentos de SGT-IP para o nó de agregação do ISE por meio do SXP.

3. Nó de agregação do ISE receba essas informações e compartilhe-as com o único Secure Web Appliance por meio do pxGrid.

4. O Secure Web Appliance usa as informações de SGT que aprendeu para fornecer acesso aos usuários com base nas Políticas de Acesso à Web.

Configurar

Configuração do ISE

Habilitar SXP

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione **Administration > System > Deployment.**

Etapa 2. Selecione o nó que deseja configurar e clique em Editar.

		Administration •	System			α,	٢	528
Certificates	Logging	Maintenance	Upgrade Heal	th Checks Back	kup & Restore	Admin Access	Sett	ings
• De	ploymer	nt Nodes	🗟 Deregister			Selected 1 Total	1 2	•
	Hostoama	Personat		Bole(s)	Remines		laide Sta	
	Certificates	Certificates Logging Deploymen	Certificates Logging Maintenance Deployment Nodes Certificates Deployment Nodes Certificates Deployment Nodes	Oertificates Logging Maintenance Upgrade Healt O Deployment Nodes Image: Complexity Synows Deregister	Certificates Logging Maintenance Upgrade Health Checks Back	Administration - System Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes Image: Deployment Nodes	Administration - System Q Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Deployment Nodes Selected 1 Total	Administration - System Q 0 Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Sett Deployment Nodes Selected 1 Total 1 2 Maintenance System Admin Access Sett Selected 1 Total 1 2 Maintenance System Admin Access Sett

Etapa 3. Para ativar o SXP, marque a caixa Ativar serviço SXP

≡ Cisco	SE		A	dministration • S	ystem			Q.	0 28 0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
			2 ~	Enable Session	Services 🧿)			
				Include Node in Nod	te Group None		~ 0		
			Enab	ie Profiling Service 🕣					
			Cheb	ie Threat Centric NAC 5	iervice 🕕				
			-	Enable SXP Se	rvice 🕣				
				Use Interface	GigabitEthernet	0	~		

Etapa 4. Role para baixo e clique em Save

Note: Repita todas as etapas para o restante dos nós do ISE em cada cluster, incluindo o nó de agregação.

Configurar o SXP nos nós do cluster

Etapa 1. Selecione o ícone de três linhas em Centro de trabalho > TrustSec > SXP.

localizado no canto superior esquerdo e selecione

Etapa 2. Clique em +Add para configurar o nó de agregação do ISE como um par do SXP.

≡ Cisco	ISE	W	ork Centers - T	rustSec					Q	0	0 8
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings			
SXP Devices All SXP Mappings		SXP Devi	ces 💿			Rows/Page 2	~ K (1 /1>>	00	2 %	cal Rows
		C Refresh + Ad	ld 🛛 Trash 🗸 /	ear A	ssign SXP	Domain				V Filter	~ •

Etapa 3. Defina o Nome e o endereço IP do nó de agregação do ISE, selecione peer role como

LISTENER. Selecione PSNs necessários em Connected PSNs, obrigatório SXP Domains, selecione Enabled em status e, em seguida, selecione Password Type e required Version.

≡ Cisco	ISE		Work Cer	iters • Tru	stSe
Overview	Components	TrustSec Policy	Policy Sets	SXP	AC
SXP Devices		SXP Devices > SXP C	onnection		
All SXP Mappings		 Upload from a CS¹ 	/ file		
		- Add Single Device			
		Input fields marked v	with an asterisk (*)	are required	i.
		Name ISE Aggregation n	ode		
		IP Address * 10.50.50.125			
		Peer Role * LISTENER		~	
		Connected PSNs *			
		ise01-CL1 ×		\sim	



Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI
SXP Devices		SVD Domaina *			
All SXP Mappings		default x			
		delaute *			
		Status *			
		Enabled		<u> </u>	
		Password Type *			
		CUSTOM		\sim	
		Password			
		Version *			
		V4		\sim	
		 Advanced Settings 			
			Cancel	Save	

Etapa 4. Clique em Salvar

Note: Repita todas as etapas para o restante dos nós do ISE em cada cluster para criar uma conexão SXP com o nó de agregação. **Repita o mesmo processo no nó de agregação e selecione ALTO-FALANTE como função de peer.**

Configurar o SXP no nó de agregação

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em Work Center > TrustSec > Settings

Etapa 2. Clique na guia Configurações do SXP

Etapa 3. Para propagar os mapeamentos IP-SGT, marque a caixa de seleção **Publicar** vinculações SXP no pxGrid.



Etapa 4 (opcional). Defina uma senha padrão para as configurações do SXP em Senha global



Etapa 5. Role para baixo e clique em Salvar.

Ativar o pxGrid no nó de agregação

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em Administração > Sistema > Implantação.

Etapa 2. Selecione o nó que deseja configurar e clique em Editar.

E Cisco ISE		Administration •	System				· · · · · · · · Q	0 53 0
Deployment Licensing Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup &	Restore	Admin Access	Settings
Deployment < 12 0 > 3: Deployment 3: PAN Fallover	Deployr	nent Node	95 • 🔒 Cempus				Selected	Tobel1 ② ● All ∽ ▽
	- Host	same 🗠 Peri	sonas		Role(s)	Services		Node Status
	a bea	NO Adm	inistration, Monitoria	g, Policy Service	STANDALONE	SESSION, PROF	LER	•

Etapa 3. Para ativar o pxGrid, clique no botão ao lado de pxGrid.

Cisco ISE	Administration - System	୍ ୦ ହା ୧
Deployment Uconsing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
	Enable Session Services ()	
	include Node in Yorks Group Name 🗸 🔘	
	📑 Enables Problem Service 🕟	
	🗌 Knable Thread Canter MHG Servers 💮	
	Enable SXP Service ()	
	Use sectors Oppositionment 0 V	
	🗌 Enalte Device Admin Service 💿	
	Chatter Persons cleantly Service 🔾	
	() todat	

Etapa 4. Role para baixo e clique em Save.

Aprovação automática do pxGrid

Etapa 1. Navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione **Administration > pxGrid Services > Settings**.

Etapa 2. Por padrão, o ISE não aprova automaticamente o pxGrid para as solicitações de conexão de novos clientes pxGrid; portanto, você deve habilitar essa configuração marcando a caixa de seleção **Aprovar automaticamente novas contas baseadas em certificado**.



Etapa 3. Clique em Salvar

Configurações do TrustSec dos dispositivos de rede

Para que o Cisco ISE processe solicitações de dispositivos habilitados para TrustSec, você deve definir esses dispositivos habilitados para TrustSec no Cisco ISE.

Etapa 1. Navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione em **Administration > Network Resources > Network Devices.**

Etapa 2. Clique em +Adicionar.



Etapa 3. Insira as informações necessárias na seção Network Devices e nas configurações de autenticação RADIUS.

Etapa 4. Marque a caixa de seleção Configurações avançadas do TrustSec para configurar um dispositivo habilitado para TrustSec.

Cisco ISE	Administration - Network Resources
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers
Network Devices	TACACS Authentication Settings
Default Device	SNMP Settings
Device Security Settings	Advanced TrustSec Settings

Etapa 5. Clique na caixa de seleção Use Device ID for TrustSec Identification para preencher automaticamente o nome do dispositivo listado na seção Network Devices . Digite uma senha no campo Senha.



Note: A ID e a senha devem corresponder ao comando "cts credentials id <ID> password <PW>" que é configurado posteriormente no switch.

Etapa 6. Marque a caixa de seleção Send configuration changes to device para que o ISE possa enviar notificações de TrustSec CoA para o dispositivo.

Cisco ISE	Administration - Network Resources					
Network Devices	letwork Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More ~	
Network Devices						
Default Device	Y Tru	stSec Notifications and U	pdates			
Device Security Settings			1			
	* Dow	rioad environment data every	Days V			
			,			
	* Dow	rioad peer authorization policy every	Days 🗸			
	* Ann	thertication every	Days ¥ ()			
	* Dree	mail SOACL Into every	1			
			Days Y			
	Other 1	number devices to must this device				
	Send o	onfiguration changes to device	Using O CoA (0 cu		

Etapa 7. Marque a caixa de seleção Incluir este dispositivo ao implantar atualizações de mapeamento de tag de grupo de segurança.

Etapa 8. Para permitir que o ISE edite a configuração do dispositivo de rede, insira as credenciais do usuário nos campos **EXEC Mode Username** e **EXEC Mode Password**. Opcionalmente, forneça a senha de ativação no campo **Senha do modo de ativação**.

Note: Repita as etapas para todos os outros NADs que devem fazer parte do domínio TrustSec.

Autorização de dispositivo de rede

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Centros de trabalho > TrustSec > Política TrustSec.**

Etapa 2. No painel esquerdo, clique em Network Device Authorization.

Cisco ISE	Work Centers • TrustSec		α,	٢	Ç8	-0
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports	Settings				
Represe Policy ~	Network Device Authorization	o rubes to channe the order				
	Laboration and the second statement of the second statement					
Matrix Source Tree	Default Bule Default Default Default Default Default Default	, Devices Exe				

Etapa 3. À direita, use a lista suspensa ao lado de Edit e Insert new row above para criar uma

E Cisco ISE	Work Centers • TrustSec	
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports Settings	
Egress Policy ~ ~	Network Device Authorization Define the Network Device Authorization Policy by assigning 503s to network devices. Drag and drop rules to change th	Ne order.
Marin Source Tree	Default Rule If no rules defined or no match than TruetSec_Devices	ta 🗌
Destination Tree		mant new row above
Network Device Authorization		

Etapa 4. Defina um **Nome da regra, Condições** e selecione o SGT apropriado na lista suspensa em **Grupos de segurança.**

Etapa 5. Clique em Concluído à direita.

E Cisco ISE	Work	Centers - TrustSec		0.020
Overview Components	TrustSec Policy Policy Sets	SXP ACI Troubleshoot	t Reports Settings	
Egress Policy ~ Matrices List	Network Device A	withorization	devices. Drag and drop rules to change the order.	
fource Tree	Rule Name	Conditions	Security Group	
Destination Tree	🗄 📴 🗠 NDAD	# DEVICE.Device Type equals to	v then Trustlee, Devices v Dove	
Network Device Authorization	Default Rule	If no rules defined or no match	then Truetlet_Devices 64 -	

Etapa 6. Role para baixo e clique em Salvar.

SGT

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Centros de trabalho > TrustSec > Componentes.**

Etapa 2. No painel esquerdo, expanda Grupos de segurança.

Etapa 3. Clique em +Add para criar um novo SGT.

E Cisco ISE	Work Centers - TrustSec	0.0 00 0
Overview Components	TrueSec Policy Policy Sets SVP ACI Truchleshoot Reports Settings	
Security Groups	Constant Constant	
IP SGT State Mapping	Security Groups	
Security Group ACLs	For Policy Expert prior Administration + Society & Review + Policy Expert Prope	
Nataork Devices		Selected II Total 18
Traities Servers >	Ant + Ant ≤ Input ≤ Equal > B Tank > O Tank ⊗ York Depley	м ~

Etapa 4. Digite o nome e escolha um ícone nos campos apropriados.

Work Centers · TrustSec					
TrustSec Policy Policy Sets SXP ACI Troubleshoo					
Security Groups List > New Security Group					
Security Groups					
* Name					
Cluster1_Endpoints					
* Icon					

Etapa 5. Se desejar, dê a ele uma descrição e informe um Valor de Marca.

Note: Para poder inserir manualmente um valor de tag, navegue até Centros de trabalho > TrustSec > Configurações > Configurações gerais do TrustSec e selecione a opção O **usuário deve inserir o número SGT manualmente** em **Numeração de tag do grupo de segurança**.

Etapa 6. Role para baixo e clique em Enviar

Note: Repita essas etapas para todos os SGTs necessários.

Política de Autorização

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Policy > Policy Sets.**

Etapa 2. Selecione o conjunto de políticas apropriado.

Etapa 3. No conjunto de políticas, expanda a Política de autorização.

E Cisco ISE	Policy = P	hicy	Sets		Q. (5 5	2 0
Policy Sets-+ Wired Access				Reset	Reset Policyset Hitcourts	5	**
Status Policy Set Name Dec	scription Condition				Allowed Protocols / Server Segu		Hits
Q Such							
Wired Access	***		DEVICE Owners Type EQUALS All Device Types#Saltebras		Default Network Access		
			Radius NAS-Part Type EQUALS Ethernet				
> Authentication Policy (2)							
> Authorization Policy - Local Exceptions							
> Authorization Policy - Global Exceptions							
> Authorization Policy (1)							

Etapa 4. Clique no botão para criar uma Diretiva de Autorização.

 Authorization Policy (1) 					
		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

Etapa 5. Defina o Nome da regra, a(s) condição(ões e os Perfis obrigatórios e selecione o SGT apropriado na lista suspensa em Grupos de segurança.

		Results		
Status Rule Name	Conditions	Profiles	Security Groups	Hits Actions
Q Search				

Etapa 6. Clique em Salvar.

Ativação do ERS no nó de agregação do ISE (opcional)

O Serviço de API RESTful externo (ERS) é uma API que pode ser consultada pelo WSA para obter informações de grupo. O serviço ERS é desativado por padrão no ISE. Depois de habilitada, os clientes podem consultar a API se autenticarem como membros do grupo **ERS Admin** no nó ISE. Para ativar o serviço no ISE e adicionar uma conta ao grupo correto, siga estas etapas:

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em Administração > Sistema > Configurações.

Etapa 2. No painel esquerdo, clique em ERS Settings (Configurações ERS).

E Cisco IS	36		A	dministration - S	ystem			Q	0 98
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Client Provisioning FIPS Mode Security Settings Alarm Settings	ĺ	ERS S	ettings						
Posture Profiling	>	External RE The ERS se An ISE Adm For more in https://10.5	STM Services (D rvice is disabled t inistrator with the formation, please 0.50.125.9060/em	(5) is a REST API based ly default. " ERS-Admin" or " ERS visit the ERS SDK page (sdk	on HTTPS over p -Operator* group at:	ort 9060. assignment is required to	use the API.		
Protocols									
Endpoint Scripts	-	✓ ERS Se	tting for Adr	ninistration Node	,				
Proxy SMTP Server SMS Gateway		 Enable Deable 	Dis forheastWire Dis	•					
System Time ERS Settings		~ CSRF C	Check						

Etapa 3. Selecione a opção Enable ERS for Read/Write.

Etapa 4. Clique em Salvar e confirme com OK.

Adicionar usuário ao grupo ESR Admin (Opcional)

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione Administration > System > Admin Access

Etapa 2. No painel esquerdo, expanda Administrators e clique em Admin Users.

Etapa 3. Clique em +Add e selecione Admin User no menu suspenso.

≡ Cisco IS	SE		A	dministration • Sy	/stem						
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & R	estore	Admin Acces	s Setti	ngs
Authentication		Admir	istrator	S							
Authorization	>								Selec	ted 0 Total 1	00
Administrators	~	0 Edit -	- Add 🛞 C	hange Status	Delete D D	uplicate				All	< 7
Admin Users											
Admin Groups		0	Create an Admir	n User	Description	First Name	Last Name	Email Addr	ess Admi	n Groups	
			Select from Net	work Access Users	> Default Admin	User			Super	Admin	
Settings	>										

Etapa 4. Digite um nome de usuário e uma senha nos campos apropriados.

= Cisco	SE		A	dministration • S	ystem			Q.	0 20 0
Deployment	Licensing	Certificates L	ogging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Administrators List 3	> wsa						
Authorization	>	✓ Admin Use	Hr.						
Administrators	~	"Name wSA							
Admin Users									
Admin Groups		Datus 🖬 D	rabled 🗸						
Settings	>	Ernal			D inclusion	system alarms in emails			
		External 📖 🕻	0						
		Read Only							
		Inactive account	never disabi	•					
		✓ Password							
		* Password			G)			
		* Ro-Enter Pare	need		G				

Etapa 5. No campo Admin Groups , use a lista suspensa para selecionar o ERS Admin.

E Cisco ISE			Administration - System					Q,	ं ज़ ल		
Deployment Lic	ensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings		
Authentication		First Name									
Authorization	>	Last Name									
Administrators	Ŷ										
Admin Users		V Account	Ontions								
Admin Groups		Description									
Settings	>										
		✓ Admin	Groups ERS Admin		v +						
								Save	Reset		

Etapa 6. Clique em Salvar.

Configuração segura de dispositivo da Web

Certificado raiz

Se o projeto de integração usar uma autoridade de certificação interna como raiz de confiança para a conexão entre o WSA e o ISE, esse certificado raiz deverá ser instalado nos dois dispositivos.

Etapa 1. Navegue até Network > Certificate Management e clique em Manage Trusted Root Certificates para adicionar um certificado CA.

	cure Web Appliance			Secure Web Appliance is get	ting a new look. Try
⇒ s100v	Web Caracity Manager	Carrielle Carriera	Baturali	Contact Administration	
Reporting	web security Hanager	security services	Network	aystem Administration	
Certificate M	anagement				
	-				
Appliance Certifica	tes				
Add Certificate					
Certificate O	ommon Name Issued	By Domains	Status Time	Remaining Expiration	Date Delet
Export Certificate					
Weak Signature Us	lage Settings				
Re	strict Weak Signature Usage:	Disabled			
					Edit Setting
Contificate LODN V	didation Kettleon				
Centil	inste ECON Validation Unane	Disabled			
Cero	case rigora vanoación osage:	0.00000			Ede Camina
					tot story
Certificate Lists					
Updates					
File Type		Last Update		Current Version	New Update
Cisco Trusted Root C	ertificate Bundle	Success - Thu Jun 30 1	5:32:47 2022	2.1	Not Available
Cisco Certificate Bloc	ked List	Success - Wed May 11	21:04:06.2022	1.3	Not Available
No undates in penne	95.				Update No
and advances on briefly a					
Certificate Hana	spement				

Etapa 2. Clique em Import.

Custom Trusted Root Certificates
Import
Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Etapa 3. Clique em Escolher arquivo para localizar a CA raiz gerada e clique em Enviar.

Etapa 4. Clique em Enviar novamente.

Etapa 5. No canto superior direito, clique em Confirmar Alterações.



Etapa 6. Clique em Confirmar alterações novamente.

Certificado pxGrid

No WSA, a criação do par de chaves e do certificado para uso pelo pxGrid é concluída como parte da configuração dos serviços do ISE.

Etapa 1. Navegue até Rede > Identity Service Engine.

Etapa 2. Clique em Enable and Edit Settings.

Etapa 3. Clique em **Escolher arquivo** para localizar a CA raiz gerada e clique em **Carregar arquivo**.

Identity Services Engine	
Edit Mentily Bervices Engine Bettings	
C Enable 150 Service	
Primary 158 pedirid Node:	The Bild Applance will communicate with the 202 period node to support Bild Applance data subscription (regaing updates). A primary 202 period node (server) must be configured.
	(Institute or (Pv4 address)
	thil pedivid Node Contribute:
	If the ISE particle noise certificate is signed by a Certificate Authority, confirm that the Certificate Authority is taked in the Trustell Root Certificates list (see Network + Certificate Menagement) and upload the CA-agreed next certificate Network (in the Section and upped, export the certificate Next Next Device Next Certificate and the Next Next Order Next Next Next Next Next Next Report The certificate Next Next Next Next Next Next Next Ne
	Certification Oceane File No The chosen

Note: Um erro de configuração comum é carregar o certificado pxGrid do ISE nesta seção. O certificado CA raiz deve ser carregado no campo Certificado do nó pxGrid do ISE.

Etapa 4. Na seção Certificado de cliente do equipamento para Web, selecione Usar certificado e chave gerados.

Web Appliance Client Certificate:	for secure communication between the Web Appliance and the ISE particle servers, provide a client certificate. This may need to be uploa to the ISE particle node(t) configured above.	ebed
	Use Uploaded Certificate and Key	
	Certificate: Choose Fire No file chooses. Upload Files	
	Keyl Choose Fire No file choose	
	C Key is Encrypted	
	No certificate has been uploaded.	
	Use Generated Certificate and Key Generate New Certificate and Key	

Etapa 5. Clique no botão Gerar novo certificado e chave e preencha os campos de certificado necessários.

Generate Certificate an	d Key	×
Common Name:		
Organization:		
Organizational Unit:		
Country:		
Duration before expiration:	months	
Basic Constraints:	 Set X509v3 Basic Constraints Extension to Critical 	
Generate Cancel		

Etapa 6. Clique em Download Certificate Signing Request.

Note: É recomendável selecionar o botão **Submit** para confirmar as alterações na configuração do ISE. Se a sessão for deixada para expirar antes de as alterações serem enviadas, as chaves e o certificado gerados poderão ser perdidos, mesmo se o CSR tiver sido baixado.

Etapa 7. Depois de assinar o CSR com sua CA, clique em Choose File (Escolher arquivo) para localizar o certificado.

Web Appliance Client Certificate:	For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.
	O Use Uploaded Certificate and Key
	Certificate: Choose File No file chosen
	Key: Choose File No file chosen
	Key is Encrypted
	No certificate has been uploaded.
	Use Generated Certificate and Key Generate New Certificate and Key
	Common name: wsa.security/abunet Organization: Cisco
	Organizational Unit: Security
	Country: SE
	Expiration Date: May 10 19:19:26 2024 GMT
	Basic Constraints: Not Orlical
	Download Certificate Download Certificate Signing Request
	Signed Certificate:
	To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.
	Certificate: Choose file No file chosen Upload File.

Etapa 8. Clique em Upload File.

Etapa 9. Enviar e Confirmar.

Ativar SXP e ERS no Secure Web Appliance

Etapa 1. Clique nos botões Enable para SXP e ERS.

156 SG7 elicharge Policesi (SRP) Service:	Enabling the service, Web Applance will retrieve SDP Binding Tapic From ESE Services.
Enable 198 External Restful Service (085)	
The Web Applance retrieves Active Directory process, and local 201 pro Group Tage (2023), you should enable DRI.	sign from 25E using the 2855. If you are configuring the Web Applance's policies using Active Directory groups, or in combination with Secure

Etapa 2. No campo **ERS Administrator Credentials**, insira as informações do usuário que foram configuradas no ISE.

Etapa 3. Marque a caixa para Server name same as ISE pxGrid Node para herdar as informações configuradas anteriormente. Caso contrário, insira as informações necessárias.

Enable ISE External Restful Service (ERS)			
	ERS Administrator Credentials		
	Username:	WSA	
	Password:		
	ERS Servers		
	Server name same as ISE pxGrid Node		
	Primary:	ise-agg.securitylab.net	(Hostname or IPv4 address)
	Secondary (Optional):		(Hostname or IPv4 address)
	Port:	9060 (Enter the port re	mber specified for ERS in 1SE)

Etapa 4. Enviar e Confirmar.

Perfil de identificação

Para usar tags de grupos de segurança ou informações de grupos do ISE nas políticas do WSA, primeiro é necessário criar um perfil de identificação que utilize o ISE como meio de identificar usuários de forma transparente.

Etapa 1. Navegue até Web Security Manager > Authentication > Identification Profiles.

Etapa 2. Clique em Add Identification Profile.

Identification Profiles: Add Profile

Etapa 3. Informe um nome e, opcionalmente, uma descrição.

Etapa 4. Na seção Identificação e autenticação, use a lista suspensa para escolher Identificar usuários com ISE de forma transparente.

t / User Identification Profile Settings	
Enable Identification Profile	
Name: 🕐	ESE Profile (e.g. my IT Profile)
Description:	Identification profile for ISE Integration.
Insert Above:	2 (Global Woffle) V
Identification Method	
Identification and Authentication: 🕐	Transparently identify users with ISE
Fallback to Authentication Realm or Guest	If user information is not available from the Identity Services Engine:
Privilegen: (2)	Support Guest Privileges
	Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).
tership Definition	
vership is defined by any combination of the h	slowing options. All criteria must be met for the policy to take effect.
Define Members by Subnet:	(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001-420-80.1115, 2000-808-11-2000-808-10
Define Hembers by Protocol:	MITR/HITPS

Etapa 5. Enviar e Confirmar.

Política de descriptografia baseada em SGT

Etapa 1. Navegue até Web Security Manager > Web Policies > Decryption Policies.

Etapa 2. Clique em Add Policy.

Etapa 3. Informe um nome e, opcionalmente, uma descrição.

Etapa 4. Na seção Perfis de identificação e usuários, use a lista suspensa para escolher Selecionar um ou mais perfis de identificação.

Etapa 5. Na seção **Perfis de identificação**, use a lista suspensa para escolher o nome do perfil de identificação do ISE.

Etapa 6. Na seção Usuários e grupos autorizados, selecione Grupos e usuários selecionados.

Identification Profiles and Users:	Select One or More Identifical	ton Profiles 👻			
	Identification Profile	Authorized Users and Groups Add Edentification			
	ISE Profile	OAll Authenticated Users			
		Selected Groups and Users (7) ISE Secure Group Tage: No tags entered ISE Groups: No groups entered Users: No users entered			
		Guests (users falling authentication)			
	Authentication information may not be available at HTTPS connection time. For transparent renew traffic, user agent information is convolibility for decreation and/cise.				
	Authentication information may proxy traffic, user apent information for the station of the second	not be available at HTTPS connection time. For transp tion is unavailable for decryption policies.			

Etapa 7. Clique no hiperlink ao lado de Tags de grupo seguras ISE.

Etapa 8. Na seção Secure Group Tag Search, marque a caixa à direita do SGT desejado e clique em Add.

withorized Secure Group Tags				
Use the search function below to 1 Secure Group Tag(s) currently in	add Secure Group Tags. To remove cluded in this policy.	Secure Group Tags from this policy, use the Delete option	n.	
Secure Group Tag Name	SGT Number	SGT Description	Delete All	Π
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	0	-
4			•	-
			Delete]

Enter any text to search for a Sec Add button to add to this policy.	ture Group Tag name, number, or d	lescription. Select one or more Secure Group Tags from th	e list and use the
learth	х		
0 Secure Group Tag(s) select	od for Add		Add
Secure Group Tag Name	SGT Number	SGT Description	Select At
Production_Servers	15	Production Servers Security Group	0
Point of Sale Systems	10	Point of Sale Security Group	0
Test, Servers	13	Test Servers Security Group	0
Development_Servers	12	Development Servers Security Group	0
syop	15	8YOO Security Group	Ö
PCI_Servers	14	PCI Servers Security Group	0
Guesta	6	Guest Security Group	0
wer .	65535	Any Security Group	0
Unknown	0	Unknown Security Group	
Network_Services	3	Network Services Security Group	0
InustSec_Devices	2	TrustSec Devices Security Group	0
Cluster1_Endpoints	191	Endpoints residing in ISE Cluster-1	
Employees	4	Employee Security Group	

Etapa 9. Clique em **Concluído** para retornar.

Etapa 10. Enviar e Confirmar.

Configuração do Switch

AAA

```
aaa new-model
aaa group server radius ISE
server name ise01-cl1
server name ise02-cl1
ip radius source-interface Vlan50
aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting update newinfo periodic 2440
aaa accounting dot1x default start-stop group ISE
aaa server radius dynamic-author
client 10.50.50.120 server-key Cisco123
client 10.50.50.121 server-key Cisco123
auth-type any
radius server ise01-cl1
address ipv4 10.50.50.121 auth-port 1812 acct-port 1813
pac key Ciscol23
radius server ise02-cl1
address ipv4 10.50.50.120 auth-port 1812 acct-port 1813
pac key Cisco123
```

TrustSec

cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode) cts role-based enforcement

aaa authorization network cts-list group ISE cts authorization list cts-list

Verificar

Atribuição de SGT do ISE para o endpoint.

Aqui você pode ver um endpoint do cluster 1 do ISE atribuído a um SGT após a autenticação e autorização bem-sucedidas:

 v
 Monty
 Despine ID
 Despine ID
 Despine ID
 Automatice Publy
 Automatice Publy

Aqui você pode ver um endpoint do cluster 2 do ISE atribuído a um SGT após a autenticação e autorização bem-sucedidas:

v Merty Expert D Depart Pulls Anternation Pully Anternation Pully Anternation Pully Anternation Pully Platters v Incomp Server

Mapeamentos SXP

Como a comunicação SXP é habilitada entre os nós do ISE do cluster e o nó de agregação do ISE, esses mapeamentos de SGT-IP são aprendidos pela agregação do ISE por meio do SXP:

III Cieco ISE		Work Center	Work Centers - TrustSec			A Describe 2000 9. 0 58 0		
Overview Components	Trustlec Policy P	AD 40	Troubleshoot	Reports Settings				
10P Invites All 10P Maggings	All SXP Map	opings o						
	O have not be t	stali filar - Warage StP Solari I	-		11111/Pape 4	<u>v ()</u>)	1) + Tool Hool ∀Alase ~ @	
	IP Address	907	1/14	Learned From	Learned By	ERP Domain	PDNs involved	
	P Address	Notes, Jacob (2002)	UN	Learned From	Lowned By	DRP Domain	PDNs involved	
	# Address 14.08.56.573 14.08.50.773	Notes, Jorea (2002) Teather, Jorean (2002)	ve	Learned From 14:34:36:121,16:34:35:3 14:34:36:122,16:34:34:3	Learned By	BP bonain ortext	PSNs involved 1+++00 1++-00	
	# Address 16:36:36:572 16:36:36:772 16:36:36:727	BAT Tratfice_Device (2000) Tratfice_Device (2000) Device_Devices (2000)	-	Learned From 16:06:00:101,10:06:06:0 16:06:00:102,10:06:06:0 16:06:00:101,10:06:06:0	Laured By 547 547 547	BP Domain onlocit onlocit	PSNs bushed 10+100 10+100 10+100 10+100	

Esses mapeamentos do SXP, de clusters diferentes do ISE, são enviados ao WSA sobre pxGrid por meio do nó de agregação do ISE:



Aplicação de política baseada em SGT

Aqui você pode ver que os diferentes endpoints correspondem às suas respectivas políticas e o tráfego é bloqueado com base em seu SGT:

Endpoint que pertence ao cluster do ISE 1



Results						
					Items Displayed 50	ř
Displaying 1 - 50 of 13	7 items.				< Previous 1 2 3 Next	1
Time (GHT +02/00) ¥	website (count)	Display All Details	Disposition	Bandwidth	User / Client 3P	
14 34 2022 14 28 17	Mass//fibic.com/st2/fibicon.ice content minit- de. Contents Block UKLs CL1 CESTIMATION IP - CELVILS - Georgeten Policy 1158_Out Malware Analytics File Verdict: -	teri", WBRS: No Score,	Block - URL CH	œ	isemg_10.50.50.321_sgr311_10.50.50. Cdemtified by 10 10.50.50.1	12012

Endpoint que pertence ao Cluster 2 do ISE



Informações Relacionadas

- Web Security Appliance e Guia de integração do Identity Service Engine
- Configurar a integração do WSA com o ISE para serviços cientes do TrustSec
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.1
- Manual do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance